Дрони, радари і розумне світло:
нове в системах охорони периметру

Сучасні технології дозволяють помічати порушника задовго до його наближення до огорожі.

Світ не стає спокійнішим, що видно, наприклад, з останніх подій у Білорусі, чиї сусіди взялися відгороджуватися від неї парканами. Тероризм, неконтрольована міграція і протести змушують уряди посилювати охорону державних кордонів і критичної інфраструктури.

Охорона периметру, як і інші напрями безпеки, постійно розвивається і поповнюється новими технологіями. Наприклад, останніми роками набули популярності радари охоронної сигналізації, які ефективно працюють незалежно від рівня освітлення і погодних умов. У сфері відеонагляду, як стверджують фахівці, майбутнє за відеоаналітикою з використанням штучного інтелекту, не зайвими будуть і лампи «розумного освітлення», які полегшують роботу СВН і одночасно самі можуть відлякувати порушників. Актуальним питанням стає боротьба з дронами, у той же час і самі БПЛА допомагають з патрулюванням території.

«СіБ» розбирався, які технологічні тренди проявляються в охороні периметру від загроз і як вони реалізовані у рішеннях, доступних на ринку.

Ринок охорони периметру стабільно зростає

За оцінками компанії ***Markets&Markets***, ринок систем охорони периметру у 2020 році становив $61,3 млрд, і до 2026-го він зросте до $96,5 млрд. Зростання, своєю чергою, викликане стрімким збільшенням кількості проникнень через загорожі, крадіжок, транскордонного тероризму, нелегальної імміграції тощо. Системи охорони периметру все частіше використовуються не лише для захисту кордону, критичної інфраструктури і військових об'єктів, але й на комерційних підприємствах, для захисту житла, торгових площ, транспортних вузлів тощо.

Найбільшу долю ринку утримує сегмент відеонагляду ($13,5 млрд у 2020 році з прогнозом у $23,1 млрд у 2026-му), і зростатиме він теж найшвидше (9,4% щорічно проти 7,9% в середньому по ринку). При цьому, зазначає агенція, традиційні аналогові камери відеонагляду інтенсивно витісняються IP-рішеннями (у тому числі бездротовими). Великі перспективи мають давачі нового покоління, що монтуються на огорожу, інфрачервоні сенсори, інтегровані системи охорони периметру на основі волоконно-оптичного кабелю, що працюють спільно з відеонаглядом. До інших інновацій належать охоронні безпілотники з технологією комп'ютерного зору для повітряного спостереження, функціональність розпізнавання облич і номерів авто, інтеграція між системами охорони периметру і контролю доступу (наприклад, у разі виявлення проникнення на територію двері будівель можуть автоматично блокуватися).

Розвитком технологій і трендом на інтеграцію охоронних систем пояснюється головний чинник, що стримує розвиток ринку, а саме брак кваліфікованих фахівців. Часто компанії винаймають персонал, який не розбирається в тонкощах охоронних систем. Для вирішення цієї проблеми виробники здійснюють тренування спеціалістів на території замовника.

Загалом компанії, які займаються дослідженням ринків, називають відеоаналітику одним з ключових трендів у охороні периметру. Зараз завдяки вбудованій аналітиці камери

10 YEARS OF SERVING EUROPEAN ENTERPRISES

HUAWEI

AirEngine Wi-Fi 6

All-New Speed for Everything

Блискавична швидкість
Постійна мобільність
Безперервна самоорганізована мережа

Перевизначення еталону Wi-Fi для галузі

e.huawei.com/ua

можуть «розуміти», що саме вони бачать, і генерувати сповіщення одразу, щойно помічено загрозу. При цьому вони здатні відрізняти справжні інциденти від фальшивих, спричинених, наприклад, тваринами, снігом, коливанням гілля тощо. Також системи відеонагляду дають можливість швидко знаходити потрібні кадри з архіву і здійснювати їх аналіз, шукати і відстежувати наперед задані об'єкти, зіставляти зафіксовані події з повідомленнями від інших давачів. Теми відеоаналітики і взагалі відеонагляду неодноразово висвітлювались на сторінках нашого журналу, і тому тут їх торкатись не будемо.

