Десятиліття в індустрії систем безпеки та підсумки 2023 року

Інновації чи стабільність, зростання чи падіння, відкриття нових ринків чи втрата існуючих, нові зірки чи нові аутсайдери. 2023 рік завершує десятиліття найдинамічніших змін ринку систем безпеки за всю історію їх існування. Якими були ці десять років та чим відзначився 2023 рік для виробників систем відеоспостереження та контролю доступу у світі та в Україні?

Світовий ринок 2023, на якій більше не впливає коронавірус, але суттєво впливає цифрова автократія

Характерною особливістю 2023 року світової індустрії систем безпеки є те, що це перший рік після епідемії коронавірусу, який продемонстрував стабілізацію, оновлення та зростання ринку. Через відновлення ринку авіаційних перевезень логістичні процеси покращилися, що забезпечило швидший цикл реалізації проєктів.

Як базу для порівняння статистичні агенції беруть 2019 рік, тому що десять років поспіль до 2019 року індустрія систем безпеки активно розвивалася, а найшвидше зростання демонстрували системи відеоспостереження, контролю доступу та охоронної сигналізації.

Згідно звіту Video Surveillance Market компанії Markets and Markets світовий ринок систем відеоспостереження у 2018 році становив $36.89 млрд і мав досягнути $68.34 млрд у 2023 році при середньорічному темпі зростання (CAGR) у 13.1%. Markets and Markets оцінює ринок систем безпеки 2023 року у $53.7 млрд, MarkNtel Advisors — у $50.5 млрд, а Allied Market Research — у $61.8 млрд, що відображає суттєвий вплив пандемії на ринок та сповільнення середньорічного темпу зростання з 13.1% до 9%.

Найбільшим у світі ринком збуту для систем безпеки були і залишаються США (North America), другим – ринок Азійсько-Тихоокеанського регіону (APAC), третім — ринок Європи, Близького сходу та Африки (EMEA). Ринок Латинської Америки (LATAM) вважається зростаючим. Звіти статистичних агенцій показували, що обладнання систем відеоспостереження становило до 60% всього ринку, а програмне забезпечення та сервіси разом займали біля 40%.

На падіння світового ринку систем безпеки (і IT-ринку в цілому) у 2020–2022 роках впливала не лише пандемія коронавірусу, але й криза постачання електронних компонентів та комплектуючих. Як та чому це сталося?

Комерційна демократія vs комуністична автократія/авторитаризм

На ринку аналогових систем відеоспостереження у 90-х роках XX сторіччя домінували європейські (Bosch), американські (Pelco, Flir), японські (Sony, Panasonic) та південнокорейські (Samsung) компанії. В 1996 році шведська компанія Axis Communications випустила першу мережеву камеру, чим створила зовсім новий ринок мережевого, чи як ми зараз кажемо, IP-відеоспостереження. Це був фактично цифровий ринок, на який досить швидко вийшли як відомі гравці аналогового ринку (Bosch, Pelco, Panasonic, Samsung Techwin), так і нові європейські (Mobotix) та американські (Avigilon) компанії.

Тайвань, як найбільший у світі виробник електронних компонентів, швидко зрозумів світову тенденцію і на кінець 2000-х років став потужним гравцем на ринку IP-відеоспостереження, зайнявши нішу бюджетних та середніх IP-камер з такими брендами, як ACTi, GeoVision, Vivotek та інші. Тайванські виробники камер впровадили модель OEM-виробництва, коли певний завод виготовляв камери не лише для власного бренду, але й для інших компаній, які продавали їх під іншими торговими марками.

Китайські компанії були присутні на ринку аналогових камер і компонентів та досить швидко почали виробляти IP-камери для внутрішнього ринку, але їхня якість не витримувала міжнародної конкуренції, і китайські компанії не займали провідних позицій у світі. До того ж Китай захищав свій ринок суттєвими податками та зборами, що унеможливлювало продаж західних брендів камер на його ринку без відкриття власного виробництва/збирання. Тому для збільшення конкурентоспроможності та зниження собівартості IP-камер європейські та американські компанії у 2000-х роках почали створювати/переносити свої виробництва у більш дешеві регіони. Так, наприклад, Bosch Security Systems у 2008-му, а Pelco у 2010-му відкрили свої заводи в Китаї, вирішуючи дві задачі одночасно: здешевлення виробництва і продаж камер на внутрішньому ринку Китаю.

Протягом майже 15 років епохи цифрового відеоспостереження європейські, американські, південнокорейські та тайванські виробники IP-камер були суто комерційними компаніями, працювали за ринковим принципом на демократичних засадах, і жодна держава не виявляла зацікавленості контролювати та розпочинати виробництво камер відеоспостереження. Держави цікавилися космічними програмами, військовою технікою, IT-технологіями, але не відеокамерами, які належали до електроніки побутового чи промислового призначення. Ніхто з комерційних виробників систем IP-відеоспостереження не очікував, що їхнім найбільшим конкурентом стане не інший комерційний виробник, а ціла держава — Китайська Народна Республіка.

