Пандемии вопреки:
рынок СВН растет, несмотря ни на что

Рынок систем охранного видеонаблюдения и технической безопасности продолжает развиваться, несмотря ни на какие пертурбации. Это справедливо как для Украины, так и для мира в целом. Более того, в новых сложных условиях производители нашли и новые возможности для развития.

Мировой рынок систем охранного видеонаблюдения растет и развивается — как в технологическом, так и в рыночном аспектах, которые, по сути, являются двумя сторонами одной медали. Появление перспективных технологий стимулирует увеличение глобальных продаж, а динамично растущий рынок, в свою очередь, требует от производителей все новых разработок.

Камер все больше, рынок все объемнее

Сегодня в тренде видеоаналитика, искусственный интеллект, облачные технологии, Интернет вещей. При этом технологии IoT, похоже, вскоре займут ключевое место на рынке видеонаблюдения. Дело в том, что по прогнозам аналитической компании IHS Markit, к 2021 году общее количество активных устройств для мониторинга и видеосъемки во всем мире превысит миллиард, притом, что вконце 2019 года их число, по различным оценкам, составляло около 770 млн. Все эти устройства генерируют огромные объемы видеоконтента, которые необходимо хранить и обрабатывать, к тому же значительная часть камер уже подключена к различным сетям передачи данных. Таким образом, глобальная инфраструктура СВН огромна и продолжает быстро расти.

По данным IDC, в прошлом году только камер для видеонаблюдения в мире было продано на $23,6 млрд, вместе с тем аналитики отмечают и растущую динамику по сравнению с 2018 годом (конкретные показатели не уточняются). При этом, как известно, со временем стоимость оборудования снижается и рост денежных показателей обеспечен, с одной стороны, за счет увеличения продаж устройств в штуках, а с другой, благодаря тому, что заказчики все чаще предпочитают приобретать оборудование с расширенными интеллектуальными функциями, такими как распознавание лиц и автомобильных номеров, инструменты торговой аналитики и т.д.

В других отчетах отмечается, что около 2/3 глобального рынка в денежном выражении составляют проектные продажи и только 1/3 — потребительские решения. Наиболее крупными региональными рынками для решений СВН в 2019 году были США и Китай. При этом Америка лидирует по финансовым показателям, а КНР — по числу проданных камер. В частности, ресурс *precisesecurity.com* подсчитал, что к концу 2019 года в Китае было установлено более 200 млн камер видеонаблюдения, а в США — «всего» 50 млн. И хотя соотношение здесь вроде бы в пользу КНР, Штаты продолжают лидировать по числу камер на сотню жителей — 15,28 против 14,36 в Китае (в первую пятерку по данному показателю попали также

Соединенное Королевство, ФРГ и Нидерланды). С другой стороны, восемь из десяти крупнейших городов мира с наибольшим количеством установленных камер видеонаблюдения находятся именно в Китае и всего два — Нью-Дели и Лондон, за его пределами.

Кстати, суровое экономическое противостояние между США и КНР, как известно, также распространилось и на системы видеонаблюдения, в результате чего американские федеральные (и некоторые региональные) госструктуры с прошлого года полностью перестали покупать китайские камеры и сопутствующие продукты. Ожидалось, что эта мера ударит по обеим странам. Но как показала практика, глобальных экономических последствий удалось избежать — на стремительно растущем рынке китайские производители быстро переориентировались на внутренний сегмент, а в США освободившееся место заняли как местные вендоры, так и компании из Южной Кореи, Японии, ЕС, причем значительно число из них — это небольшие малоизвестные бренды.

Еще одним свидетельством развития мирового рынка СВН является немалое число различных сделок, связанных с приобретением отраслевых компаний — слияниями и поглощениями. Так, в августе 2020 года известный производитель систем видеонаблюдения Pelco в очередной раз сменил хозяина. На этот раз вендор был продан за $110 млн компании Motorola Solutions, которая уже много лет подряд укрепляет свои позиции на рынке охранных систем.

Напомним, что Pelco перестала быть самостоятельной компанией в 2007 году, когда ее за $1,5 млрд приобрела Schneider Electric, позже, в 2019-м, перепродавшая ее инвестиционному фонду Transom Capital Group. Тогда стоимость сделки не сообщалась, но было известно, что выручка Pelco в 2018 году составила $185 млн и вряд ли бы компанию продали за меньшую сумму, но не прошло года, как и Transom избавился от актива (судя по всему, с ощутимым дисконтом). Возможно, Motorola Solutions сможет вдохнуть жизнь в некогда мощный бренд. Тем более, компания настроена серьезно, и Pelco — не единственная ее покупка в сфере СВН за последнее время. Ранее в 2019 году за $37 млн была куплена британская отраслевая компания IndigoVision, а в 2018-м — известный канадский производитель высококачественных систем видеонаблюдения Avigilon (за $1 млрд).

