Дешеві китайські відеокамери можуть надсилати зняте відео в РФ, – розслідування

Читать на русском

Дешеві китайські відеокамери можуть надсилати зняте відео в РФ, – розслідування

Як свідчать IT-фахівці, зловмисник може стежити за тим, що фіксує камера. Так, за повідомленням СБУ, сталося 2 січня 2024 року, в день масованої російської атаки по українських містах. Тоді силовики виявили в столиці камери на приватних будинках, які транслювали роботу української ППО та локації критичної інфраструктури.

Нещодавно журналісти медіапроєкту "Схеми" спільно з IT-фахівцями провели експеримент, який довів, що тисячі відеокамер китайського виробництва є небезпечними для України. Про це пише "Радіо Свобода".

Журналісти-розслідувачі наприкінці 2023 року розповіли, що тисячі систем відеоспостереження з російським програмним забезпеченням Trassir працювали на вулицях міст України, приватних об'єктах і могли передавати безперешкодно дані до Москви.

Проте наразі існує ще одна небезпека — китайські відеокамери, які навіть масовіше використовують в Україні. Насамперед це камери виробництва двох китайських компаній — Hikvision і Dahua. До речі, імпорт продукції цих компаній заборонений у США як "загроза національній безпеці", а в Україні вони внесені до переліку міжнародних спонсорів війни.

Проте відеокамери працюють і продаються, і через їхню дешевизну українці віддають їм перевагу, коли купують камери для побутового використання. До того ж вони виявилися й у державних системах безпеки, зокрема в проєкті "Безпечне місто". Загалом китайський технологічний гігант Hikvision виробляє приблизно 20% усіх камер відеоспостереження у світі, Dahua — 10% усіх виробів. Ними масово користуються в усьому світі: у самому Китаї, Росії, країнах ЄС та ін. В Україні їх — сотні тисяч.

Фото: Радіо Свобода

Чому це небезпечно

Насамперед, на що звернули увагу журналісти, — це те, що камери, підключені до інтернету, відразу передають зображення на сервери китайського виробника. Куди може передаватися картинка та чи легко можна зламати захист і підключитися до камери нелегально, наприклад, із території Росії?

Разом із IT-спеціалістами "Схеми" провели експеримент із камерами випусків 2015, 2019 та 2023 років. Найвразливішими з технічного погляду, звичайно, виявилися камери перших двох випусків. Тобто такими, як підкреслили фахівці, що відправляють інформацію на сервери китайського виробника та легше можуть піддаватися хакерським атакам.

"Коли цю камеру підключили до інтернету, вона одразу почала з'єднуватися зі своїми серверами. Сервіс, який деанонімізує IP-адреси, тобто зв'язує з фізичною адресою, показав, що сервери розташовані в Ірландії, а їхній власник — американська компанія Amazon. Китайська компанія Hikvision орендує ці сервери, щоб користувачі мали можливість передавати й зберігати відео. Hikvision повністю контролює ці сервери як виробник камер і софту", — пояснили IT-спеціалісти.

Як додав експерт "Лабораторії цифрової безпеки" Іван Антонюк, це стандартна практика, але в такому разі користувач має довіряти виробнику, який несе відповідальність за конфіденційність і безпеку.

