



инженеры
геологи
аналитики рынка
архитекторы
инсталляторы
социологи
о домашнем интеллекте

ТЕХНИКА БЕЗОПАСНОСТИ

Юрий Королев
президент ICS Group

О чем можно говорить через пару месяцев после Беслана (и пару лет после Нью-Йорка)? Тема всплывает сама собой.

Человечество строит информационное общество и в нем же живет — как в недостроенном доме. По ходу дела накапливая опыт, что-то меняя, делая ошибки и пытаясь предвидеть последствия следующих шагов. Информация — это продукт, созданный и потребляемый человечеством, это искусственная среда обитания. В ней — опасность, и в ней же — защита от опасности.

В большинстве стран после 11 сентября были увеличены расходы на содержание спецслужб. Терроризм был признан угрозой глобального масштаба. Ее можно игнорировать, можно попытаться сесть за стол переговоров — непонятно только, с кем. События в Беслане еще раз подтвердили известную истину: человеческий фактор — самое слабое звено во всех процессах управления, не исключая управление чрезвычайными ситуациями. Конечно, даже постфактум очень сложно понять, что именно надо было предпринимать. В этой долгой истории замешаны политика, криминал, коррупция. Однако при наличии определенного набора технических средств — системы управления малым городом — события такого рода, думаю, можно было бы предотвратить, хотя бы отчасти. Преграды должны быть выставлены на всех этапах развития угрозы, от ее появления до реализации. И если пока не удастся пресечь «посев» терроризма на благоприятном для него политическом субстрате, это не означает полной бесперспективности попыток уничтожения «урожая».

Система «Большого Брата»

Такие системы есть во многих цивилизованных странах. Каждая из них имеет свою специфику, историю, законодательный базис. Британский «Большой Брат», а именно, система тотального видеонаблюдения на дорогах под названием *City Watch*, введена достаточно давно и является частью «надсистемы» *City Management*. На улицах, площадях и автострадах страны установлено более 40 миллионов видеокамер. Цель — автоматическая фиксация событий с идентификацией автомобильных номеров. Главным инициатором «тотальной слежки» за британскими водителями выступили... страховые компании. Там, в отличие от России с нашим ОСАГО, жизнь человека стоит намного дороже. Вместе с оснащением перекрестков и дорог средствами мониторинга автомобильного потока были значительно ужесточены меры наказания за нарушения правил уличного движения, а информация от автоматических систем была легализована в качестве законного свидетельства нарушения правил. Поняв, что от дорожной полиции скрыться не удастся, водители почли за благо перейти к дисциплинированной езде с соблюдением правил. В результате количество ДТП снизилось на 75%! Что дало, кроме всего прочего, еще и серьезный экономический эффект.

На последней олимпиаде в Афинах была развернута, возможно, самая мощная на сегодня система безопасности, стоимость которой оценивается примерно в 300 миллионов долларов. Это огромное количество датчиков, микрофонов, видеокамер, которые фиксировали все, что творилось вокруг. Ясно, что такая система не могла работать в полностью автоматическом режиме, действовал также громадный человеческий ресурс. Но в списке ее технических возможностей значилась идентификация уличными микрофонами взрывов с надежным отсеиванием похожих событий: хлопков проколотых шин и пр.

Однако у нас — не Афины. В России отсутствует информационная система, способная оказать реальное противодействие терроризму. Какая там борьба, если до сих пор нет даже единой базы утерянных паспортов! Государство практически ничего не видит и не слышит. Если что-то происходит, начинается расследование, которое в лучшем случае ведется с помощью агентуры. В Москве сейчас реализуется большое число локальных систем безопасности: в частности, в метрополитене, и порой на улицах, ставятся видеокамеры. Есть и средства автоматической идентификации номеров, можно искать угнанные машины. Но масштабный эффект от всего этого станет возможен, только когда

будет создана централизованная база данных, система управления городом. Да, есть отечественные разработки, предполагающие возможность охвата целого муниципального образования и даже города. Хорошо, что они делаются на основе IP-протокола, с использованием сетевых технологий. Но даже глобальная система охраны города проблемы не решит, если отсутствуют системы диспетчеризации и управления. Многоуровневая информационная система не может быть создана, если отдельные ее компоненты отсутствуют или разрознены. И вряд ли она будет осмысленной, если ее компоненты проектируются и строятся порознь, а не интегрально. Между тем, именно так все у нас и происходит. Информационная разрозненность одновременно является и причиной, и следствием межведомственной разрозненности.

