Видеонаблюдение в мире: слияния, поглощения и новые технологии

ТЕМА НОМЕРА

Глобальный рынок СВН живет активной жизнью — старые игроки объединяются для противодействия китайской экспансии, стартапы разрабатывают новые сервисы на основе ИИ, авиадроны и роботы выводят видеонаблюдение на новый уровень. И от всех этих процессов в итоге выигрывает заказчик.

Темпы роста мирового рынка систем охранного видеонаблюдения неразрывно связаны с технологическим аспектом. Достижения в области машинного обучения, видеоаналитики и других сферах стимулируют заказчиков обновлять свои системы. При этом роль камеры, как наиболее значимого элемента СВН, постепенно снижается. Без них, конечно, не обойтись, но ведущие разработчики и производители сместили акцент с физических характеристик устройства на программную составляющую. Современная СВН — это не просто средство фиксации событий, как было раньше, а главным образом комплексная аналитическая платформа, подразумевающая максимально оперативную реакцию на инцидент или даже предсказывающая потенциальную угрозу.

Но в этом направлении еще много предстоит сделать — программные технологии, особенно те, что связны с машинным обучением, большими данными, IoT и прочими популярными нынче явлениями, имеют огромный потенциал развития. Это значит, что на рынок будут поступать все новые, более совершенные продукты. Технологии стимулируют рынок, а тот, в свою очередь, будет создавать питательную базу для новых решений. Так что пока мы находимся в восходящем тренде. Как долго он продлится? Аналитики говорят как минимум о пяти ближайших годах. Дальше пока никто всерьез не заглядывает.

Цены снижаются, рынок растет

Мировой рынок систем физической безопасности в целом и СВН в частности растет уже много лет подряд, и пока что перелома этого тренда не видно. Так, по прогнозам аналитической компании MarketsandMarkets, общий объем сегмента безопасности по итогам нынешнего года должен превысить $90 млрд, а в 2021-м — достичь $110 млрд. Основным драйвером рынка являются технологии, открывающие перед пользователями новые возможности.

Речь главным образом идет о системах на базе машинного обучения (в т.ч. роботизированных), использующих аналитику и большие данные, а также технологии IoT. По данным исследователей, 38% сегмента приходится на услуги, еще 27% — это все, что связано с видеонаблюдением. В то же время другие аналитики — из компании Global Market Insights — сообщают о том, что мировые объемы продаж только IP-камер для систем безопасности к 2024 году превысят $20 млрд при среднегодовых темпах прироста около 20%. Также есть оценки для городских систем СВН (применяемых, например, в составе решений типа «умный город»), объем продаж которых по итогам нынешнего года может приблизиться к отметке $4 млрд (такие данные приводит IHS Markit). Одним из элементов Smart City являются нательные камеры СВН, которыми оснащаются полицейские во многих странах (в т.ч. в Украине). Этот сегмент растет особенно быстро — примерно на 30% в год. По состоянию на конец 2018-го общее число задействованных устройств по всему миру оценивалось в 1,5 млн. единиц, и оно будет увеличиваться (в США, например, даже действует федеральная программа по внедрению нательных камер в работу правоохранительных органов).

Интересно то, что рынок систем видеонаблюдения растет, несмотря на то что стоимость камер в среднем снижается. Это связывают с тем, что заказчики все более активно внедряют новые технологии, такие как видеоаналитика и работа с облачными сервисами, которые смещают акцент с самой камеры в область централизованных систем управления. При этом также отмечается, что в экономически развитых странах, на которые приходится

наибольший объем продаж, пользователи предпочитают устройства, оснащенные передовыми технологиями. В их числе — поддержка разрешения 4K, использование кодека H.265, реализация видеоаналитики на самой камере и т.д. Таким требованиям обычно отвечают модели среднего и верхнего ценового диапазона.

Еще одной характерной особенностью рынка СВН является то, что видеонаблюдение все чаще интегрируется со СКУД и другими системами физической безопасности. Такая тенденция наблюдалась и раньше, но в последние несколько лет благодаря тотальному проникновению IP во все сферы охранных решений она начала развиваться стремительно, и теперь становится все сложнее выделить видеонаблюдение в общем потоке проектов, связанных с системами физической безопасности.

Но всеобщей «айпификацией» довольны далеко не все. Конечно, для многих производителей это способ получения дополнительного заработка, а для пользователей — новые возможности, но вместе с тем существует и ряд нюансов, которые позволяют успешно работать на рынке и аналоговым камерам (речь, разумеется, о современных системах типа HD CCTV). Например, в случае IP-видеонаблюдения появляются вопросы, связанные с обеспечением кибербезопасности, которых нет в аналоговых решениях. Есть свои особенности в политике лицензирования программного обеспечения (обычно на каждый канал IP-системы), частоте обновления ПО, к тому же IP-камеры, в общем случае, дороже аналоговых решений. Все это позволяет успешно сосуществовать на рынке обоим сегментам, но IP с каждым годом отвоевывает все больше пространства.

Параллельно с рынком камер растет сегмент видеорегистраторов и специальных СХД, что вполне естественно, поскольку видеоданных становится все больше, а учитывая, что большая часть из них — это бесполезная информация, в общем решении СВН возрастает роль аналитики и ПО для работы с видеоархивами.

Особым классом систем в данном случае являются облачные платформы — VSaaS (Video Surveillance as a Service, «видеонаблюдение как услуга») и ACaaS (Access Control as a Service, «СКД как услуга»).