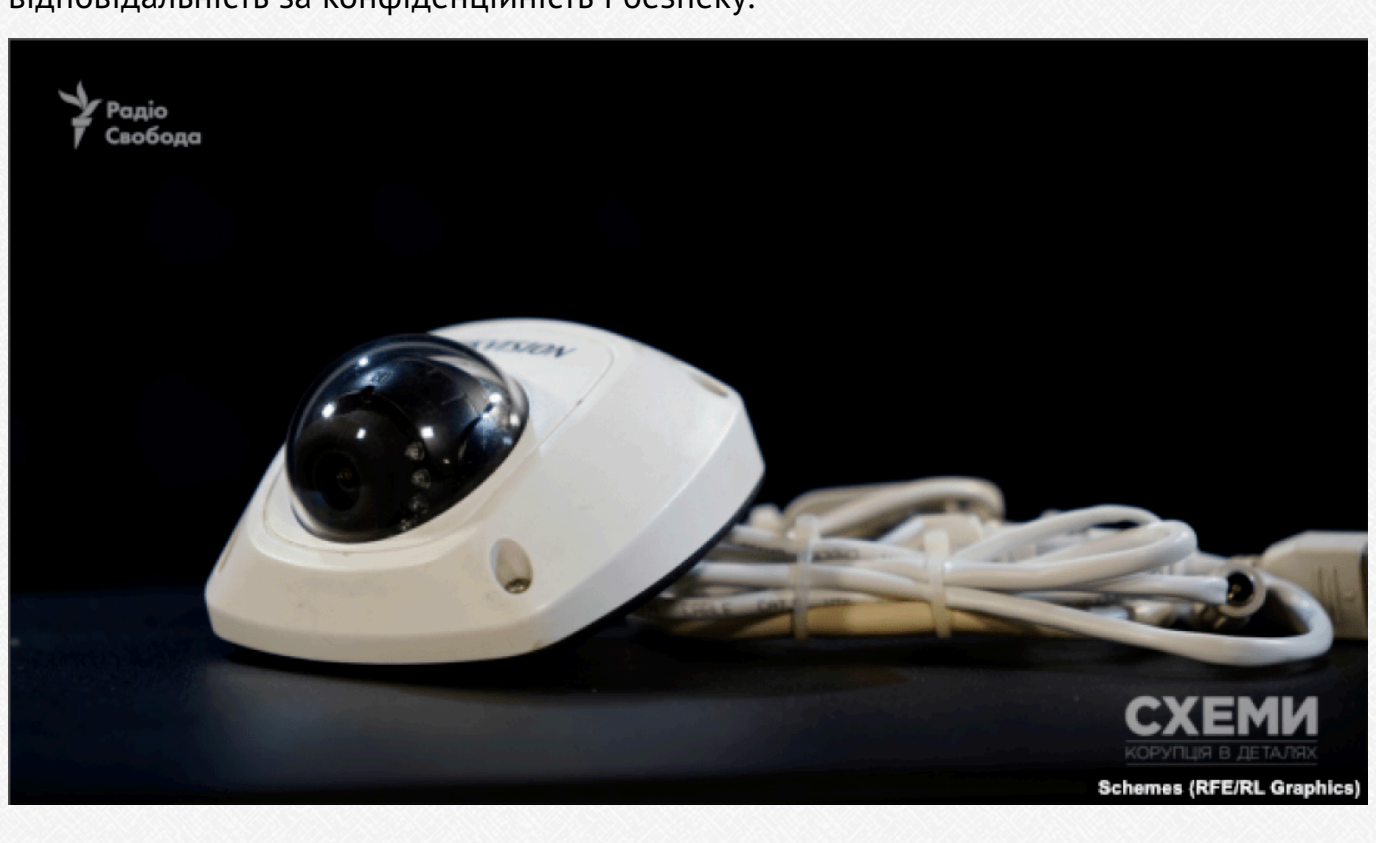

Фото: Радіо Свобода

А от коли камери підключили до телефону через інтернет, то фахівці відразу побачили, що автоматично розпочалася передача зашифрованої інформації, а саме пішли реєстраційні дані, а також логін і пароль користувача на сервери, які контролює Dahua. Примітно, що коли пристрій відключили від мережі, він усе одно продовжив спроби передати дані.

"У такому разі інформація йде на сервери, як ми бачимо, у Німеччині. Також через сервери йде й відеопотік", — коментує виконавчий директор "Лабораторії комп'ютерної криміналістики" Сергій Денисенко.

