Время возводить стены

Системы охраны периметра — вещь относительно консервативная. Но прогресс проникает и туда: видеоаналитика, машинное обучение, роботы — все это уже сейчас можно встретить на страже частной собственности.

В нашем неспокойном мире многим нужны крепкие заборы. «Европейский вал», «стена Трампа» — мир снова, как между мировыми войнами, покрывается сетью укреплений. Физическая защита востребована, а вместе с ней — решения, призванные выявить нарушителя, желательно еще на подступах к охраняемой территории.

Для ***систем охраны периметра*** (***СОП***) разработано большое количество типов устройств, реагирующих на попытки несанкционированно проникнуть на территорию, в том числе разрезав ограждение или подкопавшись под него. Различаются они и по принципу работы: есть датчики радиоволновые, вибрационные, емкостные, лучевые и т.п., а разнообразие внешнего исполнения позволяет интегрировать их в дизайн ландшафта либо вовсе скрыть. Комплексные периметральные решения могут работать совместно с другими системами (видеонаблюдения, контроля доступа, пожарной сигнализации).

Родственные системы охраны дома также включают в себя разнообразные устройства: датчики движения, разбития стекла, открытия дверей и окон, извещатели, сигнализирующие о попытках вырезания и сверления, и многое другое.

«СиБ» разбирался, какие периметральные системы можно встретить в Украине и каких уровней достигло развитие охранных технологий в мире.

Рынок СОП

В мировой практике собственно решения для охраны периметра и видеонаблюдения объединяются в один класс решений — PIDS (Perimeter Intrusion Detection Systems — дословно системы обнаружения проникновения через периметр). Согласно прошлогоднему исследованию ***Markets&Markets***, объем рынка этих систем в 2018 году оценивался в $10,74 млрд, а к 2023-му он должен увеличиться до $21,75 млрд при среднегодовом приросте на уровне 15,2%. В свежем отчете ***Global Industry Analysts***, который вышел в октябре, прогнозируется, что до 2025 года этот рынок будет расти со среднегодовой скоростью 15,5% и за это время увеличится на $19,3 млрд. Infoholic Research прогнозирует среднегодовой рост мирового рынка СОП свыше 11% до 2025 года. Наконец, еще один отчет, от ***Future Market Insights***, дает долгосрочный (до 2028 года) прогноз роста рынка СОП, который должен вырасти совокупно на $25,679 млрд. Из них сегмент систем, монтируемых на заграждение, даст $7,495 млрд, также значительно вырастут продажи подземных систем.

Фактором роста названы возросшая террористическая активность, соответствующий рост государственного финансирования и увеличение спроса на системы охраны периметра объектов транспортного сектора, таких как аэропорты и железные дороги. Также на прогнозы влияет увеличивающийся спрос на системы видеонаблюдения с удаленным доступом, повышение расходов на защиту критической инфраструктуры со стороны государств и частных предприятий, ужесточение регуляторных требований относительно периметральной защиты. Именно в силу последнего наибольший рост ожидается в Азиатско-Тихоокеанском регионе, тогда как самым крупным рынком СОП остается Северная Америка, что связано с появлением там технологических решений нового поколения.

«Безопасность периметра сейчас приобрела гораздо большее значение для объектов критической инфраструктуры, таких как коммунальные предприятия, транспорт, государственные органы и оборонные объекты. Это связано с возросшим количеством угроз, способных нарушить работу данной инфраструктуры и вылиться в огромные потери для всей экономики», — отмечает компания ***Memoori Research*** в прошлогоднем отчете, посвященном рынку физической безопасности. Главным драйвером роста отчет называет увеличение инвестиций в промышленность стран Азии и БРИКС.

Анатомия безопасности

Система охраны периметра зачастую представляет собой комплексное решение, интегрированное с видеонаблюдением, системами контроля доступа, освещения, связи. Собственно периметр являет собой первую линию обороны объекта, которая может дополняться защитой отдельных зон и расположенных на территории этого объекта зданий, вплоть до каких-то особо важных помещений внутри последних (концепция концентрических колец обороны). В зарубежной литературе цели периметральной защиты формулируются как «4D»: Deter, Detect, Delay & Deny entry (отогнать, обнаружить, задержать, не пустить).

Цели периметральной защиты формулируются как «4D»: Deter, Detect, Delay & Deny entry (отогнать, обнаружить, задержать, не пустить)

Для этой цели используются сенсоры разной конструкции и назначения. Одни из них монтируются на ограждение, другие закапываются в землю, есть и отдельно стоящие устройства (например, ИК-барьеры).