Правила гри на світовому ринку відеоспостереження кардинально змінив прихід до влади китайського державного та політичного діяча на ім'я Сі Цзіньпін, який з 2012 року і на поточний час займає посаду генерального секретаря Центрального комітету Комуністичної партії Китаю (КПК). З приходом до влади Сі Цзіньпіна країна, яка для світового ринку довгі роки була експортером текстильних виробів чи, як казали, «фабрикою планети», помітно посилила свої позиції у промисловості, освоєнні космосу та IT-технологіях, зокрема в телекомунікаціях та IP-відеоспостереженні.

Маючи виробництво компонентів, зразки IP-камер європейських і американських виробників та великий внутрішній ринок, КПК побачила нові можливості у 2013–2014 роках, коли світ переживав чергову економічну кризу. Потужні державні інвестиції у китайські державні компанії Hikvision (повна назва Hangzhou Hikvision Digital Technology Co., Ltd.) та Dahua (повна назва Zhejiang Dahua Technology Co., Ltd.) менш ніж за 5 років дозволили їм отримати суттєву долю світового ринку IP-камер. До того ж Китай швидко перебрав лідируючу роль в OEM-виробництві, почавши виробляти камери як для відомих компаній (Bosch, Honeywell), так і численні бренди для певних ринків, а також створивши власні підбренди (наприклад, HiWatch для Hikvision), таким чином збільшуючи свої прибутки.

На тлі глобальної світової економічної кризи 2013 року китайські державні дотації дозволили Hikvision та Dahua, попри гіршу якість порівняно з іншими брендами, знизити роздрібну вартість камер з середнього рівня у $300–$400 до $150–$200. Вони відібрали в тайванських, корейських та японських виробників нішу бюджетних рішень та створили масовий попит замовників на доступні IP-камери, поки ще йшла боротьба між концепціями аналогового та IP-відеоспостереження. Доступність IP-камер впливала на ринок IP-відеоспостереження і відкривала для замовників нові можливості у забезпеченні безпеки різних вертикалей: від промислових підприємств і безпечних міст до приватних будинків. Почалася гонка цін на IP-камери («race to the bottom») та чітка межа між комерційними (західними) та китайськими виробниками.

Сталі державні інвестиції, розвиток державної системи відеоспостереження, великий внутрішній ринок Китаю та накопичений OEM-досвід китайських заводів дозволили Hikvision та Dahua експериментувати. Взірцем для Hikvision був шведський Axis. На ранньому етапі ця китайська компанія не соромилася копіювати моделі та навіть назви технологій. У 2011 році, наприклад, Axis анонсувала технологію Lightfinder, яка дозволяла підвищити якість зображення у складних умовах освітлення, Hikvision у 2014 році представила схожу за принципом технологію з назвою DarkFighter та LightFighter. Щойно Axis випускала нову модель камери, через півроку-рік Hikvision демонструвала схожу ззовні модель, але у специфікаціях вказувала «кращі» характеристики. Таким досвідом Hikvision почала користуватися компанія Dahua, обидві копіювали нові західні моделі IP-камер; надавали замовникам специфікації своїх IP-камер з «кращими» характеристиками, ніж у всіх інших виробників; створювали різні специфікації IP-камер на одні й ті самі моделі під різні ринки збуту. Відомі випадки, коли Hikvision за сприянням інтеграторів на певних ринках постачала IP-камери з унікальними серійними номерами та назвами.

Європейські та американські виробники IP-камер спочатку не

сприйняли серйозно амбіції Китаю і через це втратили суттєву долю ринку IP-відеоспостереження у 2014–2015 роках. Китайська державна стратегія демпінгу спрацювала на 100%, і у 2015 році китайський державний бренд Hikvision обійшов шведський Axis та посів перше місце за кількістю проданих камер.

Згодом комерційні виробники зібралися та почали більше працювати над своїми сильними сторонами, розвиваючи власний досвід у сфері кібербезпеки, що надавало їм помітну перевагу над китайськими державними брендами. Деякі виробники IP-камер, на відміну від виробників комерційної електроніки, зупинили використання навіть дрібних та другорядних електронних компонентів, виготовлених у Китаї. Наприклад, Axis з 2018 року використовує виробничі потужності в Таїланді на додачу до своїх заводів у Швеції та Чехії. А деякі повністю перенесли свої виробничі потужності з Китаю у інші країни Азійсько-Тихоокеанського регіону: наприклад, південнокорейська Hanwha Techwin в 2019 році закрила завод аксесуарів в Китаї та відкрила новий завод повного циклу виробництва у В'єтнамі.