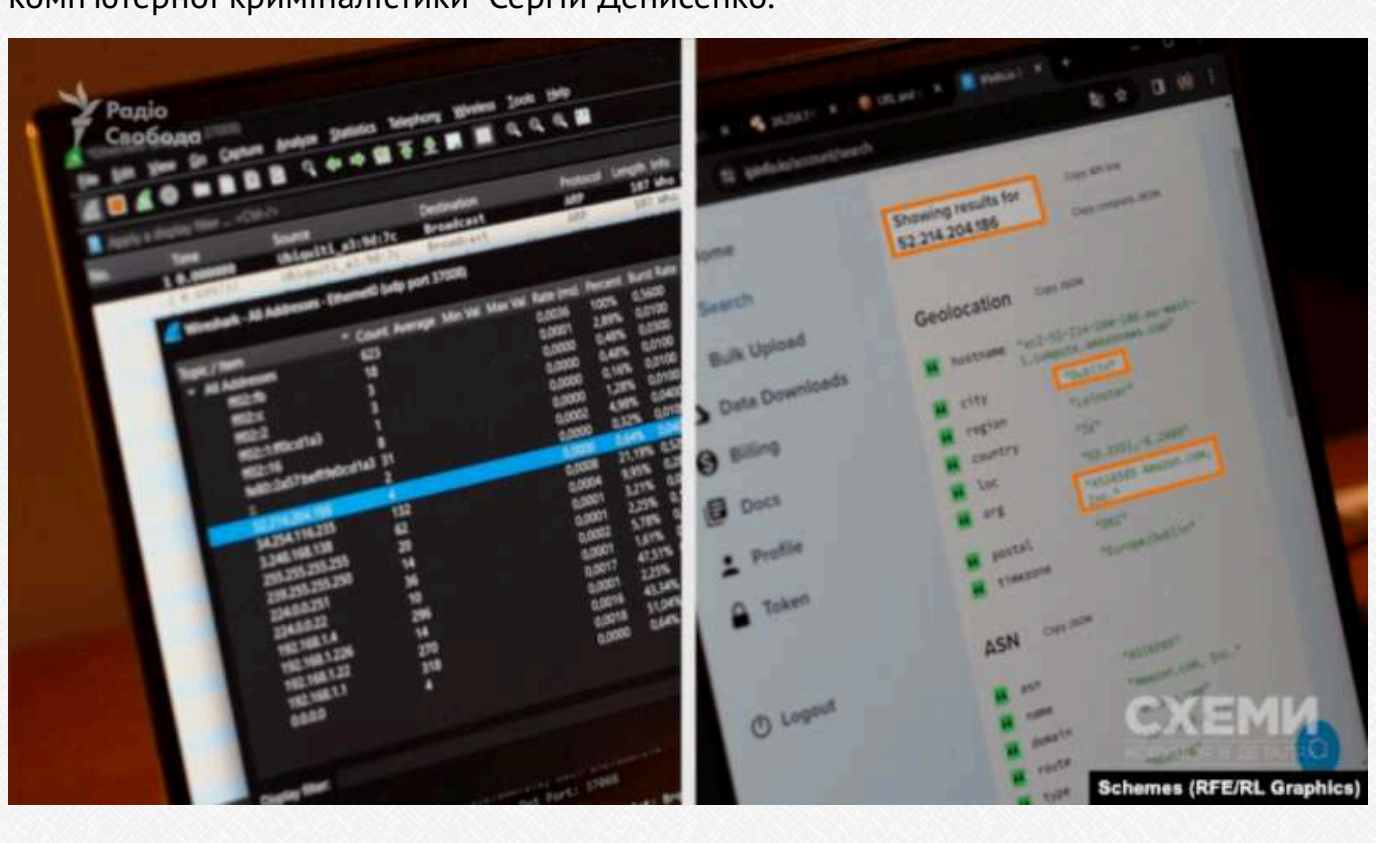

Фото: Радіо Свобода

Камера, вироблена у вересні 2023 року, як стверджують фахівці, захищеніша. Наприклад, не дає змоги встановити простий пароль, що складніше для зламу. Під час експерименту під час приєднання до мережі камера не передавала відразу дані про пристрій або користувача чи інші реєстраційні дані. Але коли користувач підключається до хмарного сховища за допомогою інтернету, відеопотік усе одно потрапляє на сервери виробника.