Чрезвычайная история

Что делает интеллектуальные системы наблюдения столь популярными? Любые ситуации, в том числе чрезвычайные, всегда имеют свою историю. И техника может помочь восстановить эту цепочку событий. В отсутствие техники источником информации становятся очевидцы, а людям свойственно ошибаться. Можно вспомнить тот же Беслан и разноречивые данные о числе заложников — были они ошибочны или искажены намеренно, но суть в том, что достоверная информация отсутствовала как таковая. Что доказывает: наша правоохранительная система не работает. И не только она, буксует все! Здесь не поможет техническая поддержка. Что даст оборудование отдельно взятого поста ГАИ интеллектуальной системой, ведущей контроль потока? Получится еще одна автоматическая «кормушка». Скорее всего, наблюдение за въезжающим и выезжающим транспортом с мониторингом скоростей и идентификацией номеров не даст полезных сведений, если не установлено еще и наблюдение за самими наблюдающими, отсутствует контроль их действий. Половинчатые решения, «недоинтеграция», блокирующая сведения на локальном уровне, лишь стимулирует произвол.

Что такое превентивное управление?

Чтобы сегодня перейти к процессу превентивного управления, нужна информация. Если фиксировать цепочки событий, предшествовавших различным чрезвычайным ситуациям, то есть накапливать соответствующие знания, то при появлении в других местах схожих «симптомов» можно вести превентивное управление ситуацией. К сожалению, мы не можем предвидеть события, которые еще не имели прецен-

тов — ведь у нас нет соответствующего опыта. И если информация не накапливается, то нечего и анализировать. Единственный способ накопления информации — внедрение интеллектуальных технологий мониторинга в домах, на улицах, в публичных местах. С помощью разобщенных, неинтегрированных систем строить цепочки событий нельзя.

Алгоритмы интеграционного процесса, в принципе, одинаковы для систем безопасности, энергоэффективности или каких-то других. Данный процесс, прежде всего, строится на аудите. Если нет цифр — показаний приборов автоматизированной системы, истории, кривых — что-либо сделать окажется крайне сложно. В противном случае результат достигается легко и просто. Это и есть то самое рациональное (превентивное) управление. Безопасность, как и энергосбережение — это вовсе не пуско-наладка той или иной аппаратуры. Нет! Решив заняться энергоэффективностью, мы вступаем на путь постоянной оптимизации всех процессов, происходящих в нашем здании. Нам придется раз за разом применять некие алгоритмы оптимизации, а затем оценивать полученный эффект. Для этого понадобится вычислительная платформа и «черный ящик», из которого можно будет извлекать цепочки событий.

Конечно, оборона всегда отстает от нападения. Но, выстроив эффективную линию обороны, можно затруднить атаку и даже сделать ее невозможной. Если хотите, невыгодной. Приведу пример: тему насильственных слияний и поглощений придумал один американец. Правительство США отреагировало очень быстро, введя 80% налог на эту разновидность бизнеса. Вот это и есть превентивное планирование.

Об информационных каналах

С «мозгами» информационной системы все более или менее ясно. С «глазами» и «ушами» — тоже. Датчиков, видеокамер и микрофонов должно быть много. А вот как быть с «нервами», по которым сигналы от органов чувств должны поступать в мозговой центр?

Недавно состоявшаяся конференция операторов сотовой связи показала, что данный рынок близок к насыщению. Сейчас количество абонентов сотовой связи составляет 57 миллионов человек, и это число увеличивается. Но количество «абоненто-часов» при этом остается практически прежним. Если раньше на каждого абонента в среднем приходилось двадцать минут в день, то теперь — пять. Поэтому отрасли сегодня нужен новый контент, способный восстановить ее реальный рост. Мы предложили включить в сети

GSM и GPRS роботов-машин. Чтобы выдержать при этом ряд требований к онлайн-услугам (в числе которых, естественно, безопасность), операторы связи должны произвести измерение собственных сетей, их настройку. Когда вы заказываете мелодию для своего мобильного, задержка в пару минут неважна. А вот в системе безопасности все тревожные сообщения должны передаваться в течение трех секунд. Плюс возникают вопросы по синхронизации и пр. Однако я уверен, что большинство операторов мобильной связи с удовольствием бы пошли на эти шаги, чтобы получить в качестве новых клиентов машины, которые куда-то смотрят, что-то слышат и чем-то управляют. Вероятно, сотовая связь не решит всех проблем, но попытаться с помощью сетей GSM создать универсальную услугу все же стоит, несмотря на мнение, что там, где производятся онлайн-операции, нужна проводная сеть. Проводные сети могут обслуживать городские пространства, а движущиеся объекты перейдут в сферу беспроводного сервиса.