Низка західних виробників у 2018 і 2019 роках показала, зокрема на корпоративному ринку, що вони можуть виграти конкурентну боротьбу, розвиваючи свої бренди, надійність та власні технології, що забезпечувало кращу сукупну вартість володіння для замовників (Total cost of ownership,TCO). Станом на 2019 рік топ-10 лідерів та їхні долі (market share) на світовому та регіональних ринках IP-відеоспостереження виглядали так (**рис. 1**):

Вплив COVID-2019 на світовий ринок 2020–2022

Через низьку вартість виробництва Китай був і є постачальником електронних компонентів для багатьох компаній. Спалах коронавірусу вперше було зафіксовано саме в Китаї (Ухань) наприкінці 2019 року. У відповідь керівництво країни запровадило жорсткий карантин, тривалість якого вплинула на виробничі потужності не лише в Китаї, але й у всьому Азійсько-Тихоокеанському регіоні, який постраждав першим. Через карантин та локдауни по всьому світі експоненційно збільшився попит на електроніку та комп'ютерну техніку, виробництво якої залежить від наявності мікрочіпів, а беззаперечне лідерство у цій галузі належить Тайваню.

Карантини та зменшення виробництва призвели до скорочення кількості працівників у 2020 році, призупинення виробничих потужностей та фактично до блокування ланцюга поставок електронних компонентів, що створило ефект доміно. Замовники систем відеоспостереження та IT-рішень відчули це у 2021 році, коли почали поступово виходити з пандемії та працювати над відкладеними проєктами, але не могли швидко отримати свої замовлення. Строки постачання деякого обладнання сягали 1 року.

В цілому ринок IP-відеоспостереження у 2020–2021 роках відчутно просів, але у 2022-му почав знову зростати через відновлення ланцюгів постачання, і у 2023 році переважна більшість виробників IP-відеоспостереження досягла рівня 2019-го.

США залишаються найбільшим та найбажанішим для усіх виробників ринком у світі. Ринок Азії за темпами зростання випередив ринок Європи (EMEA). В Азійсько-Тихоокеанському регіоні (APAC), де традиційно провідну роль відігравали Об'єднані Арабські Емірати через свою прихильність до топових брендів, почала зростати доля Австралії.

Worldwide 2019 Market Share

	Company	M/S(%)
1	Hikvision	15.0%
2	Axis	10.9%
3	Dahua	7.5%
4	Panasonic	5.3%
5	Hanwha Techwin	4.9%
6	Avigilon	4.1%
7	Bosch	3.5%
8	Johnson Control	2.5%
9	Genetec	2.5%
10	Pelco	2.1%

• North America 2019

	Company	M/S(%)
1	Axis	14.7%
2	Hikvision	7.0%
3	Avigilon	6.4%
4	Hanwha Techwin	5.0%
5	Dahua	4.8%
6	Johnson Controls	4.4%
7	Panasonic	4.2%
8	Genetec	4.2%
9	Intelbras	4.0%
10	Bosch	3.9%

• EMEA 2019

Company	M/S(%)
Hikvision	21.7%
Dahua	12.2%
Axis	10.9%
Bosch	4.3%
Hanwha Techwin	3.6%
Avigilon	3.5%
Uniview	2.8%
Huawei	2.5%
Milestone	2.2%
Pelco	2.2%

• Asia 2019

Company	M/S(%)
Hikvision	21.1%
Panasonic	11.6%
Dahua	7.0%
Hanwha Techwin	6.2%
CP Plus	5.8%
Axis	4.3%
Mitsubishi	3.6%
Uniview	3.0%
Dodwell BMS	2.6%
TOA	2.1%

Рис. 1. Топ-10 брендів ринку IP-відеоспостереження 2019 року у світі та в регіонах

Десятиліття та 2023 рік систем безпеки очима корпорацій

У далекому 2007 році французька компанія Schneider Electric купила американську компанію Pelco, потужного гравця на ринку аналогового відеоспостереження, намагаючись посилити свої позиції у сфері автоматизації будівель. В цілому ж до 2013 року ринок систем безпеки виглядав як велика кількість незалежних комерційних брендів, які успішно конкурували між собою технологіями, інноваціями та орієнтувалися за запити замовників на певних вертикальних ринках (безпечні міста, критична інфраструктура, банки, ритейл, освіта тощо). Так було, поки на ринок не вийшов Китай зі своїми державними брендами, не обвалив ціни і не привчив ринок до шаленої кількості хоч і сирих, але швидких нових продуктів.

Цей виклик першими прийняли японці, які навіть не були гравцями ринку систем безпеки, але мали лідерство у виробництві засобів отримання зображень і оптики, а тому побачили для себе нові стратегічні можливості у сфері IP-відеоспостереження.

У 2014 році японська корпорація Canon Inc. придбала датську компанію Milestone Systems, яка на той час була лідером ринку VMS (Video Management Systems), а на початку 2015 року придбала шведську Axis Communications. Ці кроки викликали певний шок на ринку IP-відеоспостереження, але оскільки обидві компанії залишилися незалежними у складі Canon Group, а замовники і канал збуту не відчули істотних змін, новини про зміну прав власності компаній стали буденністю. До прикладу, сама Axis у 2016 році придбала шведську компанію з відеоаналітики Cognimatics, чеську компанію з виробництва інтеркомів 2N та французького розробника аналітики Citilog (продала у 2021 році). У 2016 році

японська компанія Konica Minolta Inc. анонсувала придбання німецької компанії Mobotix — виробника IP-камер (як казав ринок, камер у стилі Star Wars). У 2018 році Canon Inc. придбала розробника відеоаналітики — ізраїльську компанію BriefCam.