Фото: Радіо Свобода

За даними IT-фахівців, частина зашифрованої інформації з камери йде на сервер Chinanet у Китаї, а це сервери державної китайської компанії China Telecom, яка є одним з лідерів на ринку надання інтернет-послуг у Китаї.

"Наші фахівці переконані, що в разі використання такого сервісу доступ до камер за необхідності можуть із легкістю отримувати представники виробника. Враховуючи відносини Китаю та Росії зараз, це може нести певні безпекові ризики", — підкреслює Сергій Денисенко.

"Безпечне місто"

Отже, у тому, що виробник програмного забезпечення все ще зберігає можливість доступу до будь-якого пристрою, підключеного до мережі інтернет, і є головний ризик, кажуть у "Лабораторії комп'ютерної криміналістики". Ключовий запобіжник — користуватися пристроями без інтернету, в ізольованій локальній мережі, але здебільшого це доступно приватному бізнесу чи державним структурам, а не побутовим користувачам.

Сама така мережа, як стверджують у Міністерстві внутрішніх справ, налаштована в системі "Безпечне місто". Тобто в основі "Безпечного міста" камери та софт Hikvision і Dahua, але закрита мережа начебто убезпечує від відправки інформації з пристроїв до серверів виробника.

"У системах відеоспостереження, подібних до системи "Безпечне місто", адміністраторами та власниками яких є органи місцевої влади, працює близько 24 тисяч камер Dahua та Hikvision. Саме до такої кількості камер мають доступ центральні органи виконавчої влади системи МВС. Це складає 74% всіх камер такої категорії", — повідомили в міністерстві у відповідь на запит журналістів.