З початком пандемії COVID-19 охорона периметру зіткнулася зі своїми труднощами. По-перше, об'єкти, що перебувають під охороною, опустіли через локдауни. Відповідно зросла потреба у віддаленому моніторингу. Окрім того, постала необхідність якогось використання вже існуючої інфраструктури безпеки для інших цілей: наприклад, обрахунку кількості людей, що заходять на ту чи іншу територію, для запобігання скупченням. Набули поширення термальні камери, які не лише виявляють осіб з підвищеною температурою, а й забезпечують можливість спостереження у цілковитій темряві.

Далі торкнемось коротко деяких із згаданих технологій.

Безпілотники-вартові

Останнім часом БПЛА стають усе більш доступними і набувають поширення для охоронних цілей, зокрема і на периметрі. Дрони поєднують функції камер відеонагляду і охоронців. Їх можна налаштувати в режим патрулювання території, або ж дрон може швидко висунутись у потрібне місце і почати трансляцію. Особливо актуальні такі пристрої для об'єктів, що мають велику площу (наприклад, сонячних електростанцій), значну протяжність або віддалене розташування. Також рішення допоможе там, де багато будівель і відповідно сліпих зон.

Окрім камери видимого світла, дрон може мати на борту інфрачервону камеру або навіть радар, що дозволяє йому ефективно працювати у нічний час. Є варіанти рішень, які дозволяють оператору, у разі виявлення порушника, попередити його за допомогою вбудованого прожектора або гучномовця.

Для охорони периметру найчастіше пропонується концепція «дрон-з-коробки», у якій безпілотник постачається з базовою станцією, що відіграє роль своєрідного гаража. Такий літальний апарат здатен автоматично стартувати і сідати, і його можна відправити в потрібний район впродовж півхвилини.

Наприклад, БПЛА Blackbird американської компанії ***Nightingale Security*** мають значний рівень автономності. Дрони самостійно здійснюють патрулювання за визначеними маршрутами, надсилаючи сповіщення у разі виявлення порушників (**рис. 1**). Якщо тривогу піднімають інші детектори, система автоматично відряджає дрон, який передає відео службі охорони. Дрон також можна вислати вручну у разі якоїсь надзвичайної події.

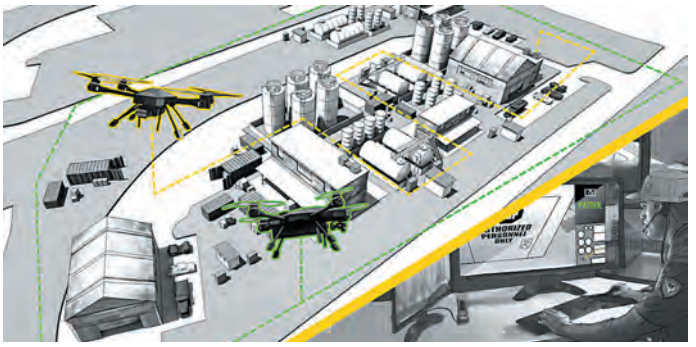

Рис. 1. Маршрут патрулювання на прикладі дрона Nightingale Blackbird

Базова станція слугує одночасно зарядним пристроєм і ретранслятором, а також здійснює координацію і обробку даних з використанням алгоритмів машинного навчання. При цьому архітектурно пристрій розташовується за мережевим екраном організації, що забезпечує захист даних. Також базова станція має нагрівальні і охолоджувальні елементи для підтримання оптимальної температури. Дрони можуть злітати і сідати самостійно, використовуючи вбудовані камери, комп'ютерний зір і інфрачервоні маяки.