Згодом до інкорпорування ринку IP-відеоспостереження долучилися американці. Motorola Solutions, відомий гравець ринку радіозв'язку, у 2018 році неочікувано придбала канадський Avigilon – відомого виробника IP-камер високої роздільної здатності. У червні 2020 року Motorola придбала шотландську компанію IndigoVision, а у серпні того ж року — Pelco, яка у складі Schneider Electric як гравець IP-відеоспостереження так і не змогла досягти вагомих успіхів. А у 2021 році Motorola придбала ще дві компанії — Openpath та Envysion — з наміром розширити лінійку продуктів і вийти на різні вертикалі та географічні регіони.

Потужні гравці ринку електроніки, південнокорейська компанія Samsung та японська Panasonic, вирішили продати свій бізнес з систем безпеки та сфокусуватися суто на електроніці. Samsung це зробив ще у 2014 році, продавши Samsung Techwin іншій південнокорейській корпорації — Hanwha Group. Таким чином у 2015 році виник південнокорейській бренд Hanwha Techwin, який у 2023-му зробив ребрендинг на Hanwha Vision. Panasonic, маючи відносно невелику частку ринку IP-відеоспостереження, у 2019 році оголосила про відокремлення свого бізнес-підрозділу систем безпеки та продала контрольний пакет акцій компанії Polaris Capital Group, яка намагається запустити бренд i-PRO на базі відділу продажів у Північній Америці та заводу з виробництва IP-камер у Китаї.

Менше ніж за 4 роки японська Canon Group стала власником потужних гравців ринку IP-відеоспостереження: Axis, Milestone та BriefCam, які можна зібрати в єдиному проєкті чи продавати окремо, чим збільшила Share of Wallet (% доля доходу від продажу брендів у проєкти замовників). Всього за 3 роки американська Motorola Solutions стала власником (поки) конкуруючих між собою гравців ринку різного класу: зростаючого Avigilon, відомого на британському ринку IndigoVision та Pelco (не в своїй найкращій формі), а також доповнила своє портфоліо рішенням з контролю доступу. Motorola стала помітним гравцем у сфері безпеки, що, з точки зору власників — також про збільшення Share of Wallet. Найближчими роками, очевидно, слід очікувати комерційної битви між Canon Group та Motorola Solutions за світову, а особливо американську долю ринку IP-відеоспостереження та, ймовірно, контролю доступу.

Жорстка конкуренція на ринку IP-відеоспостереження вимагає відповідних бізнес-рішень. У жовтні 2023 року німецька компанія Bosch оголосила про продаж свого бізнесу у сфері систем безпеки (відеоспостереження, контроль доступу та виявлення вторгнень), щоб сфокусуватися на рішеннях для автоматизації будівель і енергоефективності. При цьому охоронно-пожежні системи залишаться у складі Bosch. Продаж ще не відбувся, а серед потенційних покупців прогнозують Motorola Solutions чи навіть Amazon.

Ще однією новиною грудня 2023 року став факт, що американська компанія Honeywell придбала бізнес з контролю доступу компанії Carrier, зокрема систему контролю доступу LenelS2, готельний контроль доступу Onity та бренд Supra, чим збільшила свій сегмент автоматизації будівель Honeywell Building Automation. Тим самим Carrier — компанія, відома американському ринку — фактично вийшла з бізнесу систем безпеки.

Ринок систем контролю доступу останні десять років був досить стабільним, але він також інкорпорувався. Це демонструє шведська група компаній Assa Abloy, яка з 1994 року купила більше 300 різних компаній в галузі контролю доступу та виробництва замків: зокрема це готельний контроль доступу VingCard у 1994 році, німецький виробник електромеханічних замків Effeff у 1999 році, відомий бренд контролю доступу HID Global у 2000 році, замки Mottura у 2023 році.

Поки комерційні демократичні компанії перерозподіляли Share of Wallet на ринку IP-відеоспостереження, а традиційні гравці ринку систем контролю доступу та охоронної сигналізації були у зоні комерційного комфорту, китайські державні компанії Hikvision та Dahua нормалізували свою присутність на міжнародному ринку, відкрили представництва у різних країнах і зацікавили в співпраці топових західних менеджерів та маркетологів на цільових для себе американському та європейському ринках. З 2017 року спочатку Hikvision, а пізніше і Dahua почали поступово виходити на ринок IP-відедомофонів, інтеркомів, терміналів для розпізнавання облич, біометричних терміналів, систем контролю доступу, турнікетів та охоронної сигналізації. І якщо, у 2013 році китайською стратегією роботи з інтеграторами було «в нас камери, схожі на Axis, але значно дешевші» та «інтегровані системи безпеки — це складно і є ризик виходу всіх систем одночасно, тому краще будувати відеоспостереження окремо», то у 2023 році китайська риторика звучить так: «Ми — інноваційні компанії, які пропонують інтегровані рішення та здатні закрити всі потреби вашого бізнесу». Такі кроки, ймовірно, призведуть ближчими роками до перерозподілу ринку систем контролю доступу та охоронної сигналізації та стануть випробуванням для шведської компанії Assa Abloy, американської Honeywell та інших класичних гравців світового ринку контролю доступу.