Сейчас во всем мире усиленно разрабатывается идеология «3G» — вам гарантируется доступ, определенная пропускная способность и трафик, где бы вы в данный момент ни находились. И неважно, какие при этом используются средства связи: проводные или сотовые, наземные или спутниковые, стационарные или мобильные. Связистам стоит подумать о глобальной конвергенции всех видов связи с возможностью оперативного взаимного дополнения и замещения. На этой основе можно разработать качественную универсальную услугу, включающую и телевидение, и каналы передачи данных. Когда будет создана эта IP-сеть, станут широко востребованы и технологии интеллектуального здания, и интеллектуальные средства безопасности. Кстати, мы бы с удовольствием предложили в качестве альтернативы Интернет, но известно, что Интернет-пользователей сейчас в несколько раз меньше, чем абонентов сотовой связи.

Бесспорно, нельзя сбрасывать со счетов Wi-Fi и Bluetooth. Они позволят скорее совершить скачок в строительстве глобальных информационных сетей. В близком будущем каждый автомобиль будет оборудован персональным GPS-приемником. Но, вообще говоря, строительство сетей — вопрос освоения не только технологий, но и территорий. Если идет строительство, и так или иначе приходится тянуть кабель, почему бы в ту же самую канаву не «бросить» еще и оптоволокно? Просто об этом забывают. Газ — это да, как и электричество. Хотя это значительно более сложные и дорогие инженерные системы, чем оптоволоконная линия.

Самое правильное на сегодня решение: максимально быстро включить мониторинг

объектов с помощью любых подходящих для этого сетей и технологий, а затем постепенно переводить отдельные участки сети на кабель или оптоволокно.

Безопасность как один из компонентов комфорта требует подключенности. Как, впрочем, и другие компоненты. Всем нужен качественный и надежный ресурс, который позволит получать полноценные виды сервиса. Качать файлы MP3 — все-таки мальчишество. Нужна настоящая музыка, видео высокой четкости, различные онлайн-услуги. И, конечно, сама безопасность.

«Большой Брат» и демократия

По мере увеличения числа угроз человечеству набирает силу изнурительный спор между поборниками идей коллективной безопасности и защитниками демократических свобод. «Большого Брата» обвиняют в насаждении тоталитаризма, попрании священного права неприкосновенности личности.

Может ли Интернет служить орудием «электронных атак» и средством слежения? В принципе, да. Может ли сотовая связь стать средством тотальной слежки за населением? Запросто! Опасность того, что любое благо обернется во зло, есть всегда — все зависит от того, в чьи руки оно попадет, и как им захотят воспользоваться. Если страной правит хунта, технические средства (регулярная армия, спецслужбы) могут быть использованы против общества. Любым, самым безобидным предметом (скажем, кастрюлей) можно при желании исказить. И что, прикажете избавиться от кастрюль, электричества, телефонов, компьютеров, автомобилей?

Жизнь в информационном обществе предполагает подключенность. При этом никто никого насильно подключать не собирается: покупая сотовый телефон, вы выбираете подключенность к внешнему миру. Можете этого не делать, не пользоваться Интернетом, даже не писать писем. Тем самым вы обезопасите себя от возможного подслушивания и слежки. Но заплатите за это лишением абсолютно конкретных благ. Тогда уж лучше поселиться на необитаемом острове.

Входя в информационное пространство, мы отдаем себе отчет в том, что «подключаемся». И при этом демократические принципы несколько видоизменяются. Если ты купил себе средство коммуникации, которое имеет адрес и может быть использовано, в том числе, и против тебя — значит, ты сделал осознанный выбор. Не хочешь быть подключенным — не будь им.

Созданная нами искусственная среда обитания так или иначе переходит в глобальное информационное пространство. Если до недавнего времени связь была ус-

лугой, то сейчас она стала частью нашей среды обитания, самой средой. А любая среда всегда содержит в себе и полезные, и вредные компоненты.

Автоматическая идентификация в толпе людей, которые ведут себя агрессивно, значительно облегчает работу спецслужб. Это значит, что для достижения высокого уровня коллективной безопасности потребуются меньше необразованных милиционеров, которые будут заглядывать в паспорта и лица. Однажды, находясь не в лучшем строении, вы можете что-нибудь такое буркнуть стражу закона, а ему по чистой случайности сильно не понравится ваша физиономия. И вы окажетесь пораженным в своих демократических правах в гораздо большей степени, чем если на вас глазеет видеокамера. В отличие от людей, у машин нет эмоций!

