КОЛОНКА РЕДАКТОРА

Проблема ложных тревог в АУПС

В 2003 г. в НПБ 88–2001* впервые появилось требование установки в помещении не менее 3–4 извещателей, хотя в мире считается достаточным одного детектора. Недопустимо низкие требования к извещателям попытались компенсировать увеличением их количества. Результат 10-летнего эксперимента, по заключению экспертов: практически все неадресные системы из-за ложных срабатываний теперь эксплуатируются в режиме отключения автоматики или просто выключены.

Готовится к выпуску новая версия Свода правил СП 5.13130 "Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования". В Интернете обсуждались формулировки типов и функций извещателей, обеспечивающих повышенную достоверность сигналов "Пожар", вероятно, в расширение Приложения Р.

Однако очевидно, уровень ложных тревог от извещателя определяется отношением величины помеховых воздействий при эксплуатации к степени защиты от них. Например, извещатель, независимо от числа одновременно анализируемых факторов пожара и уровня сложности используемых алгоритмов обработки информации, защищенный от электромагнитных помех по 2-й степени жесткости, может ложнить в помещении высотой менее 6 м. По ГОСТ Р 51317.4.3–99 (МЭК 61000-4-3–95) защитное расстояние от мобильных телефонов до таких извещателей должно быть не менее 3,7 м.

Зарубежные сертификационные центры LPCB и VdS сертифицируют пожарные детекторы, защищенные от электромагнитных полей радиочастотного диапазона с напряженностью поля не менее 30 В/м, что в 10 раз выше уровня 3 В/м по нашей 2-й степени жесткости. В результате даже простейшие по алгоритму обработки зарубежные детекторы эксплуатируются годами без ложных срабатываний, а наши извещатели, сертифицированные по ГОСТ Р 53325–2009, могут ложнить каждый день. Но надо отметить, что ложнящие извещатели используются в нарушение требования СП 5.13130.2009 п. 13.1.11: "Тип и параметры извещателей должны обеспечивать их устойчивость к воздействиям климатических, механических, электромагнитных, оптических, радиационных и иных факторов внешней среды в местах размещения извещателей". Очевидно, для получения достоверного сигнала "Пожар" в текущей электромагнитной обстановке в ГОСТ Р 53325 для наших пожарных извещателей должна быть указана 4-я степень защиты от электромагнитных помех как минимальная.

Игорь Неплохов
Редактор раздела
"ОПС, пожарная безопасность"

ОПС и Интернет

Интернет проник в каждый дом и на каждый завод. Нередко он является даже единственным надежным, естественно многократно дублированным каналом связи. Чем же на это ответили производители ОПС в мире и России?

Алексей Омельянчук
Начальник КБ "Рубикон"
компании "Сигма-ИС"

ОПС – это две части. Локальное объектовое оборудование (пульт постановки – ППК-датчики) и система передачи СПИ, а также ПЦН – служба реагирования.

Традиционно на объекте использовались "сухие" контакты (максимум RS-485), а в СПИ – телефонные линии. "По занятым линиям" считалось самым большим писком науки и техники. В 1960 году. В мире более распространены "по коммутируемым линиям", ибо исключают монополизм провайдера услуг связи.

В наше время на объекте часто применяется адресный шлейф и Ethernet. А вот для СПИ – чаще то же самое, что и 50 лет назад.

Интернет в каждом доме

1. В отличие от МЧС, которое продолжает строить для себя (пожарных систем) какие-то закрытые ведомственные системы ПИ, в охранной области давно наступила либерализация, применяется то, что удобнее.

2. Естественный шаг: вместо телефонной линии – GSM. Но по GSM, безусловно, не работают варианты "надтонального канала", и более того, довольно плохо работают варианты Contact-ID. Однако зачем это все, если GSM – это вообще цифровая сеть изначально. GPRS давно решил все проблемы.

3. Проводные линии в квартирах продолжают развиваться. Но не телефонные. Аналоговая телефонная линия во многих квартирах сейчас выглядит так же, как (вы не смейтесь, они тоже есть) проводная радиоточка. Это кончик провода, заштукатуренный под плинтусом, и хозяин уже давно забыл, что это и где. Теперь проводные линии – это коаксиальное или волоконное телевидение (разумеется, с гигабитным Интернетом в придачу).

Итак, мы оказались в ситуации, когда единственным надежным, естественно многократно дублированным каналом связи в любом доме является Интернет. Чем же на это ответили производители ОПС? Сначала взглянем, что творится в мире.

