Муковнин Николай Федорович,
независимый эксперт

ЭТАПЫ ПУТИ К ПОЖАРНОМУ МОНИТОРИНГУ

опубликовано в ж. Алгоритм Безопасности №3 2018 г.

https://www.aktivsb.ru/statii/etapy_puti_k_pozharnomu_monitoringu.html

Одна из заявленных тем данного номера журнала — изменения в нормативной документации по пожарной безопасности. Прошло также публичное обсуждение проекта межгосударственного стандарта «Системы передачи извещений о пожаре». Но в данной статье речь пойдет о системе передачи извещений о пожаре (СПИ) в более широком смысле — о «пожарном мониторинге». Как многие могли заметить, в проекте обновленного СП на системы пожарной сигнализации ни про СПИ, ни про пожарный мониторинг нет ни слова, также им не уделили должного внимания в своде правил, который должен заменить приложение А СП 5.13130. А ведь все эти вещи давно взаимосвязаны.

Цель пожарного мониторинга

Цель пожарного мониторинга, как и любого инструмента, применяемого экстренными службами, — спасение жизни людей и снижение материального ущерба. Но сотрудники, связанные с тушением пожаров, эту цель воспринимают через призму своего мировоззрения, для них задача «спасения жизни» сводится к своевременному реагированию и прибытию на место происшествия.

Это сказывается на их требованиях к системе пожарного мониторинга — им нужен только один обобщенный сигнал «пожар» с объекта, чтобы быстро выдвинуться для проведения работы. Где, что и как горит, они давно привыкли выяснять уже по прибытию.

И тут, в отличие от привычных вызовов пожарных подразделений по телефону, при работе с пожарным мониторингом они периодически сталкиваются с ложными вызовами, например, кто-то просто забыл обед в микроволновке. И это формирует к нему негативное отношение рядовых огнеборцев и их начальников.

Таким образом, задача по «спасению жизни и снижению материального ущерба», на их взгляд, как и раньше, должна зависеть от своевременности поступления вызовов по телефону, что давно не соответствует реалиям.

Проблема ложных срабатываний

Ложные срабатывания СПС и, как следствие, бесполезные выезды пожарных машин — это бич не только отечественного пожарного мониторинга. Статистика, приведенная на сайтах пожарных департаментов Европы и Северной Америки, говорит о том, что более 99% автоматических сигналов о пожаре — ложные. Идет отказ от выезда по автоматическому сигналу в рабочее время без подтверждения по телефону, за исключением объектов, являющихся аналогами наших Ф1.1, Ф1.2, Ф4.1, Ф4.2. И все это с учетом того, что история пожарного мониторинга в США и Великобритании насчитывает уже десятилетия.

С данной проблемой надо бороться комплексно, как техническими, так и административными мерами. Ее нельзя одномоментно решить исключительно разработкой новых пожарных извещателей, включением нескольких извещателей по схеме «И» или штрафами.

Во всех противопожарных нормах мира вопросу снижения вероятности ложных срабатываний уделяется достаточно много внимания. И пришло это в первую очередь с внедрением пожарного мониторинга. Это понимание появляется потихоньку и у нас в стране.

Более того, пожарный мониторинг можно еще эффективнее использовать в этой работе. Зная, как часто и что отключают на объекте, где чаще всего происходят сработки СПС, что и как отрабатывает при запуске систем, неисправностях, надзорное ведомство с помощью машинной и ручной обработки данных с объектов может принимать аргументированное решение о проведении соответствующих мероприятий и призывать к ответу собственника и/или обслуживающую организацию.