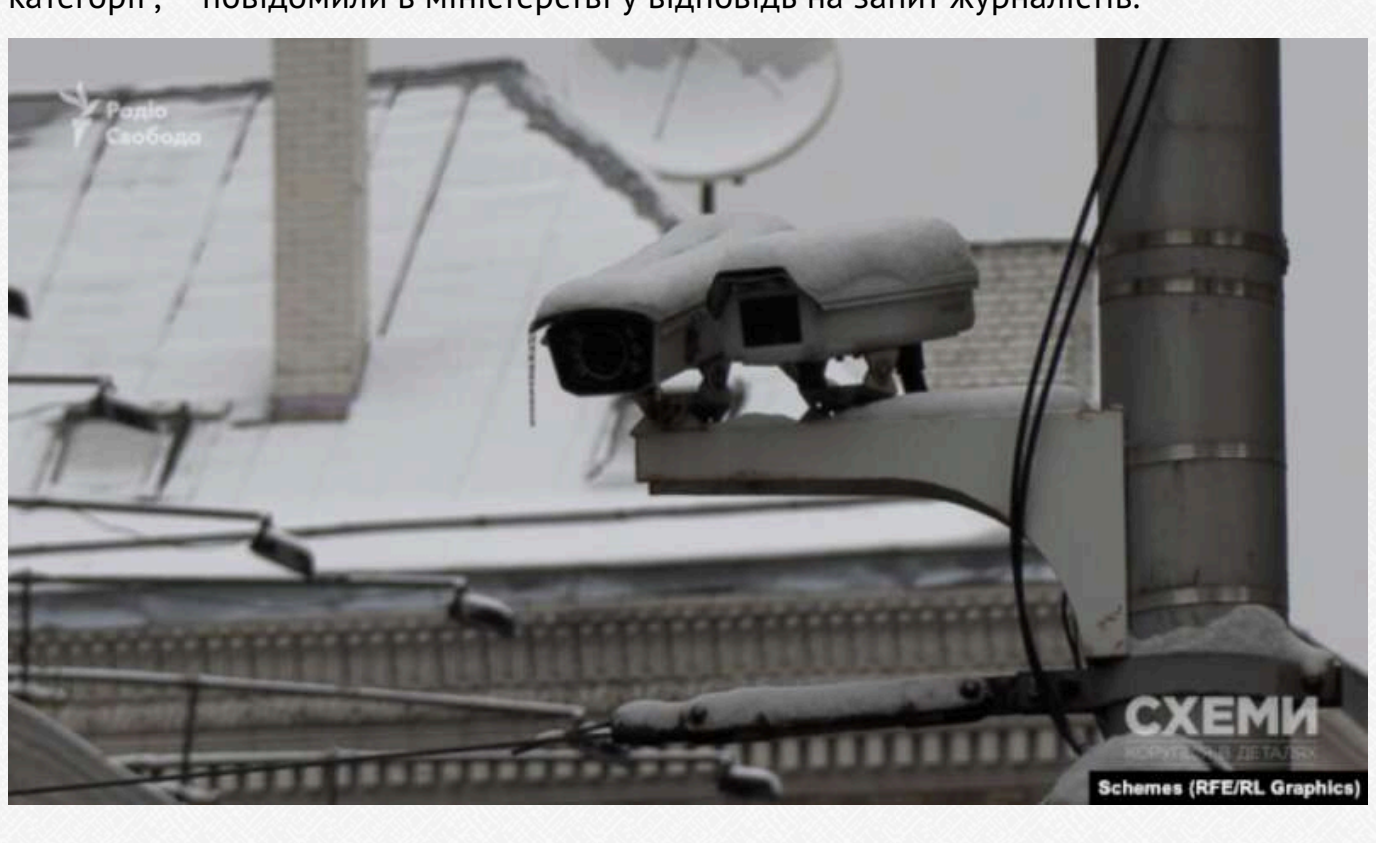

Фото: Радіо Свобода

Проте фахівці з кібербезпеки на прохання "Схем" перевірили пристрої на вразливість перед хакерськими атаками. Спеціалісту, який змоделював процес "зламу" однієї з камер Hikvision, на це знадобилося близько 15 хвилин.

"За допомогою спеціального програмного забезпечення ми бачимо, що хакер може оперативно отримувати доступ до камер відеоспостереження. Якщо в камери неналежне налаштування безпеки (наприклад, відсутність складних паролів, відкрите з'єднання з інтернетом, незахищені роутери), то зловмисник може як стежити за тим, що фіксує камера, так і зберігати цю інформацію для подальших дій", — пояснює дії IT-фахівця Сергій Денисенко.

Так, кажуть фахівці, і сталося 2 січня 2024 року, в день масованої російської атаки по українських містах. Тоді в СБУ повідомили, що виявили камери в столиці, встановлені на приватних будинках, які транслювали роботу української ППО та локації критичної інфраструктури. Це камери зовнішнього спостереження, які, за даними силовиків, зламали російські спецслужби. Загалом за час повномасштабного вторгнення, за даними СБУ, їм вдалося заблокувати понад 10 тисяч камер відеоспостереження, які російські спецслужби могли використовувати для шпигування.

На Заході й у США китайські камери майже заборонені

У 2021 році Федеральна комісія зі зв'язку США (FCC) — регулятор у галузі телекомунікацій — визначила п'ять китайських компаній, що загрожують національній безпеці США. Hikvision і Dahua — у цьому списку.

Двома роками раніше, у 2019-му, адміністрація тодішнього президента США Дональда Трампа внесла компанію Hikvision у санкційний список, і згодом у країні заборонили встановлення продукції цієї компанії на державних об'єктах. До схожих обмежень пізніше також вдалися в інших країнах.

