Система безопасности как дружественный пользовательский интерфейс

Жарков Иван Владимирович
инженер по проектным решениям MOBOTIX AG

Все мы хотим примерно понимать, куда движется рынок и технологии, с которыми связана наша работа. В процессе анализа развития систем безопасности лично мне приходит аналогия с развитием рынка вычислительной техники, а конкретно – персональных компьютеров.

Аналогия с рынком ПК

Становление рынка ПК происходило несколько раньше рынка систем безопасности в их современном представлении. И это развитие можно условно разбить на стадии. Вначале полная централизация – мейнфреймы с терминалами. Затем переход к максимальной децентрализации, связанный с появлением ПК. Вспомним слоган того времени: «Ваш персональный компьютер стал по-настоящему персональным!» Сегодня, с развитием каналов связи, способных обеспечить высокие скорости коммуникации, мы видим повсеместное внедрение веб- и облачных технологий. И даже постепенный возврат к концепции «тонкого клиента» с работой через облако и использованием его, облака, процессорных мощностей. Таким образом, в данный момент вершиной эволюции является устойчивая децентрализованная система самостоятельных устройств с высокой степенью централизации обработки данных и взаимодействия между ними. Однако подчеркну – на массовом рынке. В области специализированных IT-решений ситуация, вероятно, несколько иная, но мне трудно судить об этом, не будучи специалистом.

Какие же технологии победили в мире ПК? На данный момент, очевидно, что аппаратная платформа для массового рынка стала преимущественно унифицированной. Например, APPLE отказался от своих процессоров. Хорошо это или плохо для развития технологии – не очевидно, однако для конечного пользователя это скорее плюс.

Количество ОС сократилось до 3-х основных (Windows – MAC – Linux), которые занимают львиную долю рынка, и это уже спокойно воспринимается клиентом.

Немного разнообразнее развиваются конкретные программы-приложения. Но и здесь есть общепринятые стандарты – если документ, то WORD; если таблица, то EXCEL и т. д. Поэтому выбор приложений для большинства пользователей ограничен, зато получена совместимость всего со всем.

Максимальное же развитие получили прикладные веб-технологии. Конечному пользователю совершенно не важно, каким именно «гаджетом» он пользуется для заказа билетов или платежа через систему клиент-банк – обеспечивается совместимость практически любого клиентского оборудования.

Системы безопасности массового рынка

В области систем безопасности, и видеонаблюдения в частности, наблюдается если не аналогичная картина, то, во всяком случае, нечто близкое.

15 лет назад далеко не каждый мог позволить себе установить систему видеонаблюдения в квартире или на даче – весьма недешевое было решение. Сейчас оборудование значительно подешевело и рынок стал более массовым, что подталкивает его к более интенсивному развитию.

Субъективно, в настоящее время интегрированные системы безопасности еще проходят стадию становления стандартов и унификации. Например, стандарт ONVIF разработан довольно давно и принят большинством вендоров. Однако до сих пор есть определенные вопросы по совместимости, и 100% корректная работа по ONVIF – устройств разных производителей все еще не гарантируется. Надеемся, что постепенно стандарт будет становиться все более «стандартным».

Несмотря на некую «сырость» актуальных стандартов, очевидно, что в ближайшей перспективе на рынке массовых решений будут превалировать унифицированные технологии. Происходит выход на рынок глобальных игроков с телекоммуникационного рынка, которые наряду с предоставлением услуг связи, IP-телевидения и т. д. предоставляют облачные сервисы для систем видеонаблюдения. Пока, субъективно, эти сервисы еще не отлажены до конца: недостаточен срок реальной эксплуатации и должно просто пройти больше времени, чтобы эти системы стали привычными в быту. Но сейчас появились более-менее

удобные и доступные для каждого пользователя облачные сервисы видеонаблюдения – своего рода аналоги MS OFFICE 365 для CCTV с одновременной возможностью облачного и локального хранения записи.

Учитывая вышесказанное, можно заключить, что для массового пользователя при решении задач видеонаблюдения выбор камеры конкретного производителя и модели не столь важен, необходимо лишь обеспечить совместимость с общепринятыми стандартами, о чем уже позаботилось большинство производителей.

Особенности больших распределенных объектов

Однако задачи и особенности, возникающие при построении систем безопасности больших распределенных объектов, в значительно степени отличаются от задач массового рынка. Мой опыт однозначно говорит о том, что разработку любой серьезной системы необходимо начинать со встречи с заказчиком, обсуждения проблематики на объекте и разработки технического задания. Оно должно максимально подробно описывать функционал проектируемой системы, включая подсистемы видеонаблюдения, безопасности, автоматизации или их совокупности, объединенные в систему верхнего уровня.