Спрос на них постепенно растет, но не так быстро, как прогнозировали аналитики. В числе причин замедления темпов — относительно высокая стоимость сервисов и существенные требования к пропускной способности каналов связи, которые реализуемы далеко не везде. Согласно данным отчета компании Memoori, по итогам 2018 года мировой объем продаж в сфере VSaaS составил $1,2 млрд, ACaaS — $0,6 млрд. Причем основными потребителями в обоих случаях являются представители сегмента СМБ, а крупные организации мало интересуются подобными сервисами.

Не менее важны и технологии для центров мониторинга, куда должна стекаться вся информация, связанная с деятельностью систем безопасности. Еще совсем недавно казалось, что видеоаналитика решит все вопросы и поможет дежурным оперативно реагировать на все события вместо бездумного слежения за мониторами. Но уже сейчас становится ясно, что количество поступающих данных растет настолько стремительно, что даже с учетом помощи аналитического ПО человеческий фактор все равно остается узким местом. Эта тенденция еще не проявилась повсеместно, но там, где имеются действительно масштабные системы видеонаблюдения (например, на уровне мегаполиса), количество событий, подразумевающих реакцию человека, чрезвычайно велико. Зачастую неоправданно, поскольку большинство эпизодов не несут серьезной угрозы.

Решить задачу обращения с огромными массивами видео- и других данных планируют при помощи систем на базе «искусственного интеллекта» и машинного обучения, которые должны отчасти взять на себя функции оператора. Иными словами — требуется совершенно другой уровень автоматизации, позволяющий поднять эффективность комплексных распределенных систем безопасности на качественно новый уровень. Над этим вопросом сегодня работают как ведущие отраслевые компании, так и стартапы, но его решение — дело будущего. Особенно остро такая задача может вскоре встать перед городами, внедряющими у себя системы Smart City.

Лидеры глобального рынка

Теперь несколько слов о глобальных лидерах. Каждый год тематический Интернет-ресурс ***asmag.com*** публикует рейтинг ***Top Security 50***, в который входят пятьдесят ведущих компаний, специализирующихся на системах безопасности. Для сравнения берется суммарный доход от всех видов деятельности (СВН, СКУД и пр.) за предыдущий год и сравнивается его динамика (в свежем рейтинге сопоставляются результаты 2017 и 2016 годов). Так, согласно списку 2018 года первую позицию на мировом рынке сохранила за собой китайская Hikvision, доход которой в 2017-м составил около $5,4 млрд — это существенно больше, чем у любого другого конкурента. Вторую позицию заняла Dahua (тоже Китай), заработавшая чуть менее $2,7 млрд. В новом рейтинге она вытеснила компанию Bosch Security Systems, которая раньше занимала второе место, а сейчас находится на четвертом. Третья позиция у Assa Abloy, четвертая у Axis (обе представляют Швецию). Единственная компания с постсоветского пространства — российская DSSL (Trassir), разместившаяся на 37-й строчке, в 2017 году она нарастила обороты почти на 50% по сравнению с 2016-м.

Поскольку в рейтинге Top Security участвуют организации, занимающиеся различными направлениями безопасности (та же Assa Abloy — мировой лидер в сфере электронных замков и решений для контроля входных групп), а наша статья посвящена СВН, мы скомпилировали свою версию списка, в которой представлены ТОП-20 компаний, основная деятельность которых связана главным образом с видеонаблюдением. В таком варианте первая пятерка выглядит следующим образом: Hikvision, Dahua, Bosch, Axis, FLIR (**табл.**).

Таблица. Лидеры мирового рынка СВН по данным рейтинга Top Security 50 за 2018 год

Позиция в рейтинге среди компаний сегмента СВН*	Название компании	Страна	Годовой доход (от всех видов деятельности), $ млн		Годовой прирост, %
			2017	2016	
1 (1)	Hikvision Technology	КНР	5364	4242	26,4
2 (2)	Dahua Technology	КНР	2680	1896	41,4
3 (4)	Bosch Security Systems	ФРГ	2078	1964	6,3
4 (5)	Axis Communications	Швеция	967	830	16,5
5 (6)	FLIR Systems	США	777	772	0,6
6 (8)	Hanwha Techwin	Южная Корея	493	541	-9
7 (9)	Tiandy Technology	КНР	450	345	30,2
8 (10)	Avigilon	Канада	410	354	15,6
9 (12)	Infinova	КНР	258	255	1,3
10 (14)	Vivotek	Тайвань	174	152	14,7
11 (15)	CP Plus	Индия	171	134	27,7
12 (18)	Raysharp	КНР	133	77	71,3
13 (19)	Milestone Systems	Дания	128	103	24,3
14 (20)	Kedacom	КНР	124	97	26,9
15 (25)	IDIS	Южная Корея	80	91	-12,2
16 (26)	TVT	КНР	74	75	-1
17 (27)	Mobotix	ФРГ	71	86,2	-17,7
18 (28)	Dynacolor	Тайвань	70	62	12
19 (29)	Wanjiaan	КНР	68	64	5
20 (34)	Geovision	Тайвань	50	60	-16,7

* В скобках указана абсолютная позиция

Отметим, что Top Security 50 вряд ли можно считать исчерпывающим перечнем, поскольку в нем не представлен ряд крупных игроков рынка, таких как Honeywell, Johnson Controls (которому принадлежат в т.ч. бренды Exacq, Tyco), Sony, Panasonic, Uniview и др. Тем не менее он является наиболее полным и комплексным рейтингом, презентованным в открытом доступе, и позволяет получить общее представление о мировом рынке и динамике его основных участников.