Кібервразливості IP-камер, права людини та NDAA

Для IT-фахівців будь яке мережеве обладнання (комп'ютер, принтер, маршрутизатор, сервер тощо) чи IoT-пристрій (мобільний телефон, smart-телевізор, холодильник і т. ін.) є потенційно вразливим. Будьмо відвертими: до певного моменту для більшості виробників, інтеграторів або кінцевих користувачів на ринку систем безпеки не існувало проблеми кібербезпеки. У 2000-х, наприклад, кібербезпека не була проблемою, оскільки багато систем все ще були аналоговими. Лише з 2014 року деякі виробники IP-камер та VMS почали акцентувати увагу замовників на потенційних кіберризиках та рекомендувати конкретні кроки, такі як регулярна зміна паролів на камерах (не залишати паролі за замовчуванням), шифроване підключення між камерами та системою, рекомендації щодо побудови архітектури системи,

захищений від модифікації експорт відеоданих тощо. Але замовники до цих рекомендацій ставилися скептично і не очікували, що їхні системи IP-відеоспостереження, які вони купували для підвищення безпеки власних об'єктів, можуть самі стати небезпечними. Поки це не відбулося в реальності та не вийшло на широкий загал.

У 2016 році сталася кібератака на американського провайдера Dyn, у якій тисячі IP-камер та IP-реєстраторів, інфікованих ботнетом Mirai, були одним із джерел DDoS-атаки, що вразила більше 60 різних сервісів, зокрема Amazon, CNN, BBC, HBO та Starbucks. Розслідування показало, що джерелом атаки були інфіковані IP-камери та IP-реєстратори Dahua, що спричинило ретельну увагу до всіх китайських брендів. Оскільки Hikvision та Dahua дуже повільно реагували на інциденти з кібербезпеки або взагалі відмовлялися визнавати існуючі проблеми, у тому ж 2016 році компанія Genetec (американський виробник VMS) припинила підтримку пристроїв Hikvision і оголосила їх untrustworthy (ненадійними), посилаючись на занепокоєння клієнтів щодо китайського державного контролю цього бренду.

Протягом 2016–2018 років IT-фахівці повідомляли про численні проблеми з кібербезпекою камер, встановлених на вулицях міст, в готелях, банках, госпіталях, тощо. Кібервразливості було виявлено та підтверджено у обох китайських державних виробників — Hikvision та Dahua, а замовники систем відеоспостереження вивчили нові терміни: backdoor, злам IP-камер, buffer overflow vulnerability (вразливість переповнення буфера), cleartext passwords (паролі з відкритим текстом) тощо.

Зростання уваги журналістів до китайських брендів призвело до розслідування, яке з'ясувало, що компанія Hikvision у 2016–2017 роках була головним постачальником технологій відеоспостереження в Китаї, зокрема в Уйгурському регіоні, та співпрацювала з китайським комуністичним урядом, адаптуючи свою продукцію, щоб точно відповідати державній програмі щодо запровадження цілеспрямованого стеження за уйгурами, казахами та іншими тюркськими народами. Рішення Hikvision були встановлені в таборах та тюрмах, школах, мечетях та інших об'єктах в Уйгурському регіоні і зокрема підтримували функції розпізнавання облич. Правозахисники та активісти стверджували, що, окрім постачання технологій спостереження, Hikvision сприяє геноциду, активно керуючи системами та надаючи поліцейським дані, спрямовані проти уйгурів. Hikvision постійно заперечувала будь-які обвинувачення.

Дедалі більша кількість камер Hikvision та Dahua у різних проєктах, зокрема проєктах безпечних міст у багатьох країнах, викликала занепокоєння в державних та приватних замовників і спричинила численні дискусії та кібертестування. Результатом цього процесу став федеральний закон США, який набув чинності 13 серпня 2018 року — National Defense Authorization Act 2019 (NDAA 2019), — який з метою громадської безпеки, безпеки державних об'єктів, об'єктів критичної інфраструктури та інших інтересів національної безпеки США заборонив використання обладнання для відеоспостереження від китайських компаній Hikvision та Dahua, а також телекомунікаційного обладнання від китайських компаній Huawei, Hytera та ZTE (та будь-яких дочірніх чи пов'язаних з ними компаній).