Стоит также обратить внимание, что если система пожарного мониторинга предоставляет детальные данные по развитию ситуации на объекте, то оператор экстренной службы может принять более взвешенное решение по реагированию и о выделении сил для тушения пожара. Очевидно, что срабатывание одного пожарного извещателя скорее всего окажется «ложняком» и достаточно будет отправить на объект одну автоцистерну для проверки на месте. Но если пришел сигнал уже от нескольких извещателей или их групп, или сигнал от дымового сенсора дополнился сигналом теплового или сигнализатора потока жидкости, то последовательность действий будет другой. Поднимается уровень тревоги, высылаются дополнительные пожарные расчеты по заранее подготовленным

планам — похоже, там действительно пожар. Разумеется, принятие решений может быть автоматизировано, но, чтобы автоматизация работала корректно, предварительно нужно собрать солидную статистическую базу.

Выбор канала связи

Системы передачи извещений о пожаре появились почти одновременно с пожарной сигнализацией. В разные периоды использовались различные каналы передачи извещений: по выделенной проводной линии, по общей телеграфной линии. На смену телеграфу пришла телефонная связь, и в какой-то момент передача сообщения о пожаре «голосом» вытеснила автоматическую машинную передачу, т.к. автоматика сильно увеличивала стоимость приборов. А дежурный на объекте мог совмещать реагирование на сигналы пожарной сигнализации с охранными функциями. Именно поэтому у нас требуются круглосуточные посты, а не потому, что дежурный должен чем-то там управлять. Зная квалификацию сотрудников «пожарного поста», им, зачастую, нельзя доверить ничего сложнее звонка по номеру «01». Справляются они и с этой задачей крайне плохо, иначе не пришлось бы сейчас обсуждать тему «передачи извещений без участия персонала».

Но за рубежом активно прижились автоинформаторы и передатчики цифровых сигналов по телефонным каналам, что было следствием более высокого уровня развития микроэлектроники. У нас же до конца девяностых эта тема глобально не освещалась, хотя и решалась в частном порядке для многих объектов. В рамках изменений в НПБ-110 в 2001 году это вопрос был наконец поднят и озвучена рекомендация передавать извещения о пожаре по радиоканалу. На тот момент это было, наверное, лучшее решение из возможных. Единственная телефонная линия из обветшавших советских фондов уже не обеспечивала требуемую надежность, да и сам телефонный канал следовало оставить свободным для дублирования извещения дежурным, вызова других экстренных служб. К тому же не было поголовной «обязаловки» — подключались «исходя из технической возможности». И рекомендация о «преимуществе радиоканала» рудиментарно живет по сей день.

Все это было актуально в начале «нулевых», но сегодня почти в любом селе работают 2–3 оператора сотовой связи: Ростелеком или крупные региональные операторы обеспечивают проводное подключение к интернету и телефону. Выбор каналов связи уже не ограничен одной телефонной линией. Беспроводная связь не является единственной альтернативой, как это было раньше. Кроме того, появляется очень много проблем организационно-технического характера. Как быть, если нет прямой видимости между передатчиком и приемником? Надо ставить вышку с ретранслятором? За чей

счет будет обеспечиваться электропитанием ретранслятор, и кто его будет охранять и обслуживать? А что, если школа, на которой стоит ретранслятор, закроется из-за объединения с другой? Кто и в какой мере будет нести ответственность, если сигнал «затерялся»? Какой период времени может не работать ретранслятор? Не стоит забывать про регистрацию радиопередающей аппаратуры. Очевидно, что создание оператора связи (а ведь именно оператор связи готов ответить на поставленные выше вопросы в соответствии с законом «О связи») только для целей пожарного мониторинга кажется излишним и экономически неэффективным решением. Но, прежде чем использовать каналы, предоставляемые операторами связи, стоит решить еще один из наиважнейших вопросов, а именно их отказоустойчивость.