Год слияний и поглощений

В глобальном разрезе мировой рынок систем охранного видеонаблюдения существенно оживляют различные стартапы. Это вполне логично, ведь большинство новых и востребованных функций СВН лежит в области аналитики и управления, а значит — программного обеспечения. В то же время разработка ПО во многих случаях не требует таких существенных затрат, как, скажем, создание новых физических технологий. Удачный программный продукт вполне способна разработать небольшая группа энтузиастов или перспективная команда, поддержанная венчурным капиталом. В этом плане ведущим мировым брендам на рынке СВН сложно составить конкуренцию, поэтому они все чаще предпочитают приобретать стартапы (или отдельные технологии) вместо создания собственных программных решений.

С другой стороны, у традиционных игроков остается не так уж много места для маневра. Одна и та же компонентная база доступна всем участникам рынка — для «топовых» решений можно взять элементы получше и подороже, для бюджетных моделей — попроще и подешевле. Но при определенном желании любая компания способна поставить на рынок камеру или комплекс СВН какого угодно уровня. Поэтому вопрос стратегического развития лежит главным образом в области возможностей ПО, а также, не в последнюю очередь, — маркетинга и работы с партнерами. Здесь преимущество имеют компании, располагающие существенными финансовыми ресурсами — собственными или заемными, поэтому серия слияний и поглощений, которая отмечается на мировом рынке последние несколько лет, будет продолжаться. Причем такая тенденция характерна и для сегмента систем безопасности в целом. Как сообщает аналитическая компания Memoori, по итогам 2018 года стоимость всех сделок, связанных с приобретением отраслевых компаний на этом рынке, которых было отмечено около полусотни, составила $7,3 млрд.

Так, в начале 2018 года стало известно, что канадскую компанию ***Avigilon*** покупает за $1 млрд ***Motorola Solutions***. При этом, судя по всему, основной целью нового владельца является завидный патентный пул Avigilon. В свое время этот производитель немало потратился на приобретение различных технологий, в частности, выкупил все патенты компании ***ObjectVideo***, в числе которых — важные разработки в области видеоаналитики (такие как формирование потока метаданных, содержащих логическую информацию, извлеченную системой видеоаналитики из изображений, алгоритмы выявления пересечений виртуальных линий и т.д.). В разное время патентные отчисления в пользу ObjectVideo, а соответственно и Avigilon, платили или платят такие мировые гиганты, как Bosch Security Systems, Hikvision, FLIR, Panasonic, Pelco, Sony, Tyco. Теперь же все права на технологии перешли к Motorola Solutions, которая никогда не была игроком на рынке СВН, но сейчас, благодаря удачному приобретению, вошла сразу в число лидеров. Так, по данным аналитической компании IHS Markit, на момент слияния, Avigilon занимала восьмое место в мире по объему продаж систем видеонаблюдения — около 2% мирового рынка.

К тому же отраслевые эксперты делают предположение о том, что, возможно, еще одной целью Motorola является часть американского рынка СВН в госсекторе. Оттуда, напомним, начали активно выживать производителей из КНР, но освободившийся сегмент должен кто-то занять. Очевидно, здесь приоритет будет отдан американской компании, желательно с мировым именем, даже несмотря на ценовую разницу (решения Avigilon, в общем случае, ощутимо дороже изделий Hikvision, Dahua, Uniview и других китайских брендов).

Примерно в тот же период (февраль 2018 года) крупный американский производитель ***FLIR***, известный в первую очередь своими тепловизионными камерами, решил продать кое-что из своей собственности. В частности, было объявлено о том, что китайская компания Dahua приобретет торговую марку Lorex, под которой FLIR поставлял на рынок недорогие камеры оптического

диапазона. Сумма сделки составила около $30 млн, притом что в 2012 году сам FLIR заплатил за покупку Lorex вдвое больше. Очевидно, бизнес развивался не так активно, как на то рассчитывали, и компания решила избавиться от актива, пока за него еще готовы платить. Комментируя сделку, Джим Кэннон, руководитель FLIR, высказался в том контексте, что потребительский сегмент больше не является приоритетным для компании, которая сконцентрирует усилия на более привычном для себя рынке решений для предприятий и критически важных инфраструктур. К тому же, как отметил менеджер, продукция Lorex (чья штаб-квартира находится в Канаде) испытывает значительное ценовое давление на рынке.

Примечательно, что Dahua, которая стала новым владельцем Lorex, на самом деле являлась OEM-производителем для данной торговой марки, и теперь она сможет поставлять эти решения напрямую потребителям. При этом одной из главных целей китайской компании, как полагают специалисты, является усиление позиций на рынке Северной Америки благодаря использованию местного бренда, который к тому же в сознании потребителей ассоциируется с таким лидером сегмента, как FLIR.

Вместе с тем Dahua развивает и другие торговые марки для сегментов SOHO и SMB. Так, в 2018 году начались поставки на мировой рынок камер бод брендом Lechange, которые ранее продавались только в Китае. Примечательно, что эти устройства позиционируются в тот же сегмент, что и решения Lorex, также пересекаются и рынки сбыта. Так что цель такого хода пока не вполне понятна.

Что касается самой FLIR, то компания явно усиливает свои позиции в сферах, связанных с оборонными заказами. Для этого, в частности, была приобретена Aeryon Labs — один из мировых лидеров в сфере разработки миниатюрных (весом до 20 фунтов) разведывательных армейских квадрокоптеров. Сделка состоялась в начале 2019 года, а ее стоимость составила $200 млн.