Поступово питання використання китайських державних та комерційних брендів у критичній інфраструктурі та на державних об'єктах демократичних країн стало питанням IT-безпеки, тому що експорт китайських технологій перетворився на найважливіший інструмент Китаю у формуванні нового економічного, фінансового та технологічного порядку за межами країни, а китайські телекомунікаційні технології та мережеві системи IP-відеоспостереження можуть нести загрозу національній безпеці інших країн.

У квітні 2021 року Європейський парламент вилучив тепловізійні камери Hikvision, звинувативши компанію в «сприянні серйозним порушенням прав людини» в Уйгурському регіоні. У липні 2021 року парламентський комітет із закордонних справ Великої Британії закликав уряд заборонити Hikvision продавати продукцію в країні через зв'язок компанії з порушеннями прав людини в Уйгурському регіоні. У червні 2023 року британський кабінет міністрів оголосив, що опублікує графік видалення всіх технологій стеження, створених Hikvision і Dahua, з конфіденційних державних сайтів через занепокоєння, що ці компанії можуть надавати дані службам безпеки Китаю.

Прийняття NDAA дуже сильно вплинуло на ринок США та за 2020–2023 роки суттєво зменшило присутність китайських державних брендів на ринку Північної Америки, а також вплинуло на країни Європи, Японію та Південну Корею. Комерційні виробники IP-камер та рішень IP-відеоспостереження ставлять собі за мету бути у NDAA compliant list (список обладнання, яке відповідає вимогам NDAA), звертаючи увагу інтеграторів та замовників на важливість кібербезпеки у системах IP-відеоспостереження. На тлі гарячих дискусій щодо загроз національній безпеці (свіжий приклад — стаття the Guardian щодо хакерської атаки, яку пов'язують з росією та Китаєм, на атомну станцію Sellafield), висока ймовірність того, що уряд Великої Британії критично поставиться до питання використання китайських брендів у державних проєктах. В свою чергу китайські компанії Hikvision і Dahua запевняють своїх замовників, що вони «сфокусовані на питаннях кібербезпеки та відповідають всім сучасним вимогам», намагаючись обійти обмеження NDAA через продаж своїх OEM-камер під іншими назвами, адже вони за будь яку ціну не хочуть втрачати для себе ринок Північної Америки.

2023 рік очима проєктувальників

Згідно з інформацією від популярного ресурсу JVSG для проєктувальників, топ-10 лідерів брендів IP-камер та їх долі на світовому та регіональних ринках у 2022 та у першому півріччі 2023 року виглядає так: (**рис. 2** та **рис. 3**).

Серед проєктувальників найбільш популярними є китайські державні бренди Hikvision та Dahua, шведський Axis, південнокорейська Hanwha Techwin/Vision, американський Avigilon і німецький Bosch.