При этом ситуация усугубляется тем, что далеко не всякий заказчик может четко сформулировать свои требования и пожелания. Более того, новые требования часто появляются уже по ходу реализации системы или на стадии опытной эксплуатации. Далеко не всегда пожелания заказчика удается облечь в сколько-нибудь стандартную форму, и уж тем более сложно технически реализовать неоднозначный (а порой и фантастический) функционал. Это непросто описать, трудно алгоритмизировать и почти невозможно реализовать.

За последние 10-15 лет системность решений в области охранно-пожарной сигнализации и видеонаблюдения значительно возросла. Субъективно, в 2000-2005 годах на рынке фактически не существовало решения на базе единой программно-аппаратной платформы, которая могла бы объединить под своим управлением системы видеонаблюдения, охранно-пожарной сигнализации и контроля доступа. Чаще всего на объекте устанавливалось несколько разнородных независимых систем, а у оператора было несколько АРМ, отдельных для каждой из подсистем, которые в лучшем случае взаимодействовали друг с другом на аппаратном уровне, а чаще работали фактически независимо.

С тех пор многое изменилось в лучшую сторону, и интегрированных систем, хотя и не всегда идеальных, на рынке представлено немало. Насколько корректно они работают – другой вопрос, но они есть. Однако за это время и требования заказчиков значительно возросли. Если раньше требовали совместную работу систем видеонаблюдения, охранно-пожарной сигнализации и контроля доступа, то сегодня это подразумевается по умолчанию, при этом система безопасности рассматривается как одна из подсистем в масштабе объекта.

Речь идет не о фантазиях, а о реальных пожеланиях заказчиков конкретных объектов. Рассмотрим несколько возможных сценариев.

Допустим, на крупном промышленном объекте были когда-то установлены и успешно работают системы видеонаблюдения, охранно-пожарной безопасности и контроля доступа, обеспечивающие свой привычный стандартный функционал.

После посещения аналогичного зарубежного предприятия руководством, с целью внедрения передовых технологий предлагается:

- Для повышения эффективности обеспечения трудовой дисциплины и контроля исполнения требований техники безопасности и снижения количества несчастных случаев – в обязательном порядке обеспечить все видеокамеры, обеспечивающие видеонаблюдение внутри периметра объекта, аналитикой, позволяющей определять наличие защитных касок на сотрудниках.
- Для постоянного контроля нахождения сотрудников (в т. ч. внутри опасных производственных зон – обеспечить всех сотрудников радиоидентификационными метками дальнего радиуса с тем, чтобы в любой момент времени понимать, находится ли кто-то внутри конкретной зоны, идентифицировать его, а также получать статистику по перемещениям сотрудника по территории объекта.
- Для повышения эффективности службы логистики и автоматизации процесса пропускного контроля – обеспечить контроль проезда автотранспорта на территорию предприятия не только по номерам автотранспорта/пропускам и паспортным данным водителей, но и при помощи автоматической системы распознавания лиц и типов автотранспортных средств. Т.е. при въезде система сама автоматически проверит соответствие номера и типа автомобиля/идентификатора пропуска, поднесенного водителем к считывателю/личности водителя, полученной от системы распознавания лиц/опционально скан-копии паспорта (или прав), которые водитель приложит к сканеру в точке проезда. Если все пункты проверки совпали – автомашина будет пропущена на предприятие, иначе дальнейшая проверка будет производиться уже сотрудником службы охраны.
- Для более эффективного видеонаблюдения, в условиях низкой освещенности, плохой видимости и на больших расстояниях, удаленного мониторинга и контроля температуры оборудования (с целью предотвращения возможного перегрева) и производственных процессов (с целью контроля соблюдения технологического цикла) – часть видеокамер заменить на тепловизионные, с функцией тепловой радиометрии. При этом, в одних случаях, о перегреве будет проинформирован оператор, а в иных – оборудование будет автоматически переведено на другой режим работы или полностью выключено.
- Для информирования службы логистики о необходимости подвоза дополнительных запасов, а также службы безопасности объекта на предмет возможных хищений и т. д. (в случае значительных расхождений) – автоматический анализ изображений участков складирования, расчета по изображениям количества сырья и сравнения полученных величин с величинами, полученными непосредственно с производства.