Одно из широко применяемых решений — ***датчики на основе вибрационного кабеля***, в котором при механическом воздействии индуцируется напряжение. В качестве примера можно назвать ***FlexZone*** (**рис. 1**) — разработку канадской фирмы ***Senstar***, которая входит в состав израильской компании ***Magal Security Systems***. Эта система определяет место вторжения на расстоянии до 600 м от контроллера с точностью до 3 м, выявляет попытки вскарабкаться на ограждение, приподнять или перерезать его. Также возможно выявление нескольких вторжений на расстоянии до 15 м. Данные от каждого процессора передаются по одному и тому же кабелю. Недавно FlexZone появилась в ассортименте компании ***«Юго-Запад»***, она уже установлена в одном из украинских аэропортов, сейчас в работе еще один.

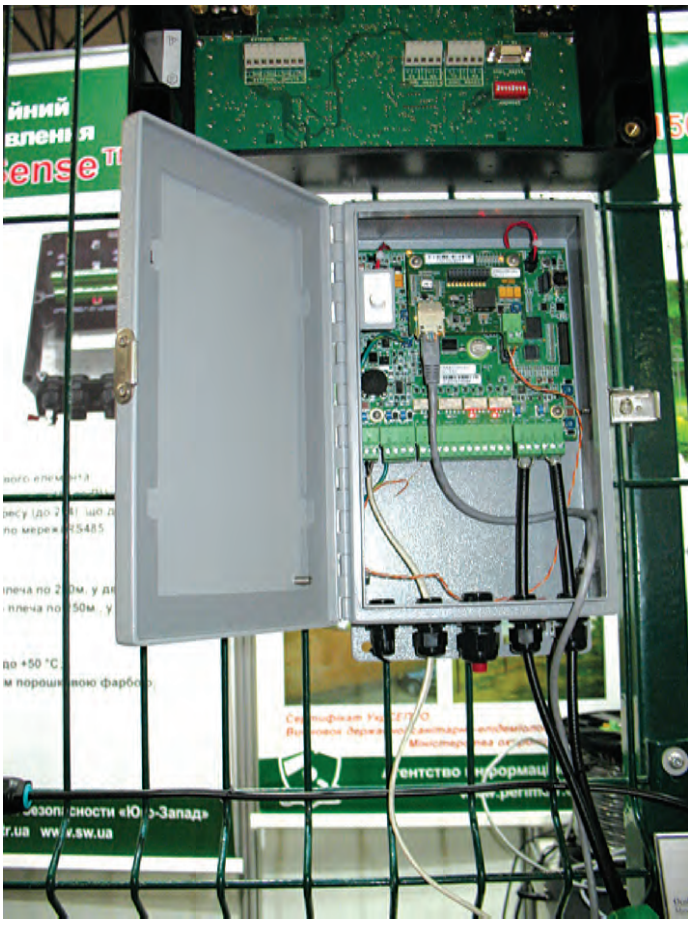

Рис. 1. Контроллер FlexZone (стенд «Юго-Запад» на выставке Expert Security 2019)

Сейчас все большую популярность приобретают ***вибрационные системы на основе волоконно-оптического кабеля***. Они работают на десятки километров без какого-либо активного оборудования, однако из-за стоимости центрального контроллера их рационально использовать на объектах с периметром большой протяженности (таких как военные базы и нефтепроводы). В США сейчас есть интерес к сенсорам на базе ВОК для охраны границ и выявления нелегальных мигрантов, пытающихся пересечь кордон по земле или через подкоп. Для этого как раз нужны детекторы, которые могут быть размещены скрытно и работают на экстремально длинных дистанциях. Как пример можно привести семейство решений ***Fiber SenSys*** (бренд японской компании ***Optex***), **PeriGuard** (Австрия), китайскую ***Raycom*** (их система ***RF900*** недавно появилась у «Юго-Запада»).

Альтернатива сенсорному кабелю — ***микроконтактные пьезоэлектрические датчики***, преобразующие механические колебания в электрические сигналы. В Украине можно встретить систему **Peridect** чешского

производителя ***Sieza***, представителем которого является компания ***«Центурион»***. Система доступна в двух вариантах: Perident и Perident+, которые отличаются максимальным количеством датчиков. Каждое устройство покрывает секцию забора длиной 3 м, при этом анализатор обрабатывает данные от двух соседних датчиков, что уменьшает число ложных срабатываний. Сами датчики предлагаются в разном исполнении, в том числе для скрытой установки в столбах ограждения (**рис. 2**) и герметичные (для размещения под землей). Система установлена, среди прочего, в аэропортах «Львов» и «Борисполь», на нескольких АЭС, в коттеджном городке Green Hills под Киевом.

Рис. 2. Датчик Perident для скрытой установки (стенд «Центурион» на выставке «Безпека-2019»)

Добавляем видео

СОП и видеонаблюдение не зря записывают в один класс решений. Обе системы зачастую дополняют друг друга, создавая синергию. С одной стороны, это позволяет разгрузить операторов СВН, которые получают оповещения от периметральных датчиков, с другой — решает проблему ложных срабатываний самих детекторов и дает возможность сразу оценить степень угрозы.

В интегрированной системе охраны периметра при поступлении сигнала от датчика на тревожный монитор выводится изображение с ближайшей камеры. Как вариант подается команда направить поворотную камеру в место срабатывания и начать запись фрагмента тревоги. Также может включиться звуковая сигнализация. В результате сотрудник сразу видит, что на самом деле произошло: попытка вторжения на территорию или реакция на животное. Последующий анализ записи инцидента позволяет не только установить личности нарушителей, но и оценить действия службы охраны при реагировании на инцидент.

Существуют разные методы интеграции систем, самый простой и дешевый — объединение через платы ввода-вывода или интерфейсные модули. Этот вариант имеет свои недостатки, прежде всего ограниченность количества портов и возможностей программирования типовых реакций. Соответственно он и имеет ограниченную сферу применения: для небольших объектов, а также там, где системы уже установлены и задача интеграции возникла позже. Кроме того, данный способ может быть единственным, если на объекте установлена какая-то редко встречающаяся система.

Более сложный сценарий — бесшовная интеграция датчиков в управляющее ПО СВН по открытым протоколам. Это вариант для крупных систем с единым интерфейсом управления, где основную роль играет видеонаблюдение. Некоторые производители предлагают такую опцию — например, у упоминавшейся компании Senstar она имеется в системе видеоуправления Symphony.

Есть и обратная возможность — интеграция видеокамер в СОП через API, она необходима в случаях, когда необходимо работать с большими картами (например, охрана трубопроводов). Здесь само количество камер может быть слишком большим, чтобы операторы могли за всеми следить, да и основная задача у них может быть иной (наблюдение за технологическими процессами). Поэтому основная информация приходит от датчиков сигнализации, камеры же используются для верификации событий. Из последних новостей — уже упоминавшаяся компания Sieza реализовала интеграцию со своей периметральной системой Perident+ роботизированных камер компании ***Partizan Security*** (известной также своим облачным сервисом хранения для систем видеонаблюдения). Результат — при выявлении вторжения внешняя камера автоматически наводится в указанный сектор для идентификации источника тревоги. Интеграция возможна как на базе программной платформы Sieza C4, так и непосредственно в блоках Perident+.

Наконец, бывают ситуации, когда на одном сервере устанавливаются обе системы (периметральная и видеонаблюдения), которые интегрируются с помощью средств разработки (SDK) от производителей.

Тренды защиты

В сфере охраны физического периметра нет такого противостояния «снаряда и брони», как в киберпространстве, где обе стороны постоянно изощряются в новых приемах. Однако и здесь появляются инновации, направленные на то, чтобы (в разных сочетаниях) повысить эффективность защиты, автоматизировать ее, уменьшить нагрузку на персонал, снизить стоимость.

В прошлом году сайт ***Security Infowatch*** опросил экспертов в области охранных систем относительно того, какие новые технологии и подходы, которые найдут или уже находят применение в периметральной защите. Один из них — ***использование искусственного***

интеллекта и машинного обучения, которые проникают и сюда. ИИ позволяет системам охраны периметра адаптироваться к разным средам и более точно отличать реальные попытки проникновения от ложных срабатываний, вызванных погодными явлениями, животными и т.д. «*Современная компьютерная техника со все возрастающей вычислительной мощностью увеличила возможности высокопроизводительных PIDS-систем, таких как сенсоры на базе когерентного OTDR-рефлектометра, где нужно в реальном времени анализировать большие объемы данных*», — приводит сайт слова Эрика Рейнолдса, вице-президента австралийской компании ***Future Fibre Technologies***, которая использует ИИ в своих решениях на базе ВОК.

Другим трендом является ***совместное использование нескольких технологий***. Например, в одном из проектов компания Senstar развернула для защиты периметра крупного аэропорта комбинированное решение из закопанного радиочастотного кабеля и смонтированного на ограждении ВОК. Это позволило существенно снизить частоту ложных срабатываний из-за прохожих и общественного транспорта; скажем, система игнорирует людей, прислоняющихся к забору в ожидании автобуса. Об интеграции СОП и видеонаблюдения уже говорилось выше, но применение видеоаналитики открывает еще более широкие возможности: например, слежение за людьми и автомобилями на объекте и вокруг него, распознавание номеров для внесения их в черные или белые списки.

Растущий тренд — системы, позволяющие защищать протяженные периметры с использованием одного контроллера, что снижает расходы на развертывание СОП и избыточное перекрытие зон. Также это позволяет расширить охраняемую территорию.

Сайт ***Asmag*** приводит еще несколько мнений. В частности, серьезно изменят индустрию интеллектуальные системы освещения периметра. Фонари, установленные вдоль ограждения, обеспечивают подсветку для камер наблюдения, а встроенные акселерометры фиксируют попытки перерезать или приподнять ограждение либо перелезть через него. При этом LED-светильник может использоваться и для отпугивания — резкое увеличение интенсивности или включение стробирующего света даст понять нарушителям, что они обнаружены, их местоположение известно и, вполне возможно, идет видеозапись.

Для удаленных объектов, таких как телекоммуникационные мачты и маленькие подстанции, нужны одиночные датчики — как вариант, с питанием от солнечных батарей, — которые передают информацию по GSM.

Опрошенные эксперты отмечают возрастающее проникновение IP-систем и устройств с поддержкой PoE. Они сокращают потребности в прокладке труб и проводки, а также время монтажа и общую стоимость проекта. Однако есть и обратная сторона: сам физический периметр теперь может быть подвержен кибератакам.

Memoori в своем прошлогоднем отчете обращает внимание на еще одну тенденцию — рост популярности ***радарных систем***. Эти устройства могут использоваться как на периметре, так и внутри зданий для выявления нарушителей. Компания называет двух производителей, которые специализируются в данной сфере: ***Blighter Surveillance Systems*** и ***Navtech Radar***, оба с британской пропиской. Например, Blighter использует в своих решениях твердотельные пассивные электронные сканирующие решетки (PESA), технологии непрерывного излучения с частотной модуляцией (FMCW) и доплеровского анализа. Лазерные радары есть у ***Optex***; эти устройства обслуживают четыре независимых зоны и могут использоваться как на периметре, так и внутри здания. Радар-детектор, дополняющий систему видеонаблюдения, есть у ***Axis***.

Есть и более экзотические варианты. Например, американская компания ***Flir Systems*** предлагает ***комбинацию радара и тепловизионных камер***. Первый обеспечивает быстрое обнаружение на дальних подступах, но генерирует большое количество ложных срабатываний из-за листвы, животных и других факторов. ИК-камеры обеспечивают верификацию событий. Они могут детектировать цели на расстоянии до километра, что хорошо сочетается с «дальнобойной» радарной системой, а кроме того, работают в условиях, где камера видимого спектра не поможет (ночью или, наоборот, при яркой подсветке сзади). Как только радар обнаруживает движение, ИК-камера автоматически поворачивается в нужную сторону и наводится на нарушителя, так что оператор может следить за ним. Добавление еще и обычных камер с аналитикой дополнительно обеспечивает идентификацию нарушителя.

Люди и роботы

Для охраны периметра также привлекаются люди, которые обходят его пешком и следят за порядком. Охранники пользуются радиостанциями с некоторыми специализированными функциями: прямая связь при выходе за пределы зоны покрытия ретранслятора, «lone worker» (пользователь должен периодически сигнализировать, что все в порядке, иначе рация блокируется), «man down» (устройство отправляет сигнал тревоги, если длительное время пребывает в горизонтальном положении). Также должна быть кнопка для передачи сигнала тревоги. Производители предлагают всепогодные выносные динамики-микрофоны, которые не только освобождают руки при работе с радиостанцией, но и обеспечивают громкий звук даже в сильно зашумленной обстановке.

Людей можно заменить роботами-обходчиками, которые фактически являют собой передвижные устройства видеонаблюдения. Для своей работы они требуют беспроводного покрытия и наличия зарядных станций вдоль маршрута, но зато освобождают персонал от рутины, особенно когда патрулирование затруднено погодными условиями.