Отказоустойчивость каналов связи

Чтобы выдвигать конкретные требования к отказоустойчивости каналов связи, надо соотнести возможные неисправности и отказы с наносимым при этом ущербом. Иначе есть риск получить на выходе систему с избыточной надежностью, но при этом очень дорогую во всех отношениях. Итак, какие параметры для каналов связи от операторов мы можем ожидать? Есть приказ Минсвязи от 27.09.2007 № 113 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования», где приведены коэффициенты готовности для сетей связи в нормальных рабочих условиях. Самый низкий показатель здесь у сетей передачи данных, он составляет 0,99. У других каналов, в том числе местной телефонной сети, еще больше девяток после запятой. Но будем честны, далеко не везде качество связи соответствует этим нормам. Представим, что в действительности коэффициент готовности составляет где-то 0,95, т.е. больше двух недель в год нет связи. Многие с таким сталкиваются? Я думаю, что такое скорее исключение, чем норма. К сведению, для каналов связи согласно п. 6.2.24.1 ГОСТ Р 56935-2016 «Услуги по построению системы мониторинга автоматических систем противопожарной защиты и вывода сигналов на пульт централизованного наблюдения «01» и «112» «вероятность прохождения» должна составлять не менее 0,9, что однозначно дискредитирует используемый преимущественно радиоканал. Теперь вернемся к операторам связи и возьмем два канала с коэффициентом готовности 0,95 (например, два подключения к сотовым сетям 3G/4G). Совокупный их коэффициент готовности составит уже 0,9975, а это уже менее суток, когда объект будет без связи. Чтобы оценить потенциальный ущерб объектам, в обязательном порядке оборудуемых СПИ, а также объектам с массовым пребывание людей, имеет смысл воспользоваться данными из статистического сборника «Пожары и пожарная безопасность» за

2016 год. Из выборки за пять лет возьмем наибольшее значение по ущербу. 22 млрд рублей (2015) по всем пожарам. В день это будет около 61 млн рублей. Человеческих жертв за те же сутки — 32 человека (в 2012 году на пожарах погибло 11 652 человека) по всем пожарам, в том числе и в жилом фонде, который СПИ не оборудуется в принципе. Попробуем вычленить из этого массива данные по гибели людей на объектах, как было оговорено выше.
Возьмем статистику, выделяя из пятилетки самые худшие годы:
- здания, сооружения и помещения предприятий торговли — 32 человека (2015);
- здания учебно-воспитательного назначения — 4 человека (2013);
- здания здравоохранения и социального обслуживания населения — 83 человека (2013);
- здания, помещения сервисного обслуживания населения — 11 человек (2012);
- административные здания — 18 человек (2016);
- здания, сооружения и помещения для культурно-досуговой деятельности населения и религиозных обрядов — 1 человек (2012);
- здания для временного пребывания (проживания) людей — 26 человек (2012).

Итого: погибло 174 человека, т.е. по статистике в день на этих объектах гибнет 174/365=0,5 человека, или 1 человек в два дня при самом дрянном раскладе. Разумеется, случаются и масштабные трагедии. В любом случае, дальнейший анализ целесообразности повышения требований к коэффициенту готовности каналов связи нуждается в более глубокой научной проработке. При этом отдельно должны быть рассмотрены случаи отключения электроэнергии, так называемые «блэкауты», работа в условиях ЧС и подобных ситуациях. Такие обстоятельства зачастую приводятся в качестве контраргумента против использования каналов связи существующих операторов и наверняка безосновательно.
Этот анализ должен быть проведен, и именно его надо взять за основу при выборе каналов связи, в том числе с экономическим обоснованием.
Информационная совместимость пожарных приборов при передаче извещений
Если возникает необходимость получать данные о работе противопожарных систем с информационной емкостью в более чем один обобщенный сигнал пожара от объекта, который иногда может состоять из нескольких корпусов, то тут же встает необходимость обеспечивать информационную совместимость между приборами различных производителей. Не важно, на каком участке передачи извещений, между прибором приемно-контрольным (ППКП) и объектовым прибором СПИ (ПОО), ПОО и пультом (ППО), ППО и АРМ пульта — это уже вторично. С каждым днем на рынке появляется все больше пожарных приборов с портами USB и Ethernet, предназначенных для