Основной принцип демократии — это, прежде всего, уважение прав других членов общества в обмен на признание ими твоих прав. Элементарная, по сути, сделка — обмен лояльностью.

Государство регламентирует поведение своих граждан законами, а закон — это всегда ограничение свобод. Так давайте посмотрим: ограничение свобод в определенной степени — это благо или зло? Если принять второе, то следует признать абсурдность таких выражений, как «демократическое государство» и «демократические законы».

Впрочем, по этому поводу можно спорить бесконечно. Можно даже вынести тему спора на референдум. В самом деле, давайте представим себе электронный референдум: 57 миллионов владельцев мобильных телефонов дадут ответ («да», «нет», «воздержался») на ряд корректно formalизованных вопросов. Такое мероприятие с подсчетом голосов и выводом результата на графики (а при желании и с дифференциацией участников) займет от силы несколько часов. Если государству интересно мнение людей, оно может проводить такие референдумы хоть по несколько раз на дню. Тогда-то граждане и начнут реально участвовать в управлении государством. Вот вам, кстати, новая модель демократии информационного общества. Современная ее трактовка, причем не только «духа», но и «буквы»: ведь «демократия» означает власть народа!

Позиция технократа по поводу всего вышесказанного оптимистична: хотим мы или не хотим, но строим информационное общество, а значит, должны в него вписываться. Так что на сегодня наш вердикт: «Иметь!» — строить электронные системы на благо общества. Однако известно, что благими намерениями выстлана дорога в

ад. И это тоже необходимо помнить. А критерием оценки того, кто прав, а кто нет, является показатель устойчивого развития. Хорошо известный треугольник, внутри которого находится точка пересечения трех векторов: экономического, социального и экологического.

А ярые «поклонники» демократии почему-то (какие у них цели?) стремятся замедлить прогресс. И технический — создание совершенной информационной среды, и гуманитарный — повышение уровня защищенности людей.

Да и демократия, в конечном счете, не цель, а средство. Не общество ради демократии, а демократия — ради общества. И нечего носиться с ней, как с писаной торбой!

Так все-таки что выбрать?

Самое важное — сохранить право выбора. Но не во всем. Родину, родителей и эпоху не выбирают. Так и в наше время очень трудно выбрать «неподключенность». Просто нет смысла. Но можно выбирать отдельные ее фрагменты. Например, не смотреть

репортажи с мест трагических событий, тех же терактов. Многих это травмирует.

Между тем, в той или иной форме мы все давно подключены. К радио, к телевидению. В нас нещадно «закачивают» что ни попадя, от политики до рекламы. Ничего, пока держимся. Реклама — это, кстати, тоже тот еще вирус глобального масштаба, виртуальный терроризм, пожирающий наше время и деньги. В США недавно произошло весьма знаменательное событие. Доходы от платного телевидения впервые за всю историю превысили доходы от телерекламы! Значит, люди в конце концов предпочли свободу выбора информации.

Есть такой стандартный (и при этом правильный) вопрос: вы что, хотите жить в атмосфере тотальной слежки? Ваш «Большой Брат» будет пострашнее любого КГБ — просто потому, что он будет гораздо эффективнее. Но на этот вопрос ответ у меня давно готов.

Либеральность и прозрачность — два взаимосвязанных явления. Если движение в сторону прозрачности имеет позитивные экономические, социальные и экологические по-

следствия, то в политической сфере это приведет именно к либерализации. Нет между этими процессами непримиримых противоречий! Людям должно быть выгодно играть в открытые игры, и задача государства — локализовать игроков в закрытые игры и защищать от них тех, кто играет в открытую.

Один известный юрист сказал: если 93% населения делает нечто, то это нечто нужно принять как правомерное действие, изменив соответствующим образом действующий закон.

Сейчас общество из состояния потребления ресурсов переходит в состояние безопасности, достраивая еще один уровень известной «пирамиды Маслоу». Предыдущие уровни — еда, секс, развлечения и т.д. Насытившись всем этим, человек начинает претендовать на дополнительный уровень комфорта — он хочет жить в безопасности. Вокруг этого великого перехода и должна выстраиваться логика «подключенных» домов, систем коллективной безопасности и единого информационного поля.