Еще в 2014 году Senstar представила автономное решение ***RoboGuard***. Этот робот передвигается по монорельсу вдоль ограждения и может работать в двух режимах: патрулирование (рутинный осмотр на предмет дыр и подозрительных предметов) и реагирование, когда автомат быстро направляется к месту тревоги. Заряда батареи хватает на 1 км пути.

Американская компания ***SMP Robotics*** выпускает серию колесных роботов S5, есть там и вариант для патрулирования периметра (**рис. 3**). Машина оснащена камерами, обеспечивающими круговой обзор, и может работать до 12 часов без подзарядки. Данные передаются по Wi-Fi, также есть встроенный рекордер для записи видео, если робот выезжает за пределы зоны покрытия. Как и RoboGuard, S5 может направляться в нужную зону при срабатывании датчика или по команде оператора. Если робот подтвердит, что тревога не ложная, оператор вышлет туда группу охраны.

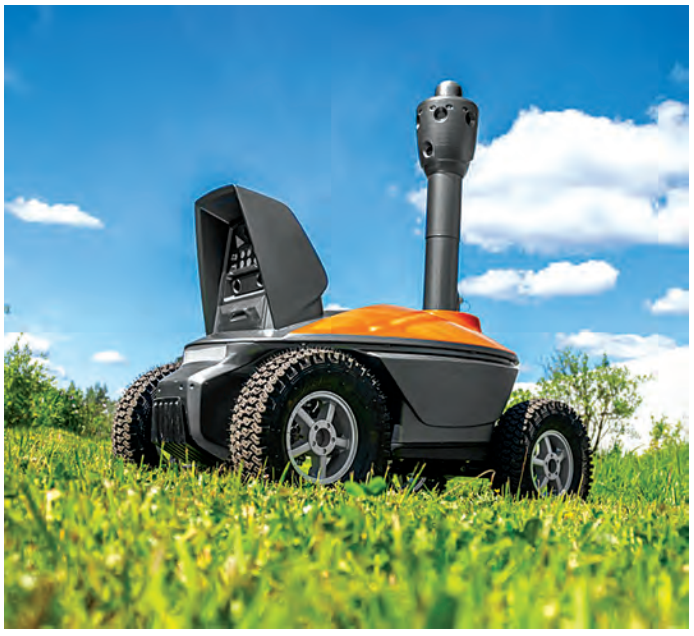

Рис. 3. Робот-патрульный S5

Китайская компания ***Xinhengjia*** разработала семейство роботов DEFA, предназначенных в том числе и для патрулирования периметра. Шестиколесная машина может передвигаться по неровной местности, имеет гибкую «шею», которая может менять высоту с 80 до 150 см, и способна автономно работать до 24 часов. Также на борту есть оборудование голосовой связи. Для передачи данных робот использует Wi-Fi или сотовые сети, в том числе на него можно установить аппаратуру 5G.

Для верификации тревожных сообщений можно также использовать БПЛА. Одно из таких решений (**рис. 4**) предложил в 2016 году стартап ***Sunflower Labs***. Система, предназначенная для частных домов, состоит из трех компонентов: «пчелы» (собственно дрона), «улья» (зарядной станции) и «подсолнухов» (светильников, которые одновременно служат датчиками сигнализации). Система снабжена искусственным интеллектом, который умеет различать людей, животных и автомобили и определять, насколько они опасны. Например, она может распознать почтальона или курьера по тому, как он приближается к дому и сколько времени стоит у двери. Если «подсолнухи» замечают незнакомца, система посылает уведомление на смартфон хозяина, который может дать команду проверить. Тогда «пчела» поднимается в воздух, передавая видео и одновременно делая запись, а по окончании работы возвращается в «улей».