Примечательным моментом является и то, что на рынок СВН, особенно в массовом сегменте, выходит действительно большой капитал. Как известно, в 2014 году Google приобрела разработчика систем для умного дома Nest, в составе решений которого краеугольным камнем являются «умные» видеокамеры. С тех пор направление активно развивалось, и в 2020 году поисковый гигант сообщил о расширении инвестиций в отраслевые проекты. Так, в августе была заключена сделка с компанией ADT — крупнейшим оператором охранных услуг в США с базой в 6 млн клиентов. В рамках соглашения Google получает 6,6% акций ADT в обмен на $450 млн целевых инвестиций. Обе компании также согласились выделить в будущем по $150 млн каждая на общий маркетинг, разработку продуктов и инвестиции в технологии и обучение сотрудников.

Вместе с тем сама ADT попала в крупный скандал, после того как стало известно, что один из ее сотрудников потенциально мог получить доступ к живому видео и записям сотен клиентов, используя уязвимость в домашней системе видеонаблюдения ADT Pulse. В этой истории примечательно то, что злоумышленник, оставаясь штатным сотрудником ADT, успешно использовал уязвимость в течение семи лет и смог получить полный неавторизованный доступ к охранным системам более чем двухсот домохозяйств. Этот случай, который стал достоянием общественности летом 2020 года, сейчас набирает обороты, и спектр поднимаемых вопросов здесь гораздо шире, чем неудачный опыт одной компании. Речь идет о необходимости глобального пересмотра правил безопасности в эпоху тотальной цифровизации.

Тем не менее сферу домашнего видеонаблюдения поддерживают все больше ИТ-гигантов. Так, компания Amazon, которая в 2018 году приобрела разработчика «умных» видеодомофонов Ring, в 2020 году продолжила развивать тему безопасности жилищ, выведя на рынок миниатюрную FullHD камеру Blink Mini (**рис. 1**) с набором интеллектуальных функций.

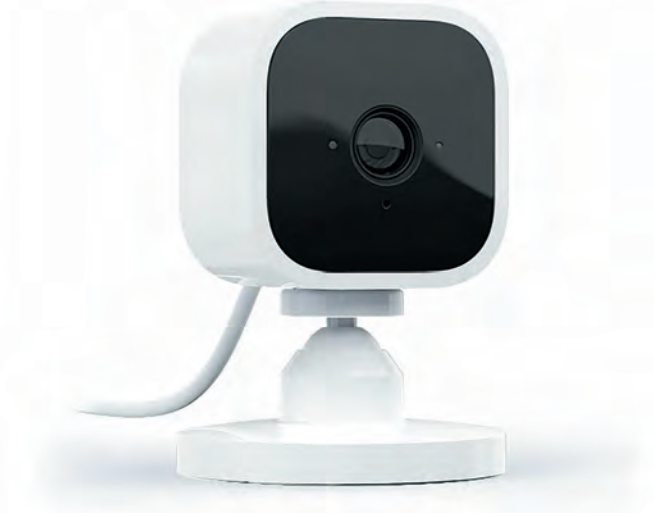

Рис. 1. Новая «умная» FullHD камера Amazon Blink Mini

В целом же, благодаря повсеместному внедрению широкополосной мобильной связи и развитию технологий IoT, сегмент решений СВН для частных домохозяйств и небольших компаний имеет очень большие перспективы развития, ведь камерами уже могут оснащаться буквально все бытовые устройства. Например, в прошлом году на рынке появились даже роботизированные пылесосы с настоящим машинным зрением, есть и другие устройства такого рода. Так что видеонаблюдение всеми силами стремится в дома, а крупные инвесторы и технологические гиганты подталкивают этот процесс. Неудивительно, что данный сегмент растет как на дрожжах — по итогам 2019 года исследователи Strategy Analytics оценили его глобальный объем в $7,9 млрд

и 56 млн проданных устройств, но уже в 2023-м ожидается рост до $13 млрд и 111 млн единиц техники.

Технологии, стимулирующие развитие

Основной тренд на рынке систем охранного видеонаблюдения, который наблюдается в последние несколько лет, состоит в том, что камеры становятся все «умнее». Достигается это, во-первых, за счет более мощных процессоров, устанавливаемых на их борту, а во-вторых — благодаря разработке новых программных алгоритмов, повышающих эффективность видеоаналитики. Отвечая на запрос рынка, ведущие мировые производители начали оснащать все больше моделей камер мощными процессорами, ориентированными на работу с машинным обучением и нейросетями.

Теперь, казалось бы, должна наступить «золотая эра» аналитики на борту, ведь благодаря новым чипам камеры способны выполнять более широкий спектр интеллектуальных функций, обрабатывать больше сцен и т.д. Но тут подоспели другие технологические новшества. Например, все больше производителей переводят свои модели на высокочувствительные матрицы, которые стали массово доступны на рынке благодаря разработкам Sony. Для новых сенсоров подоспели и объективы с увеличенной светосилой (F ~1.0), в числе которых модели от Foctek, Evetar, CWZK. Если же учесть, что все большее число моделей поддерживают формат 4K, то становится очевидным, что объем видеоданных будет расти лавинообразно и резерва мощностей новых чипов, скорее всего, надолго не хватит. Так что серверный подход, при котором аналитическое ПО работает только на центральном видеорегистраторе, также остается актуальным, несмотря на растущую вычислительную мощь камер. Более того, для эффективной и быстрой обработки изображений современные видеосерверы начинают оснащать платами графических ускорителей — GPU (graphics processing unit). Но и по сети передавать растущие объемы видеоданных все сложнее, поэтому растет число моделей камер, использующих кодек сжатия H.265.