конфигурации и передачи данных в системы верхнего уровня, в том числе на автоматизированные рабочие места (АРМ). А вот количество приборов с интерфейсом RS-232 неумолимо снижается. Т.е. вариант выбора физического интерфейса для обмена данными между ППКП и ПОО не так уж и велик.
С учетом всех преимуществ и недостатков USB-Ethernet оказываются в выигрыше.
В Европе и Америке о необходимости наличия открытых стандартизированных протоколов обмена в СПИ задумались уже давно. Сегодня существуют и широко распространены стандарты передачи извещений по IP-каналам в виде ANSI SIA DC-09 «Digital Communication Standard Internet Protocol Event Reporting» и CLC/TS 501369 «Alarm systems — Alarm transmission systems and equipment Part 9: Requirements for common protocol for alarm transmission using the Internet Protocol (IP)», а также директивы VdS 2465.
На следующем этапе, т. е. на участке связи между ПОО и ППО, эти протоколы также отлично подходят. В них уже «встроен» контроль связи между ПОО и ППО, реализованный с помощью алгоритма, знакомого многим читателям по утилите «ping». Также протоколы предусматривают обход NAT, что позволяет осуществлять передачу данных от ППО на ПОО и не использовать фиксированный IP-адрес.
Примерно этим же путем идет ФКУ НИЦ «Охрана» Росгвардии [1] при разработке нового поколения стандартов по системам централизованного наблюдения (СЦН) серии ГОСТ Р 56102.
Соответственно, уже сейчас можно с большой уверенностью говорить, что передачу извещений следует осуществлять по IP в стандартизированных протоколах на всех участках независимо от вариантов организации каналов связи на более низком уровне (самостоятельные mesh-радиосети; от второго до пятого поколений сотовых сетей; классическое проводное подключение к Интернету и т.д.). Это решение позволит сократить издержки на разработку, более гибко организовывать пожарный мониторинг и производить его включение в городские интегрированные системы безопасности с меньшими затратами. Дополнительно может осуществляться передача информации по имеющемуся каналу связи, например, данных с систем видеонаблюдения. И самое главное — можно производить модернизацию системы с сохранением обратной совместимости с действующими решениями, что является существенной проблемой при текущей организации.

Структурирование данных на пульте пожарной охраны

Когда мы говорим о пожарном мониторинге с передачей обобщенного сигнала о пожаре, то задачи по структурированию поступающих данных и извлечению

дополнительной информации из них не стоит. Все достаточно просто: есть номер объектового прибора, к нему привязывается карточка объекта, в которой собраны основные данные — адрес, этажность, функциональное назначение и т.д. В большинстве случаев этого бывает вполне достаточно, т.к. подавляющее количество оборудованных СПИ объектов достаточно малы, и задача поставлена одна — своевременный выезд на пожар. Но если посмотреть на ситуацию через призму задачи по надзору, в том числе негосударственному или страховому, и по сокращению выездов на ложные срабатывания, то поле зрения должно быть существенно расширено. Дополнительно можно принять во внимание, что наиболее резонансные пожары в последние годы происходили на довольно крупных и непростых объектах.

Извещение на пульт поступает, как правило, в виде цифрового кода, иногда может содержать какое-то текстовое описание, которое диспетчеру ни о чем не скажет, т.к. он не настолько знаком с объектом. Тем более, эта информация не будет ничего значить для огнеборцев. В таком виде данные могут пригодиться только для случаев ложного срабатывания СПС объекта — вместо внесения в «черный список» целиком объекта, можно будет ограничиться одной зоной. У надзорных же органов появится конкретика, где «ложнит», а где неисправности долго не устраняются. Кто бы что ни говорил, а на крупных объектах коммерческой недвижимости неисправности присутствуют практически всегда: непрекращающиеся реконструкции и ремонты, непростые отношения между собственниками и арендаторами вносят свою лепту. Поэтому становится очень важно понимать, что неисправность в системе сигнализации или противопожарной автоматики произошла в небольшом вещевом магазине на этапе его реконструкции, а не в действующем центре детских развлечений. Это потребует разной реакции.