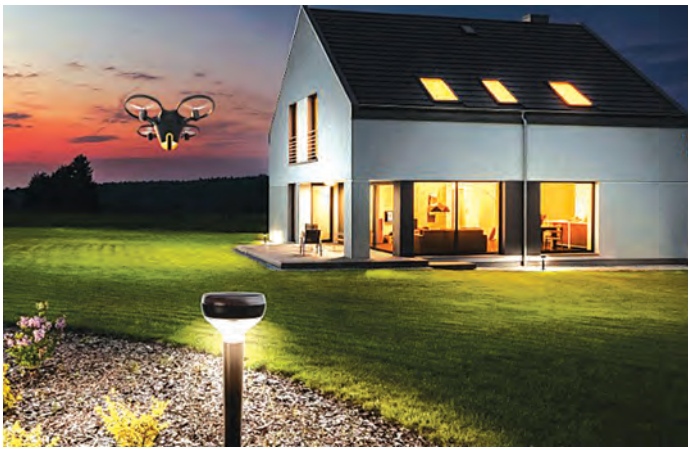

Рис. 4. Концепт системы наблюдения с помощью БПЛА в представлении Sunflower Labs

Последний рубеж

Поскольку, как говорилось, охраняемая территория может включать не только сам периметр, но и объекты внутри, вкратце расскажем и о сигнализации для зданий. Она включает в себя различные устройства, которые выявляют попытки проникновения или засекают нарушителя на подступах.

Для этого используются датчики движения, в частности пассивные инфракрасные детекторы (PIR), которые не испускают излучения, а только анализируют входящие тепловые лучи. На рынке их очень много, но если говорить о пока еще экзотике, можно опять-таки назвать Optex и их комбинированные устройства, которые сочетают две технологии: ***PIR и микроволнового детектирования***. Это сокращает количество ложных тревог, поскольку сигнал генерируется только при пересечении трех зон. Кроме того, при ярком солнечном свете или высокой температуре в помещении инфракрасный сенсор тоже может давать ложные срабатывания, но микроволновый сглаживает это явление.

Есть класс еще более чувствительных устройств — датчики присутствия, которые реагируют на очень мелкие движения (жесты, поворот головы). Опять-таки, они могут стоять как внутри, так и снаружи помещений и иметь вполне утилитарное назначение (например, регулирование освещенности в офисе в зависимости от того, есть там люди или нет). Однако их ценность для охранной сигнализации тоже неоспорима.

Не так давно американская компания ***Avigilon*** выпустила датчик присутствия Avigilon Presence Detector (APD), использующий технологии ***импульсного радара и самообучения***. Устройство может обнаруживать присутствие

людей на расстоянии до 9 м, даже если они скрыты за деревянной стенкой или гипсокартоном. Радар «видит» человека, даже если он не шевелится, хотя может также фиксировать мелкие движения и дыхание. APD хорошо подходит для установки в помещениях банкоматов, аптеках, мелких магазинах и т.д., где необходимо точное детектирование и одновременно сохранение приватности.

В целом сейчас тренд для сигнализации в помещениях — это ее объединение в систему типа «умного здания», включающую не только охранные датчики (движения, открытия двери, разбития стекла и т.д.), но и детекторы дыма и затопления, исполнительные устройства управления освещением и бытовыми приборами, видеокамеры и дверные замки. Все это работает по принципу IoT — в том смысле, что хотя устройства к Интернету подключены не напрямую (например, через центральный контроллер), они управляются и передают данные по беспроводному протоколу (ZigBee, LoRaWAN, Z-Wave и др.) и имеют очень длительный срок службы от батареи.

Центральный контроллер объединяет все эти устройства в сеть и управляет ими. Как правило, такие системы имеют приложение для мобильных устройств, через которое можно получать извещения о попытках проникновения, удаленно открывать дверь, просматривать картинку с камер наблюдения.

В Украине можно встретить множество таких систем как зарубежного, так и местного производства. В качестве примера можно привести ***Ajax*** от одноименной украинской компании. Система использует собственный протокол связи Jeweller, который обеспечивает подключение датчика на расстоянии до 2 км от централи. Кроме того, весной компания представила ретранслятор, который использует новый протокол Cargo, работающий поверх Jeweller, обеспечивает покрытие на площади до 16 км^2 и позволяет передавать файлы. С его помощью можно организовать охрану офисного центра, промышленного предприятия или территории с отдельно стоящими зданиями. В штатном режиме ретранслятор питается от электросети, но также имеет резервный аккумулятор, позволяющий продержаться 35 часов. Сами датчики могут работать от батареи до 7 лет.

В то время как Ajax постаралась сделать охранную систему автономной, перенеся логику управления на центральный контроллер, есть решения, полностью работающие через облако. Например, американская компания ***Vanderbilt*** предлагает платформу для инсталляторов, где все управление осуществляется через сервер в облаке Microsoft. Благодаря этому охрана здания и территории может быть организована с элементами модели SaaS, когда компания-оператор может удаленно управлять охранным оборудованием и обслуживать его.

Периметральные системы еще до облаков не доросли, да и вряд ли там это нужно. Технологий хватает для всех целей.

Василий ТКАЧЕНКО, **СиБ**