Не выдержала ценовых войн и ***Arecont Vision***, которая весной прошлого года подала на банкротство. Напомним, что эта компания со штаб-квартирой в Глендейле (Калифорния, США) была создана в 2003 году двумя выходцами из России — Михаилом Каплинским и Владимиром Березиным. В лучшие времена ее офисы располагались в обеих Америках, Европе, Африке, Азиатско-Тихоокеанском регионе, на Ближнем Востоке. Разработка оборудования велась на территории Японии, программное обеспечение создавалось в России, а производственная база размещалась в США. Как сообщает зарубежная пресса, в 2014 году заказчиками Arecont были, в частности, NASA и SpaceX. На пике своего развития за компанию давали $170 млн (эту сумму озвучила китайская NetPosa Technologies в ноябре 2017-го). Но ряд ошибочных управленческих решений и неподъемные долги (в сумме более $70 млн) привели к банкротству. В итоге компанию — почти все ее имущество и патенты — приобрела за $11,25 млн (еще $10,3 млн будут вложены в виде оборотных средств) компания Costar Technologies, которая занимается разработкой систем видеонаблюдения и машинного зрения. Таким образом, Arecont не уходит с рынка, а лишь меняет владельца. При этом, даже находясь состоянии банкрота, компании не только удалось сохранить всех сотрудников, но и выпустить серию IP-камер Contera, а также разработать новый веб-сервис и облачную систему хранения видеоданных.

Продолжает активные покупки и ***Canon***. К двум приобретенным ранее активам в сфере СВН — Axis Communications и Milestone Systems — добавился также израильский разработчик ПО для видеоаналитики ***BriefCam***, известный, в частности, благодаря фирменной технологии быстрого поиска в видеоархиве Video Synopsis. Кроме того, BriefCam ведет активные разработки в сфере аналитических решений на базе ИИ. О сделке было объявлено в мае 2018 года, цена покупки официально не сообщалась, однако ряд отраслевых изданий оценивают ее в $90 млн.

Konica Minolta вкладывает средства в развитие ***Mobotix*** (65% акций которой были приобретены несколько лет назад). В 2018–2019 финансовом году планируется инвестировать не менее $5 млн главным образом в сферу НИОКР. Следствием вложений стало появление в камерах Mobotix новых матриц высокого разрешения и еще более качественных объективов.

А вот бизнес СВН ***Panasonic***, похоже, переживает не лучшие времена. Так, летом 2019 года было объявлено о том, что компания выделит бизнес по производству камер видеонаблюдения в отдельную независимую структуру, после чего 80% акций в ней купит инвестиционный фонд Polaris Capital Group — за $270 млн (еще 20% останутся у Panasonic). И снова в качестве причин такого шага называется ценовое давление со стороны китайских разработчиков.

Начало работы новой компании, которая получит название Panasonic i-Pro Sensing Solutions Co., Ltd., намечено на ноябрь текущего года. Примечательно, что о планах реструктуризации бизнеса СВН японский производитель электроники сообщал уже давно. Например, в марте прошлого года компания выразила готовность продать свой завод в китайском Сучжоу (провинция Цзянсу, КНР). Причем только за этот актив Panasonic планировала выручить не менее $470 млн, в то время как в реальности кроме упомянутого завода единым пакетом был продан еще целый ряд других объектов собственности за гораздо меньшую сумму.

Планирует избавиться от своего бизнеса СВН и Schneider Electric. Как стало известно из различных зарубежных источников, электротехнический гигант ведет переговоры о продаже компании ***Pelco*** инвестиционному фонду Transom Capital Group. О том, сколько планируется выручить от продажи актива, официально не сообщается, но по мнению отраслевых аналитиков, вряд ли стоит рассчитывать на то, что покупатель предложит больше $200 млн. При этом сама SE купила Pelco в 2008 году за $1,5 млрд, что на тот момент было отраслевым рекордом.

Как отмечается, тогда еще никто не мог предположить, что китайская экспансия на рынке СВН будет столь сильна и сегмент СВН окажется под таким сильным ценовым давлением. Но реальность оказалась такова, что если в начале 2000-х выручка Pelco превышала полмиллиарда долларов, то в 2018-м не дотянула и до $170 млн. В то же время компания продолжает выпускать новые продукты для различных вертикальных рынков, в частности, недавно был заключен технологический альянс с IBM, в рамках которого планируется разрабатывать решения для СВН с использованием элементов ИИ.

Но, очевидно, самой громкой новостью последнего года стало решение правительства США о запрете использования продукции мировых лидеров СВН — китайских компаний ***Hikvision*** и ***Dahua*** — во всех федеральных ведомствах страны. Фактическое действие закона началось с августа 2019 года. Данный шаг выглядит вполне логичным в контексте торговых войн между КНР и США, а также ввиду опасения того, что контролируемая компартией Китая Hikvision и Dahua, которую подозревают в связях с правительством КНР, получат доступ к сведениям, представляющим государственную тайну. Существенную роль также сыграло и то, что в оборудовании Hikvision и Dahua не раз находили серьезные незадокументированные уязвимости, которые могли быть оставлены намеренно.

Тем не менее вопреки расхожему мнению запрет касается только федеральных структур. Решения на уровне штата, округа, муниципалитета принимаются местными органами самоуправления, далеко не все из которых разделяют видение центрального правительства.