И это только краткий список. Если рассмотреть вышесказанное и расширить список задач, например, для системы «безопасный город» (или «интеллектуальный город», что становится более актуальным), то количество подсистем значительно возрастет – добавятся управление транспортными потоками, аварийно-технические службы и т. д.

Требования к исполнительным устройствам и платформам

При разработке и описании такой системы архитектору, пожалуй, даже необходимо на некоторое время абстрагироваться от конкретного оборудования (контроллеров автоматизации, видеокамер, исполнительных устройств), чтобы не стать заложником мнимых и истинных аппаратных ограничений. Необходимо мыслить исключительно на уровне поставленных глобальных задач. Под глобальные задачи будут подобраны программные системы более низкого уровня, которые, в свою очередь, объединят под своим управлением конкретные исполнительные устройства. Если провести аналогию с миром ПК, то исполнительные устройства – это «железо» вашего ПК – процессор, память, жесткий диск; системы видеонаблюдения, охранно-пожарной сигнализации, контроля доступа, обогрева и вентиляции, автоматизации зданий и т. д., объединяющие исполнительные устройства; «драйверы», обеспечивающие корректную работу с «железом». Далее все вышеперечисленное объединяется в систему верхнего уровня – эквивалент операционной системы.

Насколько мне известно, в данный момент полноценных унифицированных систем верхнего уровня, способных объединить разнородные подсистемы объекта уровня «интеллектуальный город»,

практически не существует – интеграторы пишут такое ПО под конкретную задачу/объект/заказчика. Или глубоко модифицируют существующее, ранее написанное, что обычно фактически эквивалентно разработке с нуля. Могу лишь предположить, что развитие этого направления пойдет таким образом, что в перспективе (пусть и не очень близкой) управление разнородными (под) системами на верхнем уровне будет осуществляться при помощи стандартных интегрированных программных платформ, ядро которых, вероятно, будут разрабатывать 3-4 крупных компании, а все остальные будут обеспечивать совместимый софт. Возможно, за такую унификацию придется заплатить уязвимостью. Стандартизация платформ и повсеместное их внедрение сделают такие системы более подверженными возможным атакам, поэтому уже сейчас IT-безопасность стала неотъемлемой частью любой интегрированной системы. Большая стандартная программная оболочка более подвержена атакам, а контроль над ней обеспечит и контроль над оборудованием. Избитый сценарий фантастического фильма, не так ли?

Какие же требования будут предъявляться во всей этой пирамиде конечным исполнительным устройствам?

- В первую очередь, от них, очевидно, будет требоваться максимально высокая надежность.
- Процесс взаимодействия между исполнительными устройствами в рамках одной подсистемы (например, системы видеонаблюдения), а в идеале – и в рамках смежных подсистем, должен происходить максимально надежно и быстро, минимально используя при этом ресурсы систем верхних уровней. Это обеспечит надежность, отказоустойчивость и быстроту работы.
- Все оконечные устройства должны предполагать 100% самостоятельную работу в случае потери связи с центром.

Таким образом, с одной стороны, для обеспечения максимального функционала и гибкости в настройках, решения поставленных разнородных и меняющихся задач система должна быть в значительной степени централизованной, эффективно и гибко объединять разные (под) системы в рамках единых стандартов и делать работу максимально удобной для пользователя.

С другой стороны, требования к надежности и устойчивости работы системы в случае потери связи, аварий и нештатных ситуаций предполагают корректную автономную работу и взаимодействие любых участков, подсистем и конечных устройств, т. е. максимальную самостоятельность и децентрализацию. И это более эффективно работает лишь в случае, если оконечные устройства будут к такой децентрализации способны, т. е. более приспособлены для автономной «самостоятельной» работы и прямой коммуникации со сторонними устройствами.

Позволю себе подытожить вышесказанное в отношении выбора камер для систем видеонаблюдения.

На рынке массовых решений для малых и средних систем видеонаблюдения, очевидно, будут преобладать камеры, поддерживающие стандартные протоколы взаимодействия (например, ONVIF). На камеры не будут возлагать очень сложных задач, и большая часть функционала будет решаться средствами центрального ПО.

В области сложных системных решений и построения крупномасштабных систем центральная интеграционная программная платформа будет играть исключительно важную роль, однако для достижения максимальной надежности, быстродействия и устойчивости всей системы в целом необходимо, чтобы конечные исполнительные устройства были приспособлены для автономной работы и прямой коммуникации друг с другом.