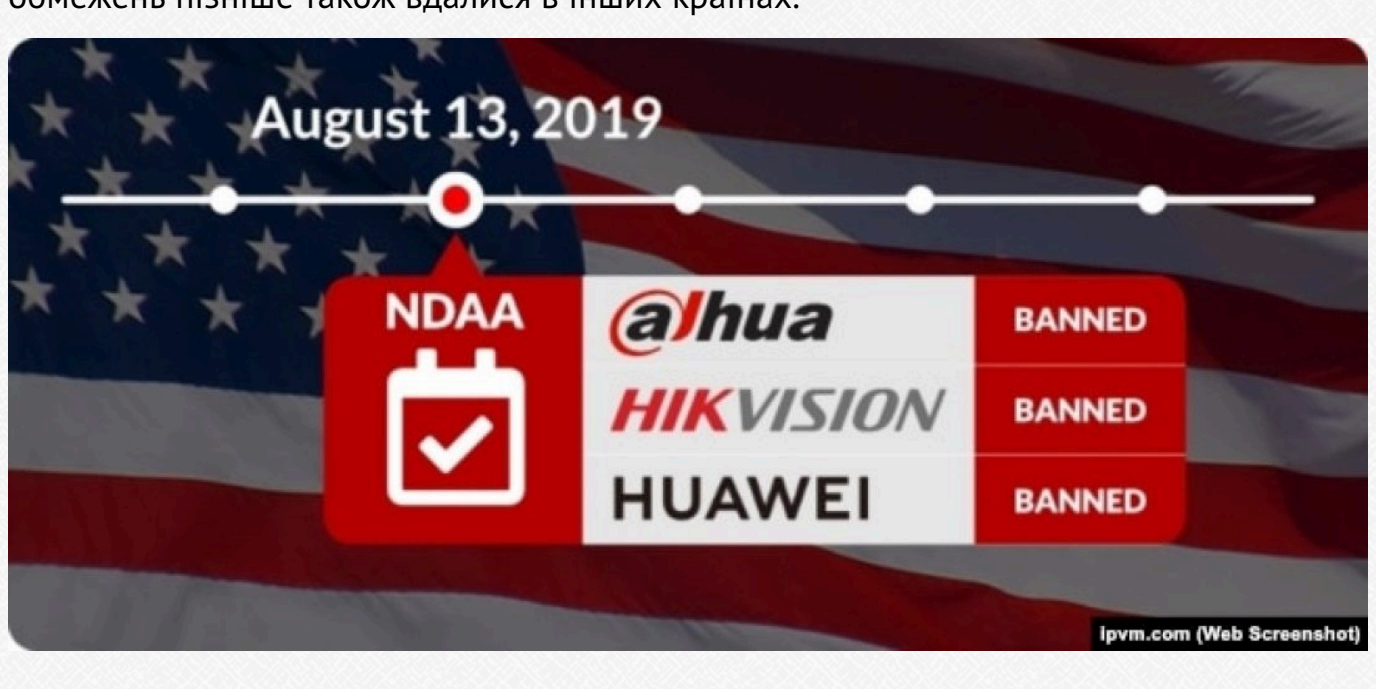

Фото: Радіо Свобода

"Єдина інша відома мені країна, яка повністю заборонила їх використання для державних потреб, — Тайвань. Існують різні приклади в Британії та Австралії, де камери Dahua або Hikvision були вилучені з обігу з міркувань безпеки. Деякі регіональні органи влади у Великій Британії заборонили їх, а сама країна заборонила їх на "чутливих об'єктах", що перебувають під управлінням уряду, але вони ще не запровадили повну державну заборону", — розповідає Коннор Гілі, директор американської організації Internet Protocol Video Market (скорочено IPVM).

Національний інститут стандартів і технологій США регулярно повідомляє про нові знайдені вразливості, які дають можливість отримати доступ до пристроїв, зокрема, у виробах Hikvision і Dahua. Останній такий звіт датується груднем 2023 року. Одна з головних причин такої пильної уваги — це те, що влада Китаю відповідно до їхнього чинного законодавства зобов'язала компанії надавати державі всю інформацію, яку вона вважає необхідною для контррозвідувальної діяльності.