Отметим также, что в связи с повсеместным появлением широкополосных сетей мобильной связи четвертого поколения производители выводят на рынок все больше моделей с поддержкой 4G, что открывает дополнительные возможности в области проектирования и построения систем видеонаблюдения, особенно в городах. Как ожидается, еще больше на развитие беспроводных СВН повлияет появление сетей 5G, но это уже перспектива ближайших нескольких лет.

Видеоаналитика в облаке и не только

Системы видеоаналитики можно без преувеличения назвать главным драйвером рынка СВН на сегодняшний день. Долгое время большинство систем видеонаблюдения ограничивались более-менее стандартным набором функций — определение людей в кадре, детекция движения и пересечения условных линий, определение автомобильных номеров и т.д. Другие, более сложные функции, хотя и были номинально доступны, зачастую работали с большой степенью погрешности. Но в последнее время, благодаря усилиям разработчиков алгоритмов машинного обучения и повсеместному распространению видео высокого качества — с разрешением FullHD и выше, — возможности систем видеонаблюдения существенно расширились. Теперь они с вероятностью, близкой к 100%, могут распознавать лица — даже те, которые частично скрыты, например медицинской маской. Существенно повысилась точность распознавания опасных действий, например, драк или попыток нападения с использованием оружия. Буквально до последнего времени камеры, как правило, не могли надежно отличить борьбу от, скажем, дружеских объятий. Как сообщают отдельные производители, данную проблему в основном удалось решить. Так же надежно камеры с аналитикой распознают наличие в руке ножа, палки или пистолета и уже почти не путают их с телефоном или другими бытовыми предметами. Такие технологии уже доступны на массовом рынке, но еще не получили широкого распространения, хотя, как ожидается, на их повсеместное появление уйдет несколько лет.

Интересным направлением научной мысли являются разработки в области т.н. «вычислительной перископии» — когда камера благодаря особым технологиям и алгоритмам может «вычислить», что происходит за преградой (например, за углом). Один из перспективных подходов основан на обработке теней, отброшенных на любую поверхность. Другой использует свойства света — здесь используется специальная «фотонная пушка», которая «обстреливает» пол и стену, расположенные на противоположной стене от угла, за который необходимо «заглянуть». Поток фотонов таким образом огибает непроницаемое препятствие и отражается от объекта, скрытого за стеной (это может быть, например, человек), затем существенно ослабленный пучок фотонов попадает на специальный сверхчувствительный сенсор камеры, преобразующий свет в электрический сигнал за счет явления фотоэффекта. В результате удается получить условное изображение объекта, который скрывается за углом. Во всяком случае, можно понять, насколько он крупный, какой примерно формы, движется ли он или стоит. Специальные алгоритмы позволяют преобразовать полученные сигналы в понятный для человека вид. Но данная технология все еще является экспериментальной и не покидает пределы лабораторий. Хотя, как отмечают эксперты, в случае доведения разработки до коммерческого образца (а для этого есть все шансы) она имеет хорошие перспективы на рынке охранных систем.

Еще один мощный тренд в сфере видеоаналитики — автоматизация процесса управления распределенными системами. Камер становится все больше, и сидеть за монитором, просматривая видео, уже неэффективно. Поэтому все основные разработчики VMS (video management system) оснащают свои решения модулями для выявления опасных и подозрительных ситуаций,

ЛИЦО ПОД МАСКОЙ, ИЛИ ВИДЕОАНАЛИТИКА В УСЛОВИЯХ ПАНДЕМИИ

Одной из важнейших опций, которую предлагают современные системы охранного видеонаблюдения, является возможность распознавания и даже идентификации лиц. Сама идея заявлена довольно давно, однако лишь в последние несколько лет здесь был достигнут ощутимый успех. Теперь камеры с аналитикой способны узнавать людей не только в «тепличных» условиях, но и при умеренно слабом освещении, пониженной видимости и т.д. Не все, не всегда, но лучшие решения в отрасли буквально удивляют своими возможностями. И все бы ничего, если бы не пандемия, которая вывела проблему распознавания лиц на совершенно новый уровень, ведь теперь они зачастую скрыты масками.

Как это отразится на эффективности видеоаналитики? Летом нынешнего года Национальный институт стандартов и технологий США (NIST) обнародовал результаты тестирования 89 систем распознавания лиц на предмет того, смогут ли они опознать человека в медицинской полумаске. Результаты подтвердили опасения исследователей – эффективность всех без исключения решений существенно снижается, а разработчики систем распознавания лиц склонны переоценивать возможности собственных продуктов. Лучшие из протестированных систем выдавали ошибку с вероятностью в диапазоне 5–50% при попытке узнать человека, половина лица которого скрыта.

В ходе тестирования использовалась база из 6 млн изображений, на которые накладывались маски разных цветов и форм. Выяснилось, например, что наилучшие результаты достигаются при использовании круглых масок, а черная маска более сложна для распознавания, чем голубая. Правда, для тестирования брались не люди в реальных условиях, а лишь их фото, но исследователи полагают, что на результаты испытаний это не оказывает критического влияния. Разработчики решений поспешили заявить, что тестировались системы, созданные до пандемии, которые сейчас доработаны (или дорабатываются) с учетом новых обстоятельств.

