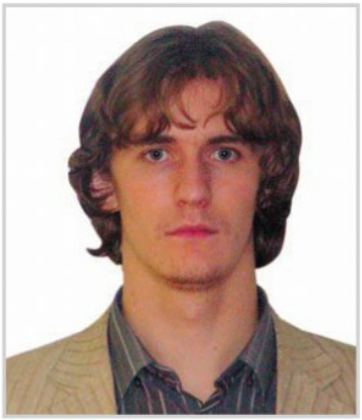

IP-технологии и модернизация ИСБ

Первое десятилетие нового века поставило перед разработчиками систем безопасности новые, более сложные задачи. Изменились сами угрозы, которые теперь приобретают террористический характер. При этом резко возросла степень организованности, оснащения и квалификации преступных групп. В связи с этим вопрос организации охраны объектов становится еще более острым. Могут ли ее обеспечить интегрированные системы безопасности (ИСБ) и какова сегодня тенденция их развития?

А.В. Леус
Заместитель заведующего кафедрой "Системы безопасности" МФТИ (ГУ)

Развитие технологий приводит в настоящее время и к отрицательным последствиям. Специальная физическая подготовка и оборудование позволяют нарушителям за короткое время преодолевать периметровые заграждения и оказывать сопротивление силам охраны. Таким угрозам могут эффективно противостоять только ИСБ – инфраструктуры, которые в конечном итоге обеспечивают высокую эффективность выполнения задач по охране объекта при оптимальной численности персонала и максимальной реализуемости его возможностей. При этом ИСБ должна позволять силам защиты реализовывать необходимую тактику действий – пресечение проникновения уже на периметре охраняемого объекта, перехват нарушителя на территории здания или его нейтрализация в данном районе. Поэтому чрезвычайно важно знать, как развивались интегрированные системы безопасности и аппаратные средства, их составляющие, какие преобразования они претерпели за некий период, как изменилось отношение заказчиков и инсталляторов к созданию систем.

Предпосылки для этих превращений определены бурным развитием информационных технологий. Растет вычислительная мощность компьютеров и пропускная способность сетей. Появилась возможность обработки и передачи огромных объемов информации, что позволяет развивать именно объединенные системы безопасности и в качестве интегрирующей платформы ИСБ в целом, и в качестве средства для повышения функциональности составляющих ее подсистем.

Системные интеграторы, кроме уже очевидного применения сетевого видеонаблюдения, все шире используют цифровые технологии в СКУД и охранной сигнализации. Например, связь контроллеров охранной сигнализации с серверами напрямую, без мастер-контроллеров и конвертеров, применение встроенных IP- и GPRS-коммуникаторов в контрольных панелях, интеграция на программно-аппаратном уровне СКУД и СТН (встроенная функция видеоидентификации) – все эти задачи решаются с применением IP-технологий. Внедряется поисковая видеоаналитика (отбор данных видеоархива по синхронизированному потоку метаданных). Становится возможным удаленное видеонаблюдение через глобальные сети в режиме реального времени, а также удаленное хранение и обработка видеоархива.

Наиболее ярко преимущества IP-решений видны в больших проектах, созданных, так сказать, по последнему слову техники. В некоторых интегрированных системах безопасности появился новый компонент – система сетевого компьютерного управления (ССКУ), которая позволяет не только контролировать потоки данных от технических средств охраны, но и администрировать рабочие места операторов, производить диагностику и дистанционное управление всеми техническими средствами, хранить информацию о работе системы, действиях операторов и т.п.

Наряду с вышесказанным можно указать и препятствия к достижению успеха, такие как отсутствие единого протокола передачи данных, который позволил бы обеспечить:

- совместимость различных аппаратных средств;
- гибкость построения системы;
- возможность последующей модернизации.

В связи с этим, действительно ли оправдались надежды на значительный прорыв в совершенствовании интегрированных систем безопасности на основе IP-технологий? Данный вопрос был адресован специалистам компаний – ведущих интеграторов рынка систем безопасности.

1. Как изменились технологии ИСБ с 2000 по 2010 г.?
2. Что главным образом стало причиной этих изменений?
3. Как повлияли IP-технологии на развитие ИСБ за прошедшие 10 лет?
4. Изменились ли предпочтения заказчиков в отношении ИСБ?
5. Стали ли внедрение и эксплуатация ИСБ более удобными и выгодными для инсталляторов и заказчиков с развитием IP?
6. Какими вы видите ИСБ в 2020 г.?