"Нинішнє законодавство Китаю, особливо те, що було оновлене у 2023 році, зобов'язує абсолютно всіх громадян країни, збирати розвіддані та передавати їх державі. Ми бачили, що там було посилено так званий закон про контршпигунство, згідно з яким уся китайська нація має бути мобілізована для служіння інтересам національної безпеки Китаю. І щодо технологічних компаній передусім — вони якраз ті центральні організації, які передають відомості", — розповідає Артур Харитонов, керівник ГО "Ліберально-демократична ліга України", що стежить за політикою Китаю.

Хто такі Hikvision і Dahua

Як засвідчує аналіз структури цих фірм, стверджує Харитонов, держава в обох компаніях є співвласницею. Найбільша частка в Hikvision (майже 37%), за даними Bloomberg станом на 2023 рік, належить CET Hik Group, якою, зі свого боку, на 100% володіє державна China Electronic Technology Corporation Group (CETC). Ця державна компанія відома тим, що займається розробками в оборонній промисловості Китаю, а саме розробкою радарів, систем РЕБ і БПЛА.

Схожа ситуація і з компанією Dahua, де значну частку (майже 9%) має державна China Mobile, хоча найбільшим співвласником та директором компанії є китайський мільярдер Фу Лікуань. Ба більше, у 2022 році в США обидві компанії Dahua та Hikvision, а також їхніх державних співвласників China Mobile та CETC визнали китайськими військовими компаніями.

Китай і Росія — наскільки великий ризик зливу інформації

Українські та зарубіжні ЗМІ неодноразово писали, що існує ризик передачі до РФ інформації з китайських пристроїв, якими масово користуються як в Україні, так і в інших країнах.

"Безумовно, вони обмінюються відомостями, ми це розуміємо. Тому що існує величезна система російсько-китайських угод в сфері безпеки. Вони підписуються декілька разів за рік щонайменше. Останні, наймасштабніші угоди були підписані під час візиту Сі Цзіньпіна до Москви, у жовтні 2023-го вже Путін був у Пекіні, де теж укладалися угоди про певні зобов'язання з обох сторін. Але наразі Китай розуміє ризики відкритої співпраці з РФ і, як ми бачимо, частково приховує свої дії, щоб це не заважало їхній "експансійній кампанії" з просування своєї продукції на світовому ринку", — підкреслює Артур Харитонов.

Хоча Китай декларує начебто нейтральність щодо російсько-української війни, але про співпрацю двох країн у військовій сфері свідчать як спільні військові навчання та заяви про "поглиблення співпраці", так і регулярні візити секретаря Ради національної безпеки РФ Миколи Патрушева до Китаю

Китай був і залишається найбільшим постачальником підсанкційної електроніки до Росії. Ця продукція згодом потрапляє в російську військову техніку, рації та ракети. До речі, за даними пекінської редакції Reuters, у 2023 році загальна сума імпорту-експорту між РФ і Китаєм становила рекордні 240 мільярдів доларів — це майже на чверть більше, ніж роком раніше.

Американська розвідка у своєму звіті за 2023 рік прямо повідомляє про те, що Пекін застосовує різноманітні механізми економічної підтримки Росії. Тож враховуючи таке співробітництво, особливо у військовій сфері, безумовно, Китай здатен, вважає Харитонов, використовувати свої технології та пристрої для передачі українських даних до РФ.

"Також для цього існує договірне підґрунтя — встановлення "військового побратимства" між КНР і РФ та відповідна інфраструктура — присутність представництва Міністерства державної безпеки Китаю в Москві", — наголошує представник "Ліберально-демократичної ліги України".

Як убезпечитися поширення китайської продукції

Насамперед це визначення дистриб'юторів продукції Hikvision і Dahua. Для першої вважаються три компанії — "Віатек", "НПО Інфотех" і "Світ камер". Усі три компанії пов'язані між собою через власників. Ще у 2018 році видання "Наші гроші" опублікувало розслідування про те, як українські постачальники допомагають "вибудувати штучну монополію" на вуличне відеоспостереження Києва під конкретного виробника через державні закупівлі. Серед них і згадуються перших два дистриб'ютори. У 2023 році компанія "Світ камер" уже потрапила в перелік фірм, які Бюро економічної безпеки вважає причетними до розкрадання бюджетних коштів пiжд час побудови системи відеоспостереження в Києві. Слідство в цій справі триває. У компанії ці обвинувачення не коментували.