Например, британская компания Facewatch заявила о том, что у нее уже есть рабочий алгоритм распознавания, для которого достаточно всего лишь области глаз и бровей. Система создавалась еще до пандемии, но сейчас пришлась как раз кстати. О похожих разработках заявили также компании SAFR и Corsight. Но все же большинство отраслевых экспертов пока не верит в высокую эффективность подобных разработок на практике. Время покажет – маски с нами, похоже, надолго. Даже после завершения пандемии многие люди, очевидно, еще долго будут носить их в целях профилактики.

в случае обнаружения которых оператору подается тревожный сигнал. Такой подход позволяет одному человеку осуществлять эффективный мониторинг систем видеонаблюдения, включающих в себя десятки камер. Также повышается результативность модулей работы с видеоархивом, обеспечивающих нахождение требуемых сцен, людей, предметов или заданных транспортных средств в огромных массивах видеоданных без необходимости их полного просмотра — в результате процесс поиска нужной информации сокращается в десятки раз.

Актуальным трендом, правда пока в основном за границей, является развитие VMS из облака, доступ к которой осуществляется по модели SaaS. Такой подход получил название «видеонаблюдение как сервис» — VSaaS. На рынке появляется все больше таких операторов, которые в борьбе за клиента соревнуются не только в цене подключения камер и емкости предоставляемого хранилища, но и стараются обеспечить самые передовые возможности в сфере аналитики, управления сетями СВН и работы с видеоархивом. Кроме того, почти все крупные производители камер видеонаблюдения предлагают в качестве опции собственные VSaaS-сервисы. Если говорить о независимых разработчиках подобных облачных платформ, то, как отмечается в различных отраслевых исследованиях, в 2019 году лидерами здесь были такие компании, как ***Arcules***, ***Eagle Eye***, ***OpenEye***, ***Qumulex***, ***Verkada*** и некоторые другие. Глобальный объем рынка подобных сервисов аналитики оценивают примерно в $800 млн по итогам прошлого года. В этом контексте интересна статистика по смежному рынку — ACaaS (Access Control as a Service — контроль доступа как услуга). Хотя этот сегмент начал развиваться позже VSaaS, растет он очень динамично. Например, аналитики оценили объем мирового сегмента ACaaS более чем в $600 млн по результатам 2019 года, правда, половину этой суммы дал рынок США.

В Украине сегодня доступны различные VSaaS-сервисы, т.ч. от местных операторов. Но особого спроса на них нет, а соответственно, у операторов отсутствует стимул предлагать отечественным заказчикам широкий спектр инновационных технологий в сфере видеоаналитики. Для нашего рынка — это дело будущего.

Распознавание лиц в разных странах — довольны не все

Распознавание лиц, а также идентификация людей — одна из наиболее востребованных сегодня функций аналитического видеонаблюдения. Технологии здесь достигли высокого уровня совершенства, но производители и заказчики столкнулись с другой внезапной проблемой — морально-этического свойства. Оказалось, далеко не все в восторге от идеи, что камера может узнавать человека без его ведома и согласия, особенно в людных местах. И если в государствах с авторитарным стилем управления, таких как РФ или КНР, подобные системы внедряются повсеместно, а их использование одобрено на всех официальных уровнях, то в странах с развитыми традициями демократии все не так однозначно. Например, в начале сентября 2020 года американский Портленд стал первым городом в США, где запретили использование систем распознавания лиц в местах общественного пользования. Уже с начала следующего года все коммерческие и муниципальные организации в городе (включая полицейское управление) должны отказаться от подобных технологий.

Ограничение не распространяется на ряд федеральных структур, которые не подчинены городскому совету, но похоже, это вопрос времени, поскольку, например, недавно на рассмотрение Палаты представителей США поступил законопроект о реформе полиции. В нем, в частности, предусмотрен запрет на использование

федеральными силовыми структурами технологии распознавания лиц, во всяком случае, тех, которые работают в режиме реального времени. Вместе с тем, не дожидаясь решения на уровне центрального правительства, опыт Портленда активно перенимают в других городах США, числе которых Сан-Франциско, Бостон, Окленд, Спрингфилд, Кембридж, Сомервилл и пр.

В августе нынешнего года исторический прецедент был отмечен в Соединенном Королевстве, где Апелляционный суд постановил запретить полиции Южного Уэльса использовать технологии распознавания лиц, поскольку это является нарушением прав человека. Как известно, страны англосаксонской правовой семьи широко применяют принцип прецедентного права, а значит, упомянутое решение, скорее всего, породит множество подобных выигранных исков по всей стране.

Не осталась в стороне и континентальная Европа, где в нынешнем году Еврокомиссия предложила запретить на срок от трех до пяти лет использование технологии распознавания лиц в общественных местах. За это время должны быть выработаны способы предотвращения потенциальных злоупотреблений, доступ к которым открывает применение данной технологии, а также сформированы специальные надзорные органы на уровне стран-членов ЕС. Запрет предлагается распространить на все сферы деятельности, за исключением научных разработок и систем безопасности особо ответственных объектов.