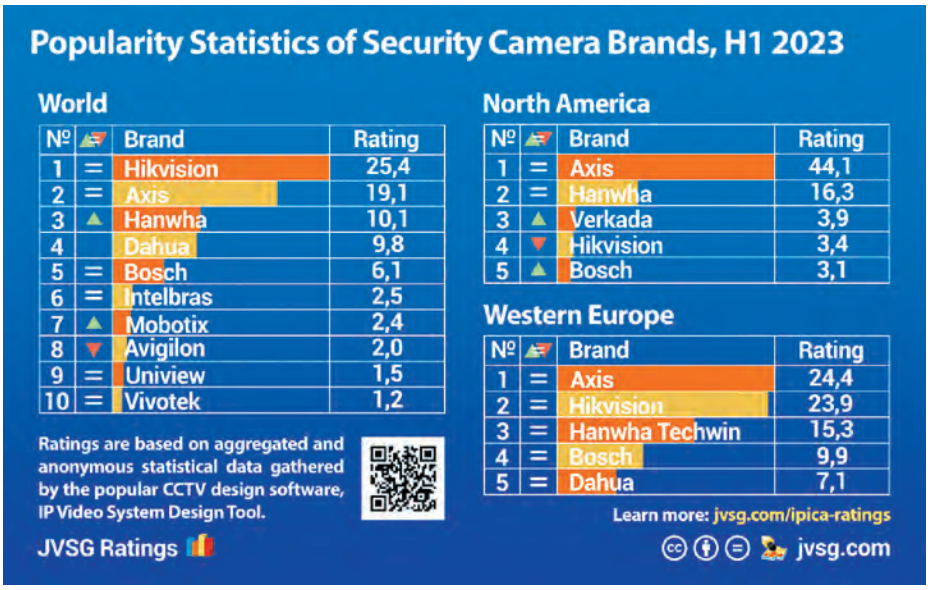

Рис. 2. Топ-10 брендів IP-камер, перше півріччя 2023 року за даними JVSG

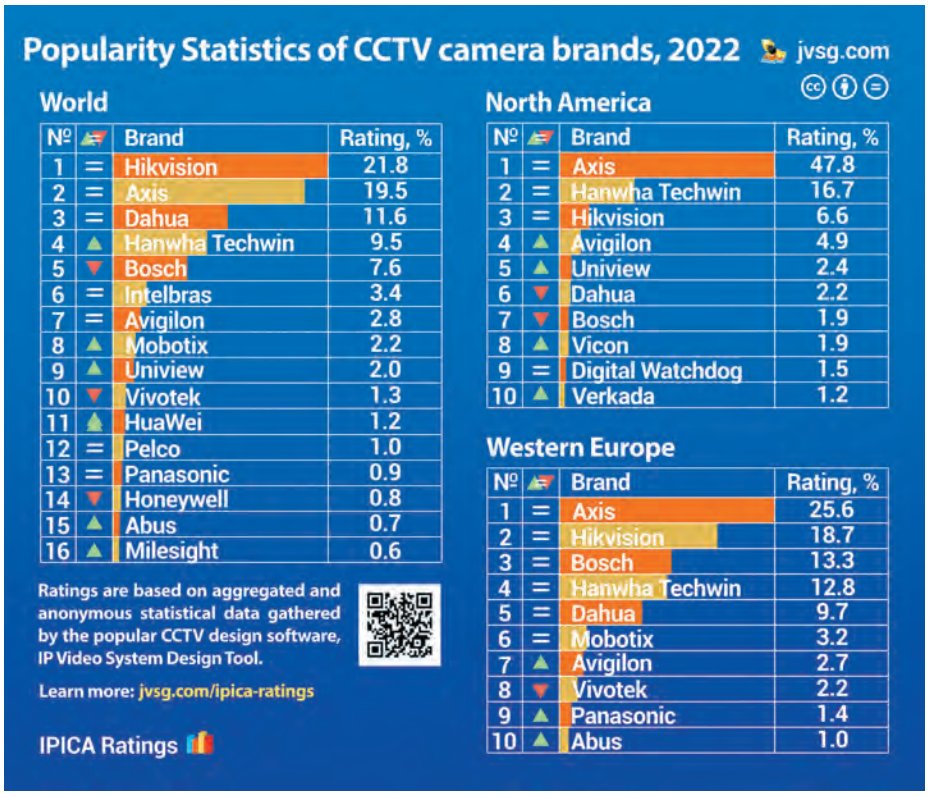

Рис. 3. Топ-10 брендів IP-камер, 2022 рік за даними JVSG

2013–2023 роки з погляду на відеотехнології та технології контролю доступу

У 2013 році стандартною роздільною здатністю IP-камер вважалося 1.3 Мп, а переважна більшість IP-камер не мала вбудованої відео– чи аудіоаналітики. Станом на 2023 рік ми маємо IP-камери з мінімальною роздільною здатністю у 2 Мп, типовою — 4 Мп та бажаною для багатьох замовників роздільною здатністю 4K (8 Мп).

Живлення IP-камер стало стандартизованим через PoE відповідного класу, що дозволило забезпечити передавання відео– та аудіосигналів, живлення та керування камерою через один стандартний мережевий кабель. Лише деякі моделі IP-камер, які працюють за наднизьких (до –50 °C) чи надвисоких температур (до +50 °C) можуть потребувати окремого живлення задля стабілізації температури всередині камери та підтримки працездатності електроніки.

Збільшення роздільної здатності IP-камер створило потребу в оптимізації відеопотоків, які видають камери, і це призвело до виникнення нового кодека — H.265 — та розвитку численних пропрієтарних технологій оптимізації потоків.

Потреба мати чітке зображення у будь-який час доби та пору року призвела до бажання замовників отримувати кольорове зображення в сутінках, що спонукало до розвитку технологій оптимізації широкого динамічного діапазону (WDR) та боротьбу за зменшення шумів IP-камер в умовах поганого освітлення.

У виробників IP-камер з'явилася спочатку мода, а потім і звичка давати назви своїм власним новим технологіям.

Зростання кількості різноманітних проєктів, зокрема безпечних міст, спонукало виробників до пошуку нових типів камер. Це принесло замовникам зміну уявлення про зовнішні камери: замість класичних корпусних, які потребували окремих об'єктивів та великих кожухів, з'явились відносно компактні буллети (навіть виникла нова назва від слова bullet) темних чи світлих кольорів. Замовники отримали мультисенсорні камери, здатні забезпечувати зображення високої роздільної здатності при великих кутах огляду, та сотні моделей для різних проєктів. З'явилися не лише кожухи, а й повноцінні вибухозахищені IP-камери різних типів. Не лише IP-тепловізори охоронного призначення, але й IP-тепловізори, які здатні визначити температуру об'єкта спостереження та навіть температуру тіла людини. IP-камери з нержавіючої сталі, здатні витримувати морські солоні вітри чи пари хімічних рідин. IP-камери з інфрачервоною підсвіткою, яку не бачить людське око (940 нм). Суттєво розвинулися оптичні технології, які дозволили створити нові моделі камер, наприклад, камери типу fisheye («риб'яче око»).