Огнеборцам важна уже другая информация — локализация возгорания на объекте, площадь его распространения, присутствуют ли в зоне возгорания люди и сколько их там может быть. Согласитесь, пожар около кинозала на 4-м этаже или в служебно-складской части одного того же торгового центра требуют разных алгоритмов действий экстренных служб с самого начала.

Таким образом, мало будет передать только номер зоны контроля пожарной сигнализации, в которой фиксируется сработка пожарного извещателя, но нужно еще привязать много дополнительных данных, начиная от номера этажа, функционального назначения, количества людей, дополнительных коэффициентов риска и заканчивая «историческими» данными по работе систем на объекте и базовой визуализацией в виде планов. Все это составляет «метаданные». Требуются довольно солидные усилия для формирования такой базы «метаданных», поддержания ее в актуальном состоянии с сохранением

взаимосвязи с конфигурацией оборудования СПС и пожарной автоматики. Очевидно, что такую работу невозможно проделать без тесного взаимодействия с собственником и техническими специалистами объекта. К тому же необходимо привести к «общему знаменателю» структуры систем на различных объектах, построенные на оборудовании различных производителей, каждый из которых имеет свой подход и идеологию. И самым простым, на мой взгляд, решением поставленной выше задачи может быть стандартизация формата такой базы «метаданных», которую будут подготавливать специалисты объекта и передавать в заданном виде коллегам, работающим с пультом.

Информационная безопасность (ИБ) пожарного мониторинга

Вопросы информационной безопасности традиционно не затрагиваются в отечественных «пожарных» нормах. Поэтому даже введение понятия уровней доступа в ГОСТ на приборы пожарные было очень серьезным шагом, хоть и не так очевидна их взаимосвязь с ИБ. С каждым новым днем все больше будет уделяться внимания информационной безопасности. Но вернемся к пожарному мониторингу.

Хочу обратить внимание на существование участка, выходящего за пределы объекта, в который могут внедриться посторонние с различными целями. Основная причина, которая сдерживает до сих пор хакеров на этом поприще, — отсутствие материальной заинтересованности в отличие от тех же систем охранной сигнализации и охранных СПИ. Все же игнорировать данный вопрос никак нельзя. Радиосети, с учетом получающих все большее распространение дешевых Software Defined Radio (SDR) приемо-передатчиков, подвержены различным типам атак. Проблемы IP-сетей и так у всех на слуху. Представьте возможный урон от кибертерроризма, если на пульт постоянно будут поступать инициированные хакером сигналы о пожаре, или если через функции телеуправления будут запускаться постоянные эвакуации из зданий.

Первым рубежом защиты «от посторонних», как правило, выступает физическое ограничение доступа. Это возможно только в редких случаях защищенных кабельных линий, прокладываемых в охраняемых коллекторах связи. Такой вариант мало пригоден для СПИ о пожаре ввиду высокой стоимости. Второй рубеж — использование шифрования (в том числе и для радиосетей), но и оно никогда не даст 100% защиты, т.к. даже при использовании криптографических алгоритмов практически с абсолютной на сегодняшний день надежностью (например AES-256), профи могут найти «черный ход» из-за особенностей реализации на конкретном оборудовании. Одно из узких мест — программные и аппаратные генераторы случайных чисел, необходимые для создания ключей шифрования. И тут первую скрипку

начинает играть скорость закрытия «дыр», т.е. выхода обновлений. Думаю, не надо разъяснять, почему ликвидация уязвимости должна решаться в первую очередь через программное обеспечение оборудования, так называемую «прошивку», а не заменой «железа». При этом крайне важно сохранять обратную совместимость с существующим оборудованием, т.к. не всегда обновление можно произвести одномоментно.