Запрещающие инициативы предпринимаются не только на уровне официальных структур. В игру включились и крупнейшие частные компании. Например, в июне 2020 года компания Amazon заявила о том, что пока не будет поставлять полиции и другим правоохранительным органам США систему распознавания лиц собственной разработки Rekognition. Исключения сделаны для организаций, которые используют распознавание лиц в целях борьбы с незаконным трафиком людей и для поиска пропавших детей. Как сообщают некоторые издания, в Amazon считают, что использование систем распознавания лиц американским правительством подпадает под определение нарушения прав человека.

В свою очередь, компания IBM вообще решила уйти с рынка систем распознавания лиц, соответствующее заявление сделал глава IBM Арвинд Кришна. Как сообщает ряд СМИ, такое решение было принято в связи с интересом силовых структур США к технологиям распознавания лиц на фоне массовых демонстраций, охвативших страну весной и летом нынешнего года.

Дроны, роботы, IoT

Видеонаблюдение становится повсеместным. Кроме традиционных стационарных камер, в СВН все чаще используются мобильные устройства. Речь не только об автомобильных видеорегистраторах или полицейских моделях, закрепляемых на одежде; элементами системы видеонаблюдения, особенно в городах, сегодня становятся дроны и роботы. Последние, правда, пока экзотика и встречаются только в крупных зарубежных универмагах, вроде Walmart, международных аэропортах и на некоторых других объектах. А вот летающие дроны, оснащенные набором камер, уже сегодня активно помогают силовым структурам по всему миру, не исключая нашу страну. Сегодня на рынке присутствует большое количество различных летающих, радиоуправляемых и автономных дронов, список моделей постоянно расширяется.

Хороших успехов в этом направлении добилась компания Amazon, которая, как известно, продвигает идею использования летающих дронов для автоматизированной развозки заказов (**рис. 2**).

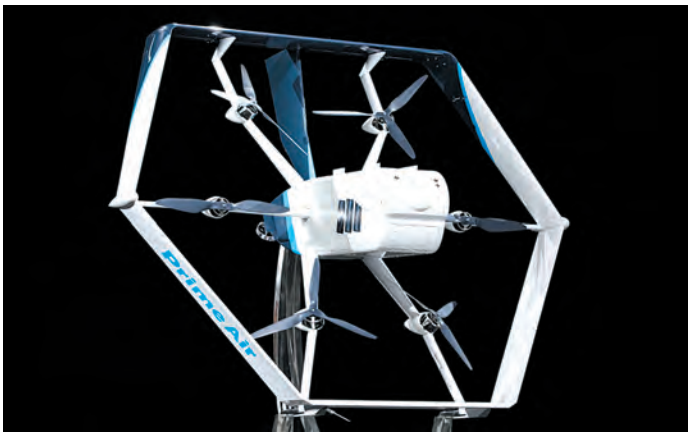

Рис. 2. Новый дрон-доставщик Amazon способен также выполнять функции охраны территории

Базовые требования включают возможность доставки до 2 кг грузов на расстояние до 25 км не более чем за полчаса. Летом прошлого года была представлена очередная версия аппарата, оснащенного системой камер и электронным блоком для машинного обучения. Такой дрон способен облетать препятствия и отличать предметы от живых существ. Все это является полезным в сфере охранного видеонаблюдения, поэтому компания позиционирует аппараты и как платформы безопасности, способные осуществлять патрулирование заданных зон с воздуха. Дрон Amazon может совершать наблюдение как днем, так и ночью, а опциональный массив микрофонов позволяет выявлять подозрительные звуки — крики о помощи, выстрелы, звон разбитого стекла и т.д. На устройство и технологии, заложенные в нем, даже был получен патент, выданный американским патентным бюро в июне 2019 года.

Еще одно интересное применение дронов, ставшее актуальным в условиях карантинных ограничений, — массовый термометрический контроль температуры тела людей и надзор за соблюдением социальной дистанции. Такие решения используются в США, КНР, Саудовской Аравии и других странах. Например, в некоторых регионах Италии полиция использует китайские БПЛА DJI Mavic 2 Enterprise Dual (**рис. 3**) с функцией дистанционного измерения температуры — при выявлении подозрительного субъекта его задерживают и производят контрольный замер ручным пирометром. При этом у дрона есть встроенные динамики, посредством которых полицейские могут обратиться к «подозреваемому» или прохожим.

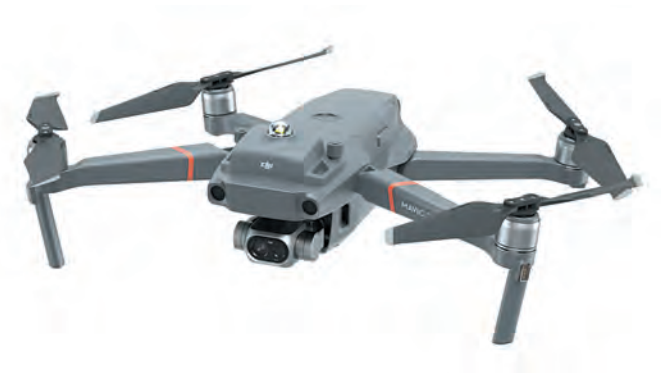

Рис. 3. Дроны DJI Mavic 2 Enterprise Dual, оснащенные тепловизором, используют итальянские полицейские для термометрического контроля населения в отдельных регионах страны

В отдельных регионах США с аналогичной целью используются БПЛА местной компании Draganfly. А в Китае вообще дошли до того, что дроны этаж за этажом облетают многоквартирные дома, и контролируют температуру находящихся там жильцов — для этого, естественно, требуется, чтобы обитатели квартиры открыли окно и позволили провести измерение, но никто, как правило, не отказывается.

Остается лишь предполагать, насколько точными являются подобные измерения, проведенные с большого расстояния в изменяющихся условиях окружающей среды, искаженные к тому же влиянием самого дрона, двигатели которого генерируют тепло, а пропеллеры охлаждают воздух.

Сегмент СКУД растет, но медленнее, чем СВН

Касаясь вопросов, связанных с обеспечением технической безопасности с помощью видеонаблюдения, сложно обойти тему систем контроля доступа. Эти два направления, которые длительное время развивались параллельно, сейчас год от года все теснее сближаются. Например, классический элемент СКУД — терминал доступа, или домофон, уже почти повсеместно, если мы говорим о современных моделях, оснащается видеокамерой, программным обеспечением для распознавания лиц и другими возможностями, которые ранее были характерны только для СВН. Иными словами, системы безопасности становятся все более и более интегрированными на базе цифровых технологий и протокола IP.

Тем не менее, если верить данным отраслевых аналитических отчетов, то рынок СКУД растет не столь быстро, как СВН, и объем его меньше. Так, MarketsandMarkets оценивала данный сегмент примерно в $8,1 млрд с перспективной увеличения до $12,1 млрд в 2024 году. Это обозначает, что средний прирост составляет около 8,5% в год. Аналитики ставят в первую очередь на развитие облачных сервисов (ACaaS), мобильных платформ, технологий IoT и все более широкое использование беспроводных технологий (в т.ч. LTE, 5G, Wi-Fi). Кроме того, СКУД все чаще интегрируются с другими системами физической безопасности и автоматизации зданий (BAS), что сегодня является общим требованием к комплексам безопасности. В последнее время возрастает спрос на решения для контроля доступа, которые будут использоваться в системах управления помещениями.

Показательным примером интеграции различных технологий, которые номинально даже не связаны со сферой СКУД, является технология WiFi Motion, созданная компанией Cognitive Systems. Она позволяет использовать Wi-Fi-устройства, находящиеся внутри помещения, в качестве детекторов движения. В основе разработки лежит понимание того, что люди, которые перемещаются внутри здания, вносят определенные возмущения в пространственную картину покрытия радиосигнала Wi-Fi. Система улавливает эти изменения и преобразует их в понятные для человека сигналы. Примечательно здесь то, что детектором может стать любое бытовое Wi-Fi-оборудование, включая то, что уже установлено у пользователя. Все, что требуется приобрести, — это маршрутизатор Wi-Fi и пакет прикладного ПО. Соответственно, затраты на создание системы безопасности будут минимальными.

3D ПЕЧАТЬ ПОМОЖЕТ ЗЛОУМЫШЛЕННИКАМ?

Самым популярным типом биометрических систем доступа в мире остаются различные варианты сканеров отпечатка пальца. Технологий реализации подобных устройств существует несколько, но, естественно, наибольшим спросом пользуются самые простые решения. И хотя в целом они достаточно надежны, со времени их появления не иссякает поток желающих обмануть систему идентификации. Очередная, и весьма успешная, попытка была предпринята в 2020 году исследовательницей и экспертом в области систем технической безопасности Ямилой Левалье из Аргентины.

Не мудрствуя лукаво, она решила имитировать папиллярный рисунок пальца, создав муляж на 3D-принтере. И эксперимент удался – на фальшивый «палец» биометрический сканер (модель которого не называется) реагировал так же, как и на настоящий. Процесс создания подделки состоял из нескольких этапов. На первом камерой высокого разрешения был сделан снимок реальной подушечки пальца. При этом имитировались реальные условия скрытой съемки, и фотография вышла размытой. Затем для повышения четкости изображение было обработано с помощью общедоступных программных инструментов для работы с графикой. На основе улучшенного снимка исследовательница создала объемную модель и распечатала ее на обычном бытовом 3D-принтере Anycubic Photon. Главным условием для устройства было поддержка разрешения на уровне 20–60 микрон, поскольку именно в этом диапазоне колеблется глубина линий папиллярного узора пальцев. Указанная модель обеспечивает разрешение в 25 мкм. На создание рабочего муляжа потребовалось много времени и более десяти попыток, но все же реалистичный образец в итоге был создан.

Описывая эксперимент, Ямила Левалье заключает, что технология создания подделки оказалась весьма непростой, потребовала много сил, времени, знаний и навыков, а также специального оборудования. Вряд ли она подойдет для массового использования злоумышленниками, но даже потенциальная возможность производства эффективного муляжа одним человеком в бытовых условиях должна подтолкнуть организации к тому, чтобы подвергнуть ревизии собственные биометрические СКУД – обновить технологии, политики доступа, алгоритмы работы и т.д.

Возвращаясь к рыночным тенденциям, стоит отметить, что несмотря на появление новых технологий, сегмент СКУД отличается высокой консервативностью. Скажем, до сих пор во всем мире традиционные считыватели смарт-карт остаются самым популярным вариантом условного доступа, несмотря на развитие инновационных решений вроде биометрических систем. Последние, конечно, также вызывают интерес, их становится больше, но все же они еще не делают погоды на рынке. Поэтому традиционные считыватели останутся с нами еще на долгие годы. В региональном разрезе без сюрпризов: крупнейший рынок — это США, самый быстрорастущий — КНР. Как ожидается, к 2023–2024 годам их объемы должны примерно сравняться.

Ведущими мировыми производителями решений СКУД по итогам 2019 года, согласно данным MarketsandMarkets, являлись такие бренды, как ***Assa Abloy***, ***Johnson Controls***, ***Nedap***, ***Allegion***, ***Gemalto***, ***dormakaba Holding***, ***Bosch Security Systems***, ***Honeywell Security Group***, ***Identiv***, ***Suprema***. Последняя компания, представляющая Южную Корею, — единственный представитель Азии в ТОП-10. В то же время китайские компании, особенно Hikvision и Dahua, стремительно наращивают долю рынка и вскоре, как ожидается, могут войти в число лидеров. Из европейских компаний сектора СВН наиболее заметную динамику в развитии направления СКУД демонстрирует ***Axis***.

Тепловизоры в условиях COVID

Одним из наиболее интересных трендов 2020 года в сфере СВН стала растущая роль тепловизионных решений, которые все чаще применяются на различных объектах для выявления людей с подозрением на COVID-19. Собственно, метод «выявления» только один — контроль температуры тела: если она превышает определенный предел (обычно, выше 37 °С) — это уже повод присмотреться к человеку повнимательнее или вовсе не пустить его в помещение. Об эффективности подобных решений ведутся горячие споры с самого начала пандемии. И это при том, что впервые использовать тепловизоры для массово термометрического контроля в местах скопления людей начали еще в 2003 году во время эпидемии атипичной пневмонии (SARS) в Китае. Но, несмотря на, казалось бы, солидный срок существования метода, до сих пор не удалось найти ни одного открытого научного источника, где подтверждалась бы эффективность применения тепловизоров для выявления повышенной температуры человека. Отсутствуют и какие-либо результаты серьезных тестов, проведенных признанными международными некоммерческими организациями. Зато имеется немало сведений от самих производителей и изрядный багаж частных случаев, но и здесь нет единства — кому-то подошло, кому-то нет. В общем, однозначности в данном вопросе пока не видно, равно как и общепризнанной объективной методики тестирования или мировых стандартов для проверки подобных тепловизионных измерений.

Тем не менее на сегодняшний день решения для бесконтактного термометрического контроля на основе тепловизоров предлагают десятки компаний. Учитывая узость задачи, зачастую параметры большинства разработок очень близки, например, погрешность измерения составляет 0,5 °С без калибратора и 0,3 °С при его использовании. При этом автоматическая настройка точности может осуществляться как с помощью специального устройства, т.н. модели абсолютно черного тела (это самый распространенный подход), так и без него — за счет фирменных ноу-хау (такое решение есть, например, у FLIR). Тепловизоры могут быть как ручными, так и стационарными, в виде специальной камеры, устанавливаемой на стене, потолке или переносном штативе. В последнем случае термочувствительный и оптический сенсоры могут объединяться в одном корпусе, и тогда речь идет о уже биспектральной камере (**рис. 4**).

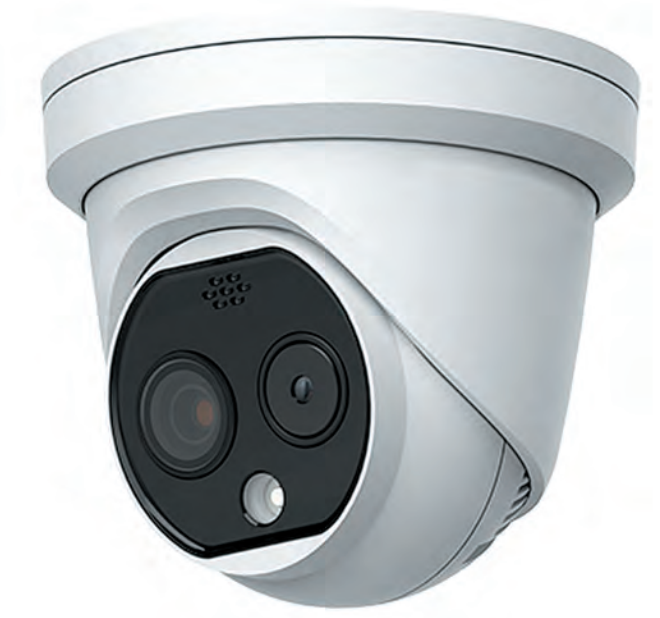

Рис. 4. Биспектральная камера с набором специального ПО — наиболее функциональное и эффективное решение для организации термометрического контроля людей на различных объектах

Это наиболее функциональное решение, которое, при наличии специального программного обеспечения может также реализовать возможность распознавания лиц, что позволяет сделать такое устройство важным элементом СКУД.