Ще одна фірма "Інженірінг-Аналітика" здебільшого просуває китайську продукцію в Україні для великих державних замовників. Наприклад, ця компанія облаштовувала й обслуговує великі державні системи відеоспостереження в Києві, Одесі, Львові, Черкасах, Рівному, Луцьку, Кропивницькому, Дніпрі й інших містах України, а також співпрацює з різними підрозділами, що підпорядковуються Міністерству внутрішніх справ — від поліції до прикордонних служб.

Найбільшим дистриб'ютором камер від компанії Dahua до України є компанія "Торговий дім систем відеонагляду", яка, згідно з даними даними Importgenius, із 2016-го до 2023 року поставила понад 1 мільйон пристроїв відеоспостереження. Ця компанія також пов'язана зі згаданими фірмами "Віатек" і "Світ камер" через керівництво та власників, але у квітні 2023 року фірма припинила свою діяльність.

У Міністерстві внутрішніх справ журналістів "Радіо Свобода" запевнили, що "після потрапляння зазначених компаній до переліку "міжнародних спонсорів війни" МВС не рекомендує та не погоджує відповідні закупівлі". І заявляють, що вже працюють над тим, щоб замінити пристрої.

"Із метою централізації всіх наявних систем відеоспостереження МВС розроблено відповідний проєкт закону України "Про єдину систему відеомоніторингу стану публічної безпеки", який наразі вже перебуває у Верховній Раді України. Передбачається, що така система буде побудована на програмному забезпеченні, придбаному для МВС у 2021 році в межах проєкту "Безпечна країна". Виробником програмного рішення є Україна й Ізраїль", — підкреслює МВС.

Зокрема, в Україні при Держспецзв'язку є структура, яка називається Computer Emergency Response Team of Ukraine, або Команда реагування на комп'ютерні надзвичайні події України. Як пишуть журналісти "Схем", вони публічно пишуть на офіційному сайті про технічні вразливості, які знаходять у різноманітних пристроях іноземних компаній, наприклад, таких як Cisco, Microsoft, Apple та інших. Але жодних згадок про Hikvision або Dahua. "Схеми" звернулися до відомства із запитанням, чи проводили такі перевірки щодо пристроїв цих двох китайських виробників.

Також журналісти направили запити безпосередньо до компаній Hikvision і Dahua із запитаннями щодо безпеки для користувачів, які мають такі пристрої, а також щодо співпраці з Росією. Редакція чекає на відповідь.

Окремо журналісти звернулися із запитами до Офісу президента, Кабміну, СБУ й РНБО із запитаннями: якою є державна візія стосовно обігу в країні сотень тисяч китайських камер, інформація з яких може потрапляти до влади КНР, а від неї, що не виключено, до Росії? Чи існує план щодо поступової відмови та вилучення китайської технології з України? Редакція теж чекає на відповідь.

А поки що для простого споживача, який має таку камеру в себе вдома, фахівці з кібербезпеки радять щонайменше змінити заводські налаштування безпеки, використовувати складні та додаткові паролі. І нагадують про те, що китайський виробник залишає за собою прямий доступ до інформації з пристроїв — щойно камера підключається до інтернету.

Теги: СБУ | Dahua | Hikvision | ЗСУ | ВСУ | ПВО | ППО | Напад Росії на Україну | Война | Війна | Росія | Россия | КНР | Україна | Украина | Відеокамери | Видеонаблюдение | Китай

Аліна Кравченко
ЖУРНАЛІСТ, ОГЛЯДАЧ

26 січня 2024 г., 00:35 | Переглядів: 2618 | Коментарі: 0

Роздрукувати | Надіслати товаришу

Коментарі:

comments powered by Disqus