Также необходимо отметить, что доступ к настройкам оборудования тоже должен быть максимально закрыт извне. Многие уже слышали про массовые взломы камер видеонаблюдения, видеорегистраторов и роутеров по всему миру. Нельзя, чтобы подобное могло повториться и в пожарной СПИ — на кону человеческие жизни. Именно поэтому важно уже сейчас задуматься над информационной безопасностью при построении пожарного мониторинга, принять продуманные и взвешенные решения, а не подставлять «костыли» и пришивать «заплатки» уже по ходу дела, как, к сожалению, у нас принято. Использование виртуальных частных сетей (VPN), частных точек доступа у операторов сотовой связи (APN), а тем более радиоканалов без шифрования или со слабой криптографией — это всего лишь ситуативные полумеры.

Структура пожарного мониторинга

Среди как обывателей, так и не вовлеченных в пожарных мониторинг специалистов, бытует мнение, что сигнал с объекта поступает напрямую в ближайшую пожарную часть. К сожалению, такое представление в большинстве случаев ошибочно. Далеко не во всех пожарных частях в нашей стране установлено соответствующее оборудование, которое позволило бы принимать сигналы с объектов. Хотя возможность трансляции сигналов на несколько пультов одновременно имеется у большинства присутствующих в данном сегменте рынка СПИ. Установка такого оборудования — это не только единовременные капитальные затраты, но и последующие расходы на техническое обслуживание, обучение и зарплату дежурного на пульте в каждой ПЧ. Поэтому сигналы поступают в дежурную диспетчерскую службу (ДДС), а уже потом по телефону (!) или по ведомственной радиосвязи передаются команды в пожарную часть. В этом есть своя железная логика, вытекающая из организационных особенностей, не буду на этом сейчас останавливаться. Но какой путь проделывает в такой ситуации извещение? Далеко не в каждом городе есть ДДС, во многих регионах она всего одна и находится в региональном центре. Извещение от объекта передается в радиоэфир, далее может путешествовать по аналогичным объектам, которые ретранслируют данный сигнал, затем попадает на ретранслятор на вышке, а далее с этой вышки по цепочке ретрансляторов до другого города, либо вовсе уходит в

магистральные проводные/беспроводные каналы операторов связи. Сколько здесь «бутылочных горлышек» и «единых точек отказа» неизвестно широкой публике, но, судя по проскальзывающим на специализированных форумах сообщениям от специалистов, дела обстоят довольно плохо. На рисунке 1 представлена приблизительная схема такой организации.