Кстати, всего через две недели после вступления закона в силу компания Panasonic объявила о прекращении поставок нескольких моделей камер. Как удалось выяснить впоследствии — все они выпускались китайской компанией Dahua в рамках OEM-соглашения, заключенного еще в 2016 году. Очевидно, таким образом, Panasonic пытается отвести от себя любые возможные подозрения, которые потенциально могут помешать компании в получении американских государственных контрактов.

Справедливости ради стоит отметить, что критические уязвимости время от времени обнаруживают и в изделиях известных брендов, которые славятся своей надежностью и безопасностью. Так, в конце прошлого года специалисты по информационной безопасности компании VDOO выявили уязвимость в камерах ***Bosch*** (чего никогда не случалось ранее). Причем угрозе был присвоен уровень опасности 9,4 балла из 10 возможных. Суть проблемы в том, что хакер, подключившись по протоколу HTTP или HTTPS к устройству, потенциально сможет вызвать переполнение буфера и затем обойти ограничение доступа, задаваемое логином и паролем, или активировать отключение функций камеры. Как выяснили специалисты, уязвимость возникла в ноябре 2016 года вместе с новой версией прошивки. Сейчас, как сообщают в Bosch, проблема устранена. Камеры этого производителя считаются очень надежными и широко используются в т.ч. государственными структурами США и стран ЕС.

Также отметим, что, несмотря на высочайшую конкуренцию на мировом рынке СВН, здесь время от времени появляются новые заметные игроки. Один из которых заявил о себе буквально в 2019 году. Речь идет о стартапе ***Qumulex***, специализирующемся на системах видеонаблюдения, облачных технологиях и видеоаналитике. Примечательна фирма своими основателями, в числе которых Дэн Риттман, Том Бакли и Дэвид Андервуд, которые известны тем, что в 2000-х, располагая капиталом в $50 млн, создали компанию Exacq. Последняя быстро превратилась в одного из крупных мировых игроков сегмента СВН и в итоге была продана Tyco за $150 млн. В 2017 году предприниматели покинули Exacq и решили развивать новый собственный проект — Qumulex, первые коммерческие продукты которого должны выйти в конце нынешнего года.

Технологии, стимулирующие рынок — «искусственный интеллект»

Тема искусственного интеллекта в последние годы муссируется более чем активно. Благодаря маркетинговым усилиям многих компаний вокруг нее творится такой ажиотаж, что системы, где ИИ не указан в качестве одного из пунктов, как бы оказываются за рамками прогресса. Сферу видеонаблюдения эта мода также не обошла. То, что камеры должны быть «интеллектуальными» (т.е. обладать определенной степенью автоматизации), стало уже общим местом. Теперь в приоритете — освоение ИИ. Но, несмотря на всю шумиху и довольно существенные вложения в НИОКР, систем, обладающих хотя бы отдельными элементами искусственного интеллекта, в сфере СВН пока нет. Да, алгоритмы машинного обучения и нейронные сети существенно обогатили арсенал охранных систем всех типов за последние годы, но до ИИ еще далеко. Например, камеры хорошо справляются с теми задачами, которые требуют распознавания различных образов — предметов, животных, лиц, но лишь в определенных условиях. Но, скажем, надежная идентификация человека при различных ракурсах съемки, особенно в условиях сложного освещения, — задача пока не решенная до конца. Есть попытки (иногда частично удачные) разработки систем на базе нейронных сетей, позволяющих узнать человека по косвенным признакам, например, походке, но такие решения еще очень далеки от совершенства и носят скорее экспериментальный характер.

В то же время определенных успехов удалось добиться в сфере распознавания подозрительного поведения — камеры уже довольно точно «научились» определять эпизоды, похожие на сцены драки, ограбления и прочие аномалии. В ноябре 2018 года компания Athena Security разработала технологию, которая позволяет определить на видео вооруженного человека и подать сигнал тревоги на пульт охраны. Для обработки изображений система использует алгоритмы машинного зрения и мощные графические карты, благодаря чему удается распознать поведение, характерное для вооруженного человека. По словам разработчиков, решение имеет точность распознавания оружия на уровне 99% за время, не превышающее двух секунд. Система уже имеет своих заказчиков.

Например, она установлена в высшей школе Archbishop Wood (Варминстер, штат Пенсильвания, США), где правда, является лишь частью комплексной многоуровневой системы безопасности. Как сообщает руководство Athena, технология оказалась удачной, и в скором времени планируется вывести на рынок системы для распознавания драк и выявления холодного оружия в кадре.

Тем не менее, как показывает практика, количество ложных срабатываний в системах такого рода довольно велико. Но, во-первых, алгоритмы постоянно совершенствуются, а во-вторых — лучше несколько раз убедиться в том, что это «ложная тревога», чем проглядеть серьезную угрозу.

Аналитика, связанная с распознаванием образов и, в частности, лиц становится все более эффективной год от года, и это внушает определенные опасения жителям западных стран с развитыми традициями демократии. За введение контроля и регулирования данной сферы в ЕС и США выступают многие политики, бизнесмены и общественные активисты. С одной стороны, игнорировать такие обращения не получится, поскольку они отражают настроения, доминирующие в обществе, с другой — полностью отказаться от технологии равносильно серьезному ослаблению систем безопасности. Необходим компромисс. Одним из вариантов являются программы, позволяющие обеспечивать избирательное распознавание, когда система обращает внимание только на лица (или номера автомобилей), которые имеются в базе данных. Другие люди не распознаются (вплоть до того, что лица случайных прохожих могут быть задымлены). Но такие решения только начинают разрабатываться. Нечто подобное в апреле 2019-го вывела на рынок компания Pimloc. Программный продукт SecureRedact как раз и создан для противодействия распознаванию лиц на видеозаписи, но его возможности пока ограничены. Полнофункциональная версия ожидается ближе к концу года.