Сайт ***ZDNet.com***, який склав рейтинг охоронних безпілотників 2021 року, назвав найкращим БПЛА для віддалених операцій рішення SAMS компанії ***Easy Aero***. Ця система, створена за підтримки американських ВПС спеціально для охорони периметру, складається з квадрокоптера або гексакоптера військового класу, що може триматися в повітрі до 50 хвилин, базової станції у міцному корпусі, яка заряджає дрон і захищає його від погоди, і системи управління. Дрон може нести декілька HD– і термальних камер, сенсори, обладнання зв'язку і лідар[*)]. Базова станція також обладнана чотирма камерами, які забезпечують круговий огляд навколо місця розгортання.

Система SAMS використовувалась, зокрема, на Суперболі — фінальному матчі сезону в американському футболі, а також успішно продається в США, Європі, Ізраїлі, Таїланді, Японії та країнах Центральної Африки.

Ще одним цікавим рішенням є Skeyetech від французької компанії ***Azur Drones***, яке не вимагає жодних навичок пілотування. Зліт і посадка здійснюються автоматично, а персонал лише запускає готові місії або задає курс через систему управління відео (VMS). Також дрон має серед свого ПЗ програму предиктивного обслуговування, яка попереджає про ризик відмови. Завдяки цьому всьому дрон можна підняти в повітря у будь-який момент впродовж 30 секунд.

В базовій конфігурації цей октокоптер має на борту дві камери: HD і високоприцизійну термальну, тобто мінімальний набір для спостереження вдень і вночі. Обидві здатні виявити людину з відстані кількасот метрів. Дрон виробляється у надміцному корпусі, а ключове обладнання (двигуни, електроніка, джерела живлення) мають

[*)] LIDAR (Light Identification Detection and Ranging) – технологія отримання та обробки інформації про віддалені об'єкти за допомогою активних оптичних систем, що використовують явища відбиття світла і його розсіювання в прозорих і напівпрозорих середовищах. Випромінювачами світла в таких системах зазвичай є лазери. Про застосування лідарів для охороні периметру йтиме мова далі.

Smart Camera Box для відеоспостереження

Пристрій «все в одному» від PHOENIX CONTACT

Smart Camera Box надійно з'єднує відеокамери спостереження IP з відеосервером. Цей пристрій об'єднує функціональні можливості розподільних коробок, оснащених стандартними пристроями DIN-рейки, в один компактний пристрій.

За додатковою інформацією, звертайтесь:
ТОВ "Фенікс Контакт"
м.Київ, вул.Краснова, 27
(044) 594 55 22
phoenixcontact.ua

PHOENIX CONTACT
INSPIRING INNOVATIONS

AI 03-19.001.L1
© PHOENIX CONTACT 2019

подвійне або й потрійне резервування. Окрім того, зв'язок між дроном і базовою станцією шифрується, а завдяки інтеграції з VMS відео передається безпосередньо в корпоративну мережу.

Розумні лампи

Освітлення — важлива складова системи захисту периметру, яка забезпечує гарну видимість загорожі, нівелює можливі схованки, покращує роботу камер відеонагляду (дозволяючи розпізнавати обличчя), а також відлякує порушників. Сучасні системи освітлення базуються на LED-лампах, які є достатньо дешевими і забезпечують високий індекс якості відтворення кольору (Color Rendering Index), що дозволяє операторам віддалено ідентифікувати порушників: як для реагування, так і для подальшого розслідування інцидентів.

Останнім часом з'явилася концепція «розумного освітлення» (Intelligent Lighting), яка усуває недоліки традиційних ламп і поєднує функції освітлення території та відлякування порушників. Зокрема, традиційні ліхтарі, які розташовуються на стовпах, просто створюють світове коло, яке засліплює камери, у той же час навколо виникають тіні, де можуть ховатись порушники. Особливо густа тінь утворюється за огорожею із щільної сітки, оптимізованої для запобігання спробам перелазу. Також яскраве світло відбивається від рослин і калюж води, ще більше заважаючи камерам.