Ответ мировых вендоров ОПС

Конечно, многие производители уже лет десять предлагают IP-коммуникаторы помимо стандартного дозванивателя по телефонной линии (в мире практически не применяются знакомые нам "Атласы" и тому подобные системы, работающие по выделенной или занятой телефонной линии, поскольку такую систему можно поставить только непосредственно на АТС, а соответственно услуга приема сообщений монополизируется, что обычно не одобряется ни в Америках, ни в Европе). Как правило, они имеют собственные форматы, нередко являющиеся вариациями на тему привычного Contact-ID, только поверх TCP/IP. Выглядит это странно – использовать 100-мегабитную сеть для передачи всего трех байт сообщения.

США: закрытые протоколы против стандарта

Разумеется, приняты меры по стандартизации, однако они оказались не очень популярными в США. То есть стандарт есть, даже освященный именем ANSI (называется ANSI-SIA DC-09–2007). Кстати, кто не в курсе – аббревиатура SIA означает Security Industry Association, собственно организация, в которую входят всякие Honeywell/Ademco и прочие Tyco Security. Именно эта организация в 2007 г. разработала стандарт. Надо отметить, у нее не очень хорошо получается со стандартами. Как правило, они настолько запаздывают, что мало кто их реально применяет. Вот и с этим стандартом получилось так же.

Некоторые (например, GE Interlogix) заявили о выпуске изделий, которые поддерживают стандарт ANSI, но по умолчанию их устройства (и приемные мониторинговые станции) работают в других протоколах, закрытых и значительно более информативных.

Европа: безусловная стандартизация

Несколько иная ситуация сложилась в Европе. Европейский (точнее, немецкий) аналог Contact-ID, называемый VdS 2465, просто получил (тоже недавно – в 2006 г.) приложение с указанием, как те же самые весьма простые сообщения пересылать поверх TCP/IP. Этот стандарт в обязательном порядке поддерживается всеми европейскими производителями, включая чехов, словаков и, конечно, Bosch и Esser. Да, некоторые производители добавляют собственные расширения для передачи данных в обратную сторону (для централизованного управления и конфигурирования системы), но сам по себе стандартный протокол реализуется безусловно.

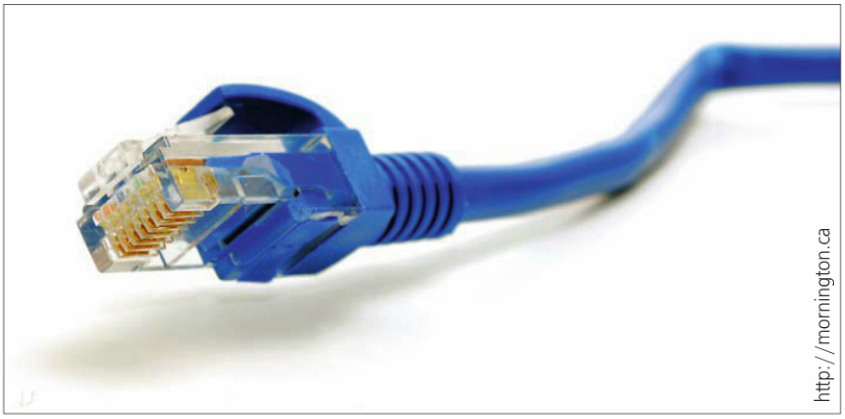
Кстати, для многих устройств IP-телефонии существуют прошивки, поддерживающие прием обычного Contact-ID (или обычного VdS 2465) по обычной аналоговой телефонной

паре проводов и передачу этого сигнала в форматах IP. Такие версии выпускает, например, непосредственно Cisco и некоторые другие производители Phone-over-IP. Это позволяет легко модернизировать существующие старые охранные приборы с аналоговым выходом для работы по TCP/IP. Между тем некоторые VoIP-адаптеры имеют встроенные роутеры и, более того, возможность переключаться на резервный канал через GPRS-модем. Что еще нужно для счастья?

Счастье в облаках

Для полного счастья осталось оглядеться и обнаружить, что не только облачное видеонаблюдение, но и облачные центральные станции давно присутствуют. Давно – это "уже несколько лет". Точнее, "уже более года".

Как пример – британский стартап IP Alarms, продвигающий услугу alarmcloud.net. Вы можете запрограммировать свою охранную панель на передачу сообщений к ним на облачный сервер (ужасно надежный, динамически масштабируемый и даже с плавающими IP-адресами для защиты от DDoS-атак). А их сервер уже зафиксирует все события, передаст их вам по электропочте или SMS, а также направит вашей любимой службе охраны посредством поддерживаемого ими протокола связи. Так что необязательно добиваться, чтобы все охранные компании срочно переключались на IP-передачу сообщений – облачный сервер примет IP и перетранслирует охранникам в приемлемом виде.