Індустрія контролю доступу доповнилася не лише безконтактними ідентифікаторами, але й можливістю роботи з біометричними характеристиками людини (відбиток пальця, сканування ока, розпізнавання

а)

б)

Рис. 4. Серверна AI-відеоаналітика: детекція сміття (а) та детекція каски (б)

Рис. 5. Камерна AI-відеоаналітика: детекція об'єктів, визначених замовником

обличчя тощо). Детальніше у статті: «СКД на шляху до IoT: від електронних замків до хмарних рішень», «МтБ» №4–5/2023.

У 2023 році ми маємо не лише цифрові IP-інтеркоми чи IP-відеодомофони, а й цілі IP-аудіосистеми, які з часом замінять аналогові системи озвучування.

Але найвпливовішою технологією десятиліття стала відеоаналітика, яка мігрувала від простих математичних правил для обчислення руху в полі зору камери до відеоаналітики на базі штучного інтелекту. Камерна та серверна AI-відеоаналітика дійсно відкрила нові можливості для замовників систем IP-відеоспостереження (детальніше у статті: «AI у відеоспостереженні: очікування та реальність», «МтБ» №3/2023).

Розробники вже не перший рік навчають серверну AI-відеоаналітику розпізнавати різні проблеми, але нарешті у 2022–2023 роках за співвідношенням ціна/якість вона стала спроможною вирішувати реальні завдання замовників: наприклад видати сигнал тривоги, у разі, якщо водій викинув з машини сміття у місті чи коли співробітник на виробництві не вдягнув каску як засіб індивідуального захисту (**рис. 4**).

Абсолютно новим та дуже цікавим нововведенням 2023 року стала пропозиція виробників IP-камер щодо можливості визначати та розпізнавати user-defined objects (об'єкти, визначені замовником), **рис. 5**. Це досягається не лише завдяки навчанню серверної AI-аналітики, але також завдяки вбудованому штучному інтелекту в IP-камерах.

Ринкова ситуація в Україні 2013–2023 та новини 2023 року

До 2013 року Україна не відрізнялась від інших країн СНД: на ринку працювали як іноземні, так і російські бренди. З 2014 року через агресію росії відбулося поступове збільшення ваги західних та китайських брендів та зменшення впливу російських, але, на жаль, останні не зникли (детальніше у статті: «Мімікрія російських VMS та СКД в Україні та світі», «МтБ» №2/2023).

Ринкова ситуація в індустрії безпеки в Україні протягом 2020–2023 залишається стабільно важкою. У 2020 та 2021 роках — вплив пандемії, локдауни та перерозподіл бюджетів на інші потреби. Перша половина 2022-го — майже повна зупинка ринку через повномасштабну війну. Для вирішення оперативних задач навесні 2022 року були закуплені та встановлені всі можливі камери, які залишалися на складах у дистриб'юторів. Відомо, що у перші три місяці війни цілодобово працювали IT-спеціалісти та українські фахівці з відеоаналітики, допомагаючи всім державним службам покращити ситуаційну обізнаність та отримати користь від існуючих систем відеоспостереження та зібраних відеоматеріалів за допомогою відеоаналітики.

Український ринок у другій половині 2022 року відійшов від шоку і поступово замовники розморозили проєкти, але на строки їх реалізації сильно вплинуло ускладнення ланцюгів поставок обладнання в Україну. В той же час багато державних замовників, яким вендори з дружніх країн з початку війни надали у вільне користування на тривалий час ліцензії та апаратне забезпечення, знайшли під кінець 2022 року бюджети та закрили свої критичні потреби з систем безпеки.

2023 рік став дуже неоднорідним. З одного боку, українські фахівці систем безпеки працюють разом з державними та приватними замовниками над вирішенням стратегічних завдань у різних сферах безпеки та оборони України. І це, зокрема, призвело до рішення Національного агентства з питань запобігання корупції від червня 2023 року щодо внесення до переліку міжнародних спонсорів війни компаній Hikvision і Dahua (та ще десятка китайських компаній). З іншого боку, 2023 рік приніс повне розчарування через безвідповідальність частини замовників та тунельне мислення — деякі українські замовники продовжують експлуатацію раніше встановленого російського обладнання (камери, контролери, сервери) та програмного забезпечення VMS і продовжують анонсувати тендери на китайському обладнанні. Боротьба за незалежність України триває і у кіберпросторі, і у сфері систем безпеки. І кожен замовник, незалежно від форми власності, має перевірити свої існуючі системи відеоспостереження, контролю доступу тощо на наявність вразливостей та контроль цілісності критичних даних.

Що виглядає оптимістичним у 2023 році — це остаточне усвідомлення, що українським замовникам потрібні не лише професійні західні демократичні рішення та продукти, але й українські розробки у сфері defense-tech та систем безпеки. Низка українських компаній вже почала свій шлях у цьому напрямку. Побажаємо їм наснаги, успіхів, професіоналізму та чекаємо на результат.

Альона ШВЕЦОВА,
незалежний експерт з систем безпеки, cctvmadonna