А.К. Крахмалев
Заместитель генерального директора ООО "Сигма-ИС"

1. Технологии построения ИСБ за это время мало изменились. Основные принципы конструкции и структуры ИСБ были разработаны в 1990-е гг. IP-технологии в то время уже активно использовались в ИСБ, только в основном на верхнем уровне интеграции – на уровне АРМ ИСБ (автоматизированных рабочих мест), которые (и раньше, и сейчас) строятся на базе компьютерных ЛВС. Некоторые из первых моделей ИСБ основывались исключительно на стандартных возможностях персональных компьютеров. Тогда это было явным недостатком. Развитие IP-технологий за прошедшие годы позволило существенно расширить их новые возможности применительно к ИСБ.

В целом ИСБ за это время развивались самостоятельно в части расширения своих функциональных и качественных характеристик. Можно отметить, что первоначальный всплеск интереса к ИСБ, проявленный в 2000–2002 гг., был связан больше с влиянием инновационного фактора, некоторого "модного" направления, которому стали с энтузиазмом следовать как разработчики, производители, проектировщики, так и заказчики. Однако к 2010 г. реальное количество ИСБ (серийное производство на российских предприятиях), завоевавших существенную долю рынка, можно пересчитать по пальцам одной руки.

Подтверждением перспектив развития ИСБ и интереса к ним в мировом масштабе служит тот факт, что в CENELEC (европейский комитет по электротехнической стандартизации) рассматривается проект международного стандарта, предложенного BSI (Британский комитет по стандартизации), Alarm systems – Combined and Integrated Alarm Systems – General Requirements ("Системы безопасности. Комбинированные и интегрированные системы безопасности. Общие требования"). В значительной мере на международный рынок повлияло развитие ИСБ в России, исследования, разработки, публикации российских специалистов.

2. Ключевым фактором в продвижении технологий ИСБ является потребность заказчика обеспечить безопасность, учитывая экономические интересы.
3. Наибольшее влияние IP-технологии в развитии ИСБ оказали на интеграцию СОТ в составе ИСБ. Появление цифрового видео, а затем и IP-видео, которое полностью базируется на IP-технологиях и Ethernet, сделало IP-сети основой для построения ИСБ. В связи с этим СОТ в ИСБ стало играть ключевую роль, что в принципе не совсем правильно, так как СОТ не может решить основные задачи обеспечения безопасности. Кроме того, СОТ – наименее автоматизированная составляющая подсистема ИСБ, и в ней велико влияние человеческого фактора. Глобальная перспектива развития ИСБ – расширение сферы защиты от различных угроз безопасности, а также снижение человеческого фактора в обеспечении безопасности.
В связи с этим можно отметить негативные моменты развития ИСБ. Некоторые разработчики, увлекаясь возможностями IP-технологий в СОТ, уделяли этой подсистеме ИСБ основное внимание в ущерб развитию остальных подсистем.
Из особенностей можно отметить также все более широкий переход на сети Ethernet при построении ИСБ и подключение напрямую к Ethernet контроллеров ИСБ (второй уровень сетевого взаимодействия в ИСБ).
4. Предпочтения заказчиков мало изменились. Им нужна защищенность в целом и обоснованность затрат на обеспечение безопасности. А каким образом она будет осуществлена, их мало интересует.

Если рассматривать в качестве покупателей ИСБ проектно-монтажные организации (они приобретают оборудование ИСБ, чтобы продать заказчику уже законченную систему – проектный продукт единичного производства для конкретного объекта), то с развитием IP можно отметить следующие моменты:

- IP-технологии предполагают большую стандартизацию и совместимость оборудования (наличие уже готовых компонентов различных производителей для построения IP-сетей), но требуют более высокой квалификации специалистов по проектированию, монтажу и обслуживанию;
- IP-оборудование, как правило, более дорогое и требует специальной программной поддержки и специалистов по программированию;
- открытость и широкая доступность IP-стандартов и IP-оборудования требуют особого внимания к вопросам защищенности от несанкционированного доступа как к аппаратным средствам, так и к информационным ресурсам, каналам.

Можно сделать вывод