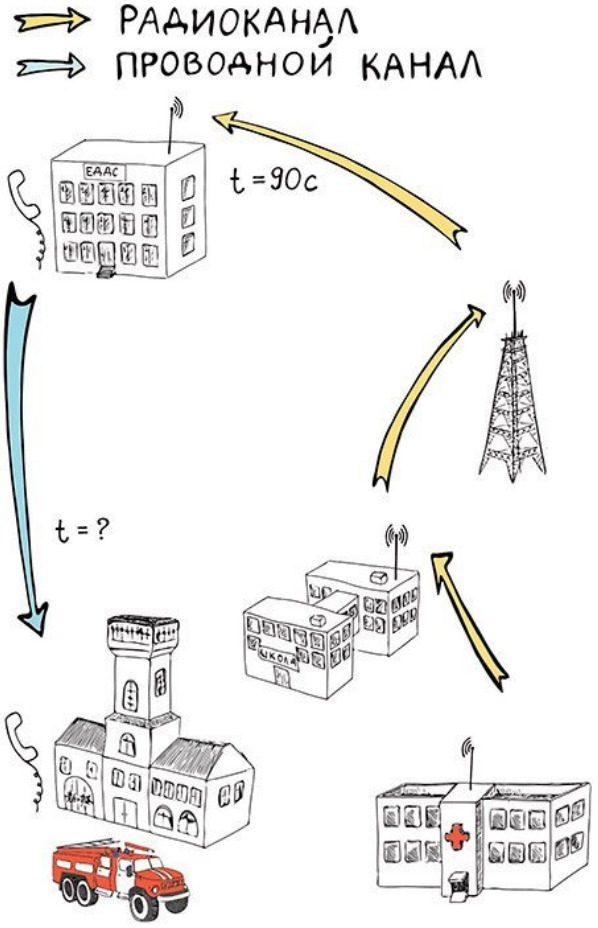

Рис. 1. СПИ сегодня

На рисунке 2 предложена альтернативная схема организации пожарного мониторинга с потенциалом «синергетического эффекта», но он возможен лишь в том случае, если будут достаточно жестко стандартизированы варианты передачи извещений, их формат и протоколы. Иначе не стоит ожидать, что обслуживающая организация будет вкладывать деньги в СПИ, т.к. по тендеру договор на ТО заключается всего на год и подразумевает минимальную цену, куда не заложено дополнительное оборудование. Также не стоит ожидать, что и страховщики будут подключаться к такой системе, т.к. нет никаких гарантий, что применяемое ими оборудование будет совместимо с объектовым (ППО и ППКП).

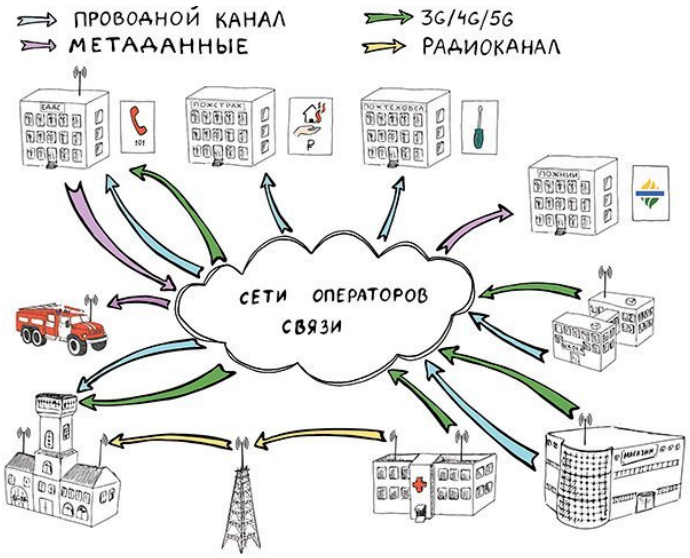

Рис. 2. СПИ завтра?

Заключение

К счастью, наверное, на сегодняшний день под пожарный мониторинг попадают всего четыре группы объектов. Но в скором времени к ним прибавятся объекты с массовым пребыванием людей, потом особо опасные промышленные объекты, а там и все объекты при отсутствии на них круглосуточных пожарных постов. Поэтому проблема развития пожарного мониторинга, его нормирования — это следующая головоломка, которую придется решать нашим законодателям и комитетам по стандартизации в ближайшее время, как бы ни хотелось пустить все на самотек или отдать на откуп производителей. Решение о перекладывании финансового бремени вопроса на другие ведомства или коммерческие структуры не поможет распутать этот клубок и является классическим примером коррупционного мультипликатора. Но начинать нужно в первую очередь с фундамента — стандартов и сводов правил. Основные моменты, которые должны быть четко и ясно освещены в них, уже довольно подробно раскрыты в данной статье, но в качестве резюме приведу их ниже:

- Требования к каналам связи: коэффициенты готовности, пропускная способность.
- Требования к резервированию каналов связи: дублирующие ретрансляторы, выбор операторов связи, оценка влияния кризисных ситуаций на конечный результат.
- Стандартизация протоколов: принятие зарубежных стандартов или разработка своих.
- Требования к обеспечению информационной безопасности.

А пока будет вестись вся эта работа, лучше не трогать то, что сейчас работает. Пожар не спрашивает о нашей готовности его предотвратить или потушить. Для внедрения новых направлений требуется взвешенный анализ всех вышеперечисленных моментов. Истории последних пожаров должны напоминать – что слишком велика цена ошибки.

Литература

1. Колесов К.В., Морозов А.Н. О нормативном обеспечении разработки унифицированного АРМ пунктов централизованной охраны // Алгоритм безопасности. 2018. № 5.