Розумні лампи забезпечують рівномірний розподіл світла вздовж огорожі, не створюючи зон глибокої тіні і повної яскравості («світляних бомб»). Завдяки тому, що промені можна спрямувати вниз або вздовж огорожі, також зменшується «світлове забруднення». Промені не поширюються вгору або поперек паркану, завдяки чому він гарно освітлений і при цьому не заважає сусідам.

Іншою можливістю розумного освітлення є відлякування порушників. Тут, навпаки, важливе саме яскраве світло, яке дезорієнтує порушника, а також необхідною вимогою є підтримка регулювання яскравості і миттєвого увімкнення. Наприклад, у нормальному режимі лампи можуть працювати на 30%, а у разі виявлення порушника вмикатися на повну потужність або у режимі стробоскопа. Таким чином сторонні особи сповіщаються, що їх виявлено (а також, імовірно, їх записують камери відеонагляду). Додатково система може увімкнути аудіопопередження або двосторонній канал для переговорів.

Як приклад розумного освітлення можна навести систему LM100 американської компанії ***Senstar***, яка першою запропонувала рішення, що поєднує підсвітку і контроль проникнення (**рис. 2**). Лампи потужністю 2,5 Вт мають вбудований акселерометр для виявлення спроб перерізати чи підняти сітку або перелізти через загорожу. У разі виявлення такої спроби автоматично вмикається посилене або стробуюче світло для відлякування порушника, а також починають працювати камери. Лампи можна встановлювати як на дротове загородження, так і на стіни чи ворота. А завдяки підтримці бездротових стандартів зв'язку, таких як ZigBee, світильники можна поєднувати у самовідновлювану Mesh-мережу, що не лише дозволяє зекономити на проводці, але й забезпечує стійкість до відмов, оскільки вихід з ладу одного пристрою не вплине на стан мережі в цілому. Вбудований інтелект забезпечує

групування світильників, тож вмикатимуться лише окремі зони чи ліхтарі.

Рис. 2. Приклад розумного освітлення з підсвічуванням лінії огорожі і вбудованими давачами проникнення (джерело: Senstar)

Інше рішення, Security Lighting від компанії ***CAST Perimeter***, отримує інформацію про порушників від сторонніх давачів. Його можна налаштувати на різні варіанти реагування: наприклад, перемикання з інфрачервоної підсвітки відеокамери у видиме світло, стробуючі вогні, періодична зміна яскравості. Приміром, лампи можуть упродовж 45 секунд переходити від повної темряви до максимальної яскравості, таким чином не даючи очам зловмисників пристосуватися. Функція FlashGlare працює ще цікавіше: після виявлення порушника лампи починають вмикатися і вимикатися кожні 10 секунд. Спалах у 2200 люменів засліплює людину, вона бачить зірки і плями і через 1–2 секунди рефлекторно заплющує очі. Далі лампи гаснуть, і очі розплющуються знову, намагаючись пристосуватися до зміни освітлення. Щойно після цього знову вмикається світло, і все починається спочатку. За заявою виробника, після 6–10 таких циклів порушник буде настільки дезорієнтований, що забуде про огорожу і інстинктивно втече. Щось бачити він зможе лише через 5–8 хвилин, а для повного відновлення зору знадобиться 20–30 хвилин, при цьому шкоди очам завдано не буде.

Охоронні радари

Ще один клас рішень, які доповнюють систему відеонагляду (або навпаки), — це охоронні радари. На відміну від камер, вони здатні виявляти порушників за будь-якої погоди і незалежно від освітлення, а також не реагують на тіні і відбиття світла, через які відеокамери можуть генерувати хибну тривогу.

Радар робить серію «знімків», створюючи фіксовану картинку території, а потім відстежує зміну положення підозрілих об'єктів і здіймає тривогу, якщо просторова різниця відповідає заданим пороговим критеріям. Радар може відображати дані на карті, а також запускати камери відеонагляду для оцінювання загрози. Окрім того, що подвійна перевірка зменшує кількість хибних тривог, радар також надає камерам пріоритетні цілі для стеження. Це відбувається без участі персоналу, який, таким чином, звільняється від рутинних операцій і може займатися власне реагуванням.

Компанія ***Teledyne FLIR*** стверджує, що їхній радар визначає відстань до об'єкта з точністю до 1%, а у туманний день може помітити людину на 60 секунд раніше, аніж термальна камера. Також радари добре справляються з відстеженням цілей. Якщо у системі відеонагляду для цього може знадобитись переключення між кількома камерами, то радар точно вказує, яку саме камеру треба націлювати. Якщо камера втратить ціль через фізичну перешкоду, погане освітлення або туман, радар продовжуватиме відстеження і передасть координати порушника наступній камері.

Радарні системи гарно підходять, наприклад, для електричних підстанцій, які можуть не мати власної постійної охорони, аеропортів, виправних установ і дата-центрів, тобто об'єктів, які мають великий периметр і/або розташовуються у віддалених місцях. Радар помітить зловмисника на великій відстані і попередить охоронний персонал, який зможе вчасно дістатися місця події.

Радари, втім, мають і свої недоліки. Зокрема, вони чутливі до відбиття сигналу від металевих об'єктів, таких як будинки, автомашини і дротяні огорожі. Дерева і кущі поглинають сигнал, зменшуючи дальність і точність дії радара. Тому радар загалом розташовують таким чином, щоб ніщо не заважало йому бачити місцевість. Ще одним обмежуючим чинником може бути нерівність рельєфу. У цьому разі радар, встановлений надто високо, може не бачити територію безпосередньо біля землі, тоді як розміщення його під кутом спричинить завади через відбиття від землі. Тут виходом може бути використання ешелонованої системи, де пристрої розташовуються на різній висоті або під різними кутами. Нарешті, на роботу радарів також впливає електронний шум, будь то природного чи штучного походження.

Радарні системи ізраїльської компанії ***Magos*** (дистриб'ютор в Україні — ***«Ромсат»***) забезпечують, залежно від моделі, виявлення людини-порушника на відстані від 150 до 800 м, а людини або човна — на відстані від 150 до 1000 м з точністю до 1 м. Також радар бачить цілі, що рухаються зі швидкістю 0,3–30 м/с. Обладнання накриває площу від 50 тис. до 810 тис. м^2. Приклад такої радарної системи представлений на **рис. 3.**

Окрім того, Magos пропонує програмне забезпечення MASS+AI, яке здійснює управління радарами і відображає всі помічені цілі на мапі. Також програма автоматично скеровує камери відеонагляду для верифікації загроз, а алгоритми на основі нейромережі забезпечують класифікацію цілей, відрізняючи, наприклад, людей від тварин. «Дружні» цілі, такі як патрульні та охоронці, що користуються застосунком Magos, також ідентифікуються і не генерують сигналів тривоги. Пакет MASS+AI може, серед іншого, працювати на апаратних пристроях (які також пропонує Magos), що здатні обробляти по 10 відеопотоків кожен і можуть об'єднуватись за допомогою сервера.

У згаданої вище компанії FLIR радар Elara R-190 може «бачити» автівки на відстані до 300 м і людей на відстані до 125 м з точністю до 1 м, а також одночасно відстежувати

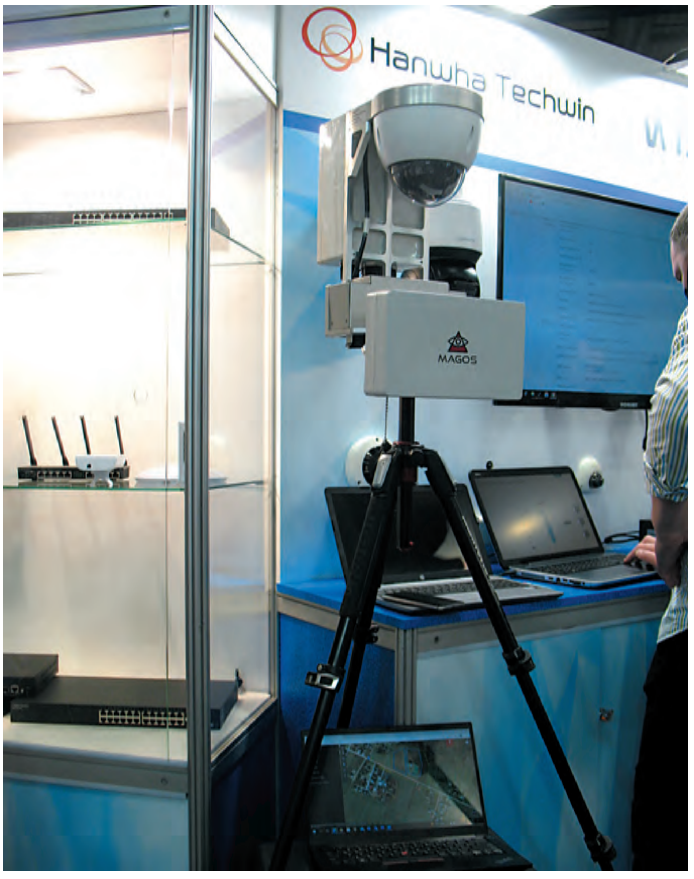

Рис. 3. Один з радарів Magos, представлений на виставці Expert Security влітку 2021 року

до 32 цілей. Взагалі ж FLIR більше відома своїми камерами інфрачервоного і видимого діапазону.

Є радар і в асортименті ***Axis Communications*** (дистриб'ютори в Україні — ***IQ Trading*** та ***ELKO Ukraine***). Пристрій D2110-VE використовує методи машинного і глибокого навчання для виявлення і класифікації цілей, він здатен помічати людей на відстані до 60 м, транспортні засоби — до 85 м. Встановивши два радари «спина до спини», можна забезпечити круговий огляд території площею до 22 км^2. Вбудоване ПЗ з цифровим підписом убезпечує пристрій від зламу; обладнання також розпізнає удари і спроби відкрити корпус, негайно повідомляючи оператора. Радар має аудіовихід і може з'єднуватись з рупорним гучномовцем. Нарешті, пристрій інтегрується з системами управління відео сторонніх розробників.

Радари-антидрони

Безпілотні літальні апарати не лише використовуються у охороні периметру, але можуть і самі бути порушниками. Дрони становлять небезпеку для аеропортів, об'єктів критичної інфраструктури, військових баз і ще багато чого. Кінокомпанії відганяють БПЛА від знімальних майданчиків, а розслідувачі за допомогою дронів оглядають маєтки можновладців.

Існує окремий клас обладнання на основі радарів, розроблених для виявлення дронів. Одне з таких рішень, зокрема, пропонує нідерландська компанія ***Robin Radar Systems***. Створена нею система ELVIRA (**рис. 4**) діє за принципом безперервної хвилі з частотною модуляцією (FMCW)[*)]. На відміну від звичайних радарів, які сканують простір за допомогою імпульсів і виявляють цілі за відлунням, FMCW-радар працює в безперервному режимі, що забезпечує точне відстеження і швидке оновлення даних. Окрім того, радар є мікро-доплерівським і здатен помічати не лише рух, а й зміни у русі, завдяки чому він може виявляти рух пропелерів, підтверджуючи механічне походження об'єкта, і відрізняти дрони від птахів. Інша розробка під назвою IRIS визначає положення дронів також за висотою, маючи кут нахилу 60°. Радари спроможні відстежувати як окремі БПЛА, так і цілі рої з сотень дронів.

Усі виявлені об'єкти позначаються на супутниковій мапі: червоним та оранжевим кольорами — підтверджені та здогадні дрони і їх маршрути, зеленим — птахи. Власник може налаштувати зони, які треба контролювати, а які ігнорувати. Також радар можна обладнати відеокамерою для візуального підтвердження.

Рис. 4. Протидроновий радар ELVIRA

Компанія ***AntiDrone***, як видно з назви, спеціалізується на системах для протидії БПЛА. Зокрема, їхнє рішення Harrier, яке базується на власній технології, здатне одночасно виявляти малі і великі дрони, човни, літаки і кораблі. Наприклад, радар помічає мікро-БПЛА (класу Phantom) на відстані 4–6 км, а середнього розміру (класу Raven) — за 7–11 км.

Взагалі ж виробників протидронових радарів досить багато.

Інший принцип пошуку дронів базується на моніторингу радіочастот. Так працює, наприклад, система Aartos DDS німецької компанії ***Aaronia AG***, яка відстежує неперервний спектр (100 МГц–6 ГГц) і може засікати канали, що використовуються безпілотниками, а також ідентифікувати виявлені БПЛА. При цьому дрон не обов'язково повинен перебувати у прямій видимості. Випромінення системи дистанційного управління також дозволяє виявити розташування оператора дрона. Система здатна виявити пристрій класу Phantom на відстані 50 км. Aartos, зокрема, захищала саміт NATO 2018 року у Брюсселі і зустріч Дональда Трампа з Кім Чен Ином того ж року у Сінгапурі.

[*)] Радіолокатор безперервного випромінювання з частотною модуляцією (Frequency-Modulated Continuous Wave radar, FMCW-radar) – це особливий тип радіолокаційних датчиків, що безперервно випромінюють сигнал, як і звичайний радіолокатор безперервної дії (CW-Radar). Але, на відміну від CW-радіолокатора, у FMCW під час вимірювання постійно змінюється робоча частота. Це дуже нагадує лінійно-частотну модуляцію (ЛЧМ), що використовується в IoT-системах LoRaWAN. Більш детально про ЛЧМ можна дізнатися із статті «Низькошвидкісний Інтернет речей в Україні: LoRaWAN та NB-IoT», СіБ 4 2021, с.44–55.

Лідари і просторовий контроль

Скануючий лідар — це, простою мовою, радар, який використовує лазерне випромінювання. Технологія давно використовується в авіації та космонавтиці, проте останнім часом набула поширення у самокерованих авто. Знайшли лідари своє місце і в охороні периметру, де компенсують недоліки, притаманні радарним системам. Зокрема, радар сам по собі не має достатньої роздільної здатності, щоб надійно розрізняти об'єкти (і саме тому працює у парі з відеокамерою). Лідар має набагато вищу (сантиметрову) точність, що радикально скорочує кількість хибних тривог. Оскільки він використовує десятки променів, людське око може безпосередньо зчитувати передане ним зображення на екрані.

Завдяки круговому огляду лідар дозволяє стежити не лише за периметром, але й за територією, що знаходиться усередині, слідкуючи за переміщеннями порушників вже після проникнення; зазвичай традиційні периметрові давачі «перестають бачити» людей, які перелізли через огорожу. Це нагадує ситуацію, яка наразі склалась у царині кібербезпеки, де контроль периметру доповнюється пошуком злочинців усередині мережі.

Наприклад, чеська компанія ***Accur8vision*** створила систему Tacticaware, що базується на різних моделях лідарів. У системі використовуються багатоканальні детектори (від 16 до 128 променів), кожен з яких здійснює кілька тисяч вимірювань на секунду, дальність роботи сягає 300 м, а точність — 2–3 см.

У Tacticware територія об'єкта ділиться на тривимірні зони, які відображаються на мапі. У разі, якщо в одній з таких зон з'являються чужинці, здіймається тривога, і на мапі відображуються дані про подію: кількість порушників, час проникнення і номер зони, а також швидкість і траєкторія руху. Після цього в потрібну точку спрямовуються камери відеонагляду. Понад те, камери можна націлити ще до того, як порушник з'явиться в полі зору.

Зони являють собою прості паралелепіпеди, які, однак, мають змінні характеристики. Наприклад, увечері територія може охоронятися, а вранці — вже ні. Також у зонах можна створювати коридори, де тривога не генеруватиметься. Системі можна наказати ігнорувати об'єкти, більші або менші за певну межу (наприклад, поїзд або, навпаки, дрібну тварину). Періодично здійснюється сканування місцевості для встановлення базової картини з урахуванням зміни листяного покриву тощо.

Accur8vision пропонує різноманітні сценарії застосування своєї розробки, які далеко не обмежуються охороною периметру. Наприклад, в аеропорту можна створити навколо фізичної огорожі «невидиму стіну», яка заздалегідь попереджатиме службу безпеки про наближення сторонніх осіб. Таку саму стіну можна облаштувати довкола літака, щоб ніхто чужий не наближався під час його завантаження (**рис. 5**). У приміщенні аеропорту лідари можуть показувати, скільки людей перебуває у тій чи іншій зоні: наприклад, чи не перевищено кількість пасажирів у черзі або чи дотримуються вони соціальної дистанції. На залізничному транспорті за допомогою лідарної системи можна встановити охоронну зону довкола вагонів, щоб уберегти їх від вандалів, або на переході через колії — у такому разі машиніст поїзда буде заздалегідь попереджений, що на рейках хтось є. На виробництві, серед багатьох інших застосувань, лідарна система може використовуватись для контролю доступу. Неавторизована особа не знає, що на віртуальній мапі вона відображається в оточенні червоного прямокутника, це дозволяє охоронцям таємно стежити за порушником.

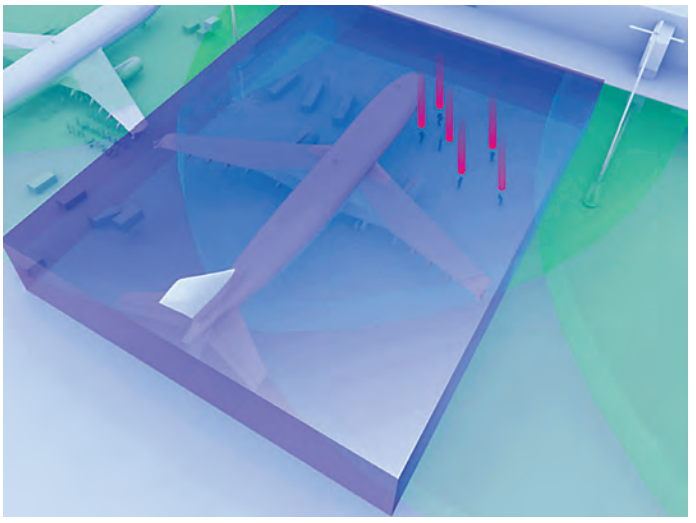

Рис. 5. Використання лідарної системи Accur8vision Tacticaware для створення охоронної зони довкола літака

В Accu8vision також успішно експериментували з детектуванням дронів. Для цього лідар розташовувався з нахилом, що створювало в небі сітку лазерних променів. У разі потрапляння БПЛА в охоронну зону оператор отримував сигнал тривоги.

Яке ж воно, світле майбутнє

Звісно, це не все, чим збагатився арсенал охорони периметру останніми роками. Цілком імовірно і те, що якісь інші технології розвинуться у напрямку, який дозволить застосовувати їх для охоронних цілей. У цій царині, так само як і в кібербезпеці, не припиняється боротьба меча та щита, і наполегливий злочинець відшукає спосіб обійти просунуті технічні засоби. Наприклад, прочитавши розділ про відлякування порушників мигтінням світла, наш редактор зауважив, що в цьому випадку можна вдягти захисні окуляри. Існують і давно використовуються (в авіації) технології обману радарів.

Безперечним залишається (як, втім, і скрізь) намагання розвантажити і убезпечити персонал і автоматизувати виявлення порушників. Технологічні новинки мають на меті виявити небажаного гостя заздалегідь, при цьому не генеруючи хибних тривог, отримати дані для розслідування, а найкраще — змусити його забратися геть. Можливо, з плином часу з'являться роботи-охоронці, які патрулюватимуть територію і ганятимуть порушників, тоді як охоронці-люди питимуть каву перед моніторами.

Василь ТКАЧЕНКО, **СиБ**