Справедливости ради стоит отметить, что разработчики подобных решений пока не слишком спешат выводить их на рынок, поскольку насущной необходимости в них прямо сейчас нет. Но если ситуация в правовом поле будет развиваться так, как сегодня, вполне возможно, что вскоре в ЕС и США примут законы, регулирующие вопросы распознавания и идентификации людей в общественных местах. И тогда производителям надо будет иметь что предложить, а пока это скорее работа на перспективу.

Еще из практических реализаций алгоритмов машинного обучения в СВН можно отметить интеграцию их с аудиоустройствами и программами для распознавания речи. Так, одной из проблем видеонаблюдения является то, что камера фиксирует все подряд, что не всегда уместно. Например, в случае домашних систем владельцы зачастую хотят, чтобы камера работала только в их отсутствие и не снимала происходящее дома, когда там только «свои». Все это, конечно, реализуемо на различных уровнях, но недавно появились решения, отключающие конкретные устройства по звуковой команде. Такие системы предлагает, например, Angee Technologies. Камера умеет идентифицировать владельца по голосу и способна выполнять некоторые команды — к примеру, включаться и отключаться по кодовой фразе. С другой стороны, звук нужного голоса можно воспроизвести с проигрывателя, что, по идее, позволит обойти защиту. В общем, подобные решения еще находятся в начале технологического пути, но интерес к ним есть.

В то же время удачных примеров в области интеграции аудио и видеокомпонентов в системах комплексной защиты существует немало. Так, все более популярными (ввиду постепенного снижения стоимости) становятся системы, позволяющие не только зафиксировать аномальный звук (выстрел, взрыв, крик и т.д.), но также определить его направление и сфокусировать камеру на нужном участке.

Умение «слушать» — не новость, гораздо интереснее то, что скоро, похоже, камеры научатся «видеть» сквозь стены. Во всяком случае, разработки в этом направлении ведет группа исследователей из MIT. Речь идет о блоке особых сенсоров, сканирующих окружающий радиоэфир диапазона Wi-Fi. Принцип работы системы, получившей название RF-Pose, основан на том, что радиоволны, проходящие сквозь стены, особым образом меняют форму, отражаясь от человеческого тела. Если уловить эти сигналы и преобразовать их с помощью определенных алгоритмов, то по данным исследователей, можно с высокой точностью выявить не только сам факт наличия человека за стеной, но и построить модель его движения (для этого уже используются нейронные сети), которая, в свою очередь, преобразуется в графическое изображение (**рис. 1**). Пока что разработка носит экспериментальный характер.

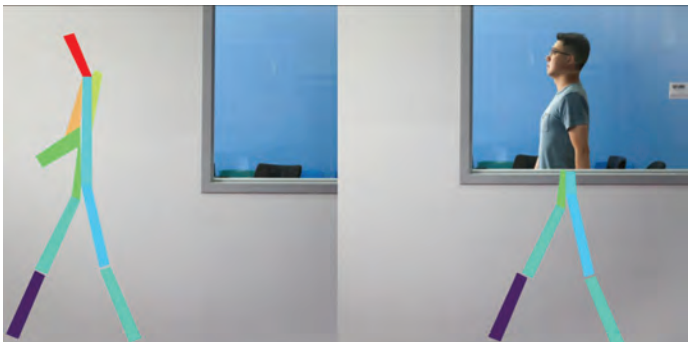


Рис. 1. Система RF-Pose «видит» человека за стеной

Наблюдение с воздуха

Очень активно развивается видеонаблюдение с использованием беспилотных летательных аппаратов. Рост функциональности и надежности устройств с одновременным снижением их стоимости ведет к все более широкому применению дронов в области СВН. Их уже широко используют спасательные службы и полиция в экономически развитых странах. Беспилотники используются не только ситуативно — при осмотре мест происшествий, но и осуществляют скрытое патрулирование потенциально опасных территорий. Удобно использовать их для охраны обширных территорий — лесов (от возгораний) железных дорог или границ.

Тем не менее большой проблемой в этом отношении является емкость аккумуляторов, которая существенно ограничивает время использования беспилотников. Отчасти решить эту проблему позволяет применение... электрического кабеля. Сейчас сегмент таких дронов «на поводке» развивается очень динамично, и они находят широкое применение в сфере безопасности. Фактически такие устройства представляют собой вариант мобильной наблюдательной вышки, которую при необходимости можно легко переместить в любое место, где есть постоянный источник электропитания. От АКБ в этом случае можно отказаться вовсе, а поскольку передача сигнала также может осуществляться по кабелю, негласно перехватить управление таким беспилотником существенно сложнее, чем в традиционном случае, когда все данные транслируются по радиоканалу.

Отдельное интересное направление — микродроны. Сегодня они массово поступают в армии стран-членов НАТО, где принята программа внедрения PRC (Personal Reconnaissance System, персональная система разведки). Примером системы такого типа является модель FLIR Black Hornret 3 (**рис. 2**)

Это миниатюрное устройство весом всего 33 г оснащено одним пропеллером и двумя камерами — оптической (с разрешением 640×480 пикс. для видео и 1600×1200 пикс. — для фото) и тепловизионной (160×120 пикс). Максимальная скорость полета — 21 км/ч, дальность — до 2 км, время в воздухе — до 25 мин. Ветроустойчивость достигает 10 м/с. Может летать в дождь. Защита канала передачи данных обеспечивается за счет применения взломоустойчивых алгоритмов шифрования. Управление (одними или несколькими устройствами сразу) осуществляется удаленно с помощью специального контроллера и дисплея. Но цена системы впечатляет — комплект для одного дрона (с учетом инструментов управления и ПО) стартует от $40 тыс. Тем не менее уже в начале 2019 года FLIR подписал минимум три крупных контракта общей стоимостью около $130 млн на поставку Black Hornret 3 для армий США, Франции и Великобритании.

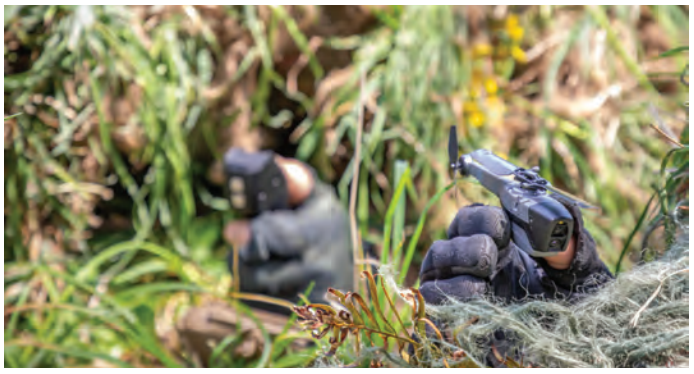
Но дроны также используют и злоумышленники. Например, с их помощью в последнее время все чаще доставляют нелегальные передачи в места лишения свободы. А устройства, оснащенные камерами, способны вести нелегальную слежку, объект которой даже не догадывается о наблюдении за собой. Такой метод часто применяют домовые и офисные воры.

Технологии противодействия тоже не стоят на месте. Системы для захвата дронов сегодня довольно развиты, вместе с тем они все еще достаточно дороги. Но в прошлом году инженеры университета Бен-Гуриона в Негеве (Израиль) разработали относительно недорогую бытовую систему, позволяющую определить факт несанкционированной съемки с беспилотника. Решение включает в себя небольшую параболическую антенну, подключаемую к ноутбуку, и набор специального ПО для ОС Linux. Второй компонент — полоски мерцающих светодиодов, которые можно прикрепить, например, на оконную раму. Дело в том, что дрон передает данные по зашифрованному радиоканалу, взломать который бывает довольно сложно. Но с помощью антенны можно выявить колебания в интенсивности окружающего радиосигнала. Таким образом, если в поле зрения шпионской камеры попадают светодиоды, битрейт будет колебаться пропорционально частоте их мерцания. Антенна сразу же уловит такую аномалию и подаст сигнал тревоги, уведомив владельца о том, что за ним наблюдают.

Однако беспилотники — это уже повседневная реальность СВН. Последнее слово сейчас за спутниками. Скажем, компания EarthNow планирует в будущем использовать обширную группу низкоорбитальных сателлитов, оснащенных камерами высокого разрешения, которые будут транслировать изображение в режиме реального времени. Пока что EarthNow — это перспективный стартап, но деньги в него уже вложили Airbus, SoftBank Group, а также сам Билл Гейтс. Для реализации проекта будут использованы спутники глобального интернет-проекта ***OneWeb***. На первом этапе изображения EarthNow будут доступны различным правительственным структурам с целью слежения за развитием природных катаклизмов, контроля состояния урожая или обнаружения нелегального вылова рыбы. Позже доступ планируется предоставить и коммерческим пользователям.

Ползущая роботизация

Весьма перспективным направлением СВН в частности и охранных систем вообще является робототехника. Есть даже компании, которые специализируются в данном направлении. Например, Knightscope в 2018-м представила уже четвертое поколение уличных роботов-охранников K5 (**рис. 3**), выпускаемых с 2014 года, о которых уже много говорились и писалось в Интернете.



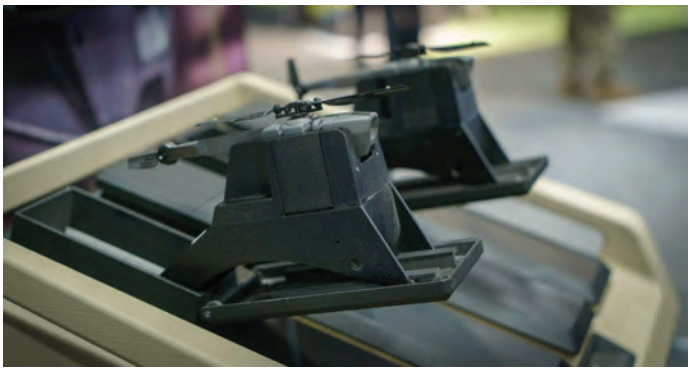


Рис. 2. Армейский микродрон FLIR Black Hornret 3 в одиночной версии и на платформе для группового запуска

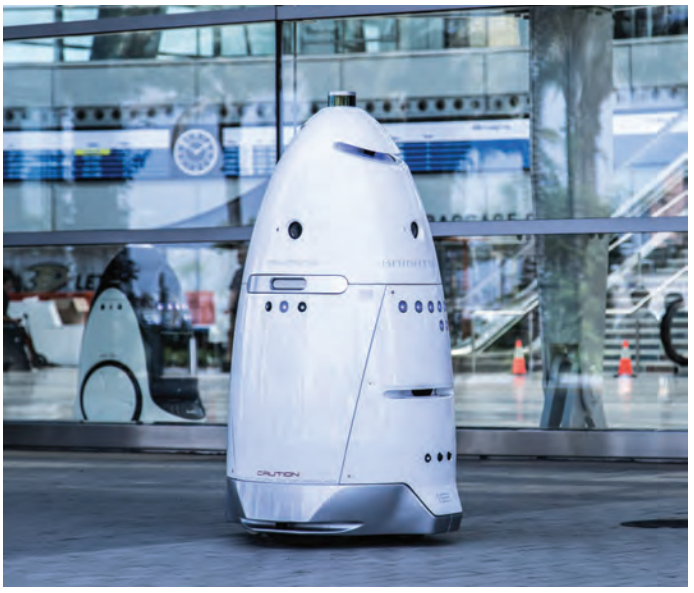


Рис. 3. Робот Knightscope K5 за работой

Эти «интеллектуальные» комплексы высотой полтора метра оснащены не только камерами оптического диапазона, но и тепловизорами, различными датчиками, GPS-навигатором, средствами освещения и связи, а также другими устройствами. Робот имеет усиленную тележку, которая позволяет ему ездить по неровному грунту, и вандалоустойчивый корпус. K5 выполняет задачи патрулирования в автономном режиме и умеет вовремя возвращаться на станцию подзарядки. В США — основном рынке подобных решений — всерьез опасаются, что роботы будут лишать работы людей. Ведь, например, человеку-охраннику нельзя платить менее $14 в час, притом что аренда того же K5 обходится в $7 за то же время. Вместе с тем такие системы все еще несовершенны и не вызывают ажиотажного спроса. Так, несколько лет назад Knightscope планировала реализовать около шестисот роботов до конца 2018-года. Но реальный план продаж был выполнен менее чем на 8% от заявленного. При этом, что интересно, заказчики, совершившие покупку, как правило, больше не приобретают новых роботов.

Тем не менее производитель продолжает технологическое развитие своих систем — в ближайшем будущем планируется оснастить их средствами аналитики для распознавания и идентификации лиц. Сейчас такая возможность реализована только в стационарных роботах Knightscope серии K1. В целом же мировой рынок роботов-охранников оценивается в $2,1 млрд, что, по мнению исследовательской компании Mordor Intelligence, немало, учитывая то, что сегмент начал фактически развиваться всего около пяти лет назад. Пока что аналитики затрудняются выделить здесь лидеров — рынок слишком фрагментирован. Здесь присутствует большое количество разнообразных стартапов, каждый из которых имеет свою небольшую долю. Борьба за рынок только начинается.

Видеонаблюдение — в начале пути

Сегодня многие эксперты сходятся во мнении, что охранное видеонаблюдение все еще имеет огромный потенциал для развития, поскольку нынешние технологии могут обеспечить безопасность лишь в очень ограниченных пределах. Несмотря на то что СВН внедряются повсеместно, а камеры становятся «умнее», это не оказывает пропорционального влияния на статистику преступлений. Так, наибольшее количество камер в мире, если считать на душу населения, установлено в Соединенном Королевстве — более 6 млн устройств (или одна камера на 11 человек) — такие данные приводит сеть инсталляторов систем видеонаблюдения Великобритании CCTV — co.uk. Но как показывает национальная статистика, существенного влияния на раскрываемость это не оказало — лишь 3% преступлений успешно расследуются благодаря данным СВН. Более того, проводились специальные исследования по отдельным регионам, которые показали, что в двух похожих друг на друга округах Британии уровни преступности и раскрываемости также являются примерно эквивалентными, притом что в одном из них используется в десять раз больше камер СВН, чем в другом. Например, Лондон охвачен сетью из 627 тыс. камер, или в среднем одно устройство на 14 человек, и все равно доля преступлений, раскрываемых с их помощью, не превышает нескольких процентов. По другим европейским странам и городам реальная ситуация еще хуже.

В этом смысле интересна статистика по украинской столице, где камер почти в тысячу раз меньше, чем в Лондоне — около 7 тыс. устройств (примерно 1 на 500 постоянных жителей). Так, 31 октября прошлого года начальник полиции Киева Андрей Крищенко сообщил о 2,5 тыс. раскрытых уголовных производств (с начала 2018-го), при расследовании которых использовалась информация, полученная из записей установленных камер. Это составляет примерно 9–10% от общего числа зарегистрированных преступлений на соответствующий период времени. Выходит, СВН, работающая в украинской столице, существенно превосходит по эффективности лондонскую? Хочется в это верить, но вряд ли. Очевидно, дело в том, что даже если материалы видеонаблюдения использовались в ходе уголовного производства, это вовсе не означает, что они как-то помогли в расследовании. В то же время статистику случаев, когда видеоданные оказывались решающим фактором, в публичном доступе найти не удалось.

Как бы то ни было, видеонаблюдение все еще не является достаточно надежным элементом защиты — слишком много факторов влияют на качество его работы. Экстремальные температуры, плотные осадки, сложные условия освещения — все это может свести на нет эффективность видеокамер, не говоря уже о том, что их достаточно легко повредить физически (разбить, закрасить объектив, оборвать провода). К тому же преступник запросто может заранее скрыть свое лицо одним их множества способов, особенно зная, что за ним будет наблюдать камера. Данные вопросы постепенно решаются теми или иными методами, но очевидно, что в технологическом плане еще очень многое предстоит сделать для того, чтобы СВН стали по-настоящему эффективным инструментом обеспечения физической безопасности.

Игорь КИРИЛЛОВ, СиБ