Все решения такого рода следует использовать только внутри зданий и желательно при максимально стабильных параметрах воздуха в помещении. Измерения температуры входящих людей рекомендуется проводить по очереди. Но некоторые производители декларируют высокую эффективность даже для движущейся массы людей (например, в метро или на массовых мероприятиях), заявляя о том, что их решения могут делать до нескольких десятков замеров в секунду, безошибочно определяя лица в толпе. Но в целом фактических различий между предложениями различных производителей не слишком много, во всяком случае в аспектах, касающихся функциональности. Тем не менее, несмотря на всю неоднозначность с определением эффективности подобного подхода,

за границей, особенно в Китае, ЕС, Британии, США и ряде других экономически развитых стран, тепловизоры активно применяются для термометрического контроля на самых разных объектах: аэропортах, железнодорожных станциях, круизных лайнерах, при входе в универмаги и ТРЦ.

Проекты такого рода есть и в Украине — автору статьи лично доводилось видеть термометрические системы на основе тепловизоров, установленные в бизнес-центрах и на входах в офисы крупных компаний, в т.ч. за пределами столицы. Но больше всего шума наделала попытка киевских властей провести масштабную закупку термометрических решений для борьбы с распространением COVID-19. Напомним, в апреле 2020 года одна из структур КГГА — КП «Информатика» — решила купить без тендера 400 термометрических комплектов Hikvision на основе тепловизоров. Заявленная стоимость проекта составила почти 65 млн грн, и если бы его удалось реализовать — это было бы одно из крупнейших подобных внедрений в континентальной Европе на тот момент. Но этот спорный по своей полезности проект вовремя завернула Государственная аудиторская служба, которая выявила нарушения в процессе проведении закупки. Договор о поставке был расторгнут, а новых попыток решили не осуществлять.

В целом же нынешняя пандемия заметно активизировала сегмент тепловизионных решений, которые теперь прочно заняли новую нишу.

Сегодня технологии охранного видеонаблюдения переживают новый виток технологического развития. Если на предыдущем этапе все производители соревновались в разрешении матрицы и качестве изображения, то сегодня основной акцент сместился в область программного «интеллекта», и такое положение, надо сказать, вполне способно повлиять на изменение баланса рыночных сил. Поскольку европейские, американские и японские компании имеют очень сильные позиции в сфере разработки ПО, что может позволить им отвоевать существенную часть рынка у азиатских брендов в течение ближайших нескольких лет. С другой стороны, и китайцы не сидят сложа руки, более того, они не ограничены многими юридическими препонами, связанными с отношением к правам человека, характерными для США и ЕС. Это дает возможность местным разработчикам совершенствовать технологии, запрещенные в демократических странах, но востребованные на рынке. Как бы то ни было, все это стимулирует развитие технологий видеонаблюдения, предела потенциальным возможностям которых пока не видно.

Игорь КИРИЛЛОВ, **СиБ**

ХРОНИКА

IBM Think Digital Summit — форум инноваций снова в Киеве… на этот раз онлайн

В нынешнем году пандемия «уханьского вируса» внесла существенные коррективы в планы многих компаний. Коснулась проблема и сферы популярных мероприятий. На этот раз традиционный киевский форум IBM Think Digital Summit состоялся ***17 сентября 2020 года*** в режиме онлайн.

Тем не менее на условной территории «виртуальной» площадки конференции гости мероприятия смогли прослушать выступления известных экспертов ИТ-отрасли, посетить тематические сессии, пообщаться с коллегами и представителями производителя. В общем, организаторы сделали все, чтобы максимально приблизить онлайн-формат к личному общению.

В числе наиболее обсуждаемых вопросов, которые рассматривались во время IBM Think Digital Summit, можно отметить повышение надежности ИТ-инфраструктуры и обеспечение непрерывности бизнеса, трансформацию корпоративных технологий для сохранения конкурентоспособности, защиту организаций от различных киберугроз. И, конечно же, было рассказано о том, как новейшие технологии в сочетании с отраслевой экспертизой IBM могут ускорить внедрение передовых стратегий для коммерческих и государственных организаций.

В нынешнем году форум был разделен на четыре тематических потока (т.н. «кампуса»): Облачные технологии и искусственный интеллект, Кибербезопасность, Инфраструктурные решения, а также сессия для разработчиков.

В кампусе «Путешествие в Облака» много говорили о нюансах использования частных, публичных и гибридных облаков. Докладчики снабжали выступления не только технической информацией, но и множеством интересных примеров организаций, которые

успешно достигают своих бизнес-целей, используя различные облачные стратегии.

Сессия, посвященная кибербезопасности, также была наполнена практическими примерами – своим опытом реализации систем защиты данных на базе продуктов IBM поделились некоторые украинские интеграторы: «Свит ИТ», IT Specialist, «РДТЕХ». Кроме того, о взаимодействии между корпоративными подразделениями ИТ, ИБ и внешними поставщиками услуг в рамках проекта построения SOC рассказал представитель АО «Концерн Галнафтогаз».

В программе докладов об инфраструктурных решениях присутствовали как традиционные для IBM темы – мейнфреймы и серверы для критически-важных сервисов, так и выступления, посвященные облачным услугам. Например, созданию резервных вычислительных узлов корпоративных ИТ-инфраструктур на внешних площадках IBM.