Нередко Интернет является даже единственным надежным, естественно многократно дублированным каналом связи

Ответ российского рынка

Теперь посмотрим, что у нас внутри страны. Видны две основные тенденции.

1. GSM/GPRS-сигнализации

Во-первых, уже несколько лет на сверхмалых объектах (дачи-гаражи) популярен класс "GSM-сигнализаций", которые ориентированы на управление и передачу сообщений путем SMS или тонового набора кнопочками. В последнее время в них все более распространено использование GPRS-канала для связи с ПЦН.

Обратите внимание, GPRS означает не очень стабильный, непостоянный канал связи. Как правило, он легко восстанавливается при необходимости передачи данных, но каждый раз при таком восстановлении IP-адрес объектового устройства может оказаться новым. Известны три решения. Первое: купить у оператора связи "фиксированный адрес". Второе: воспользоваться бесплатной (или почти бесплатной) услугой динамического DNS – услуга предоставляется интернет-компаниями, а не сотовыми операторами, а в Интернете, как известно, ценообразование совсем иначе устроено, нежели на высокомонополизированном рынке услуг телефонной связи. Третий вариант: облачный ПЦН, то есть сервер с фиксированным IP-адресом, на который подключается как оборудование, так и компьютер оператора, после чего общение оператора (тоже, как правило, работающего с мобильного телефона) и ППК на объекте осуществляется опосредованно через специальный сервер. Увы, у отечественных производителей я пока не встречал поддержку оборудования конкурентов, так что если облачный сервер и есть, то у каждого производителя GSM-сигнализаций он собственный и ни с чем более несовместимый. Популярных стандартов просто нет. Общественные ассоциации, мягко говоря, не слишком активны, а госорганы либо устранились, либо ограничиваются стандартизацией в стиле МЧС: издается приказ использовать одно конкретное оборудование одного конкретного производителя – вот вам и вся стандартизация.

2. Специализированные системы для крупных объектов

Вторая тенденция – помимо GSM/GPRS-сигнализаций – это проникновение систем, изначально разработанных под крупные госмонополистические объекты. Там Ethernet давно стал применяться для подключения аппаратуры к компьютерам с интегрирующим ПО, поэтому по мере удешевления аппаратуры и появления систем, масштабируемых "вниз" (на не очень большие и даже средние объекты), наработанные технологии и готовое программное обеспечение стали применяться не только на ведомственных постах охраны, но и на пультах централизованного наблюдения общего назначения. При этом, как ни странно, выяснилось, что оборудование, предназначенное изначально для крупных систем, более совместимо у разных производителей. Поскольку на крупных объектах нередко возникала ситуация, что полобъекта оснащено техникой одного типа, а вторая половина – другого (потому что раньше это были два разных объекта, а после их "объединения" стали одним). Так вот, в такой ситуации никто, конечно, не будет переставлять работающее охранное оборудование, чтобы обеспечить унификацию. Цена вопроса такова, что дешевле заплатить за создание программного обеспечения, которое сможет работать с обоими типами оборудования.

Как результат, практически все крупные производители ПО интегрированных систем поддерживают оборудование "Болид", "Сигма-ИС", Apollo и ряда других отечественных и импортных типов, наиболее распространенных в РФ. Поэтому можно брать почти любое ПО этого класса и к нему по IP-сетям (через кабельный Интернет) легко подключить весьма широкий ряд охранного оборудования различных производителей. Конечно, программное обеспечение, предназначенное для службы охраны крупного завода, – это не совсем то, что нужно на пульте охраны для разбросанных по району коттеджей или магазинов. Но тем не менее такой подход развивается и уже работает, ПО совершенствуется и адаптируется к новым задачам.

Итак, что мы видим

Возможность подключения к IP-сетям – естественная (встроенный порт) или через дополнительный адаптер – есть практически у всех современных ОПС. А вот реальное использование такой возможности несколько ограничивается наличием программного обеспечения и состоянием стандартизации интерфейсов.

Программное обеспечение, ориентированное на применение в качестве интегрированной части в больших системах, как правило, поддерживает некоторый набор подсистем ОПС, как при подключении по старинке (RS-232, RS-485), так и при подключении через Ethernet. ПО для работы в качестве "домашнего сервера" сейчас по большей части являются "закрытыми", поддерживающими только оборудование того же производителя.

ПО для работы в качестве ПЦН – пока реализуют только минимальный функционал, доступный через старые стандарты передачи извещений, адаптированные к IP-сетям. При этом состояние стандартизации этих "адаптированных" вариантов и их поддержка производителями оборудования оставляет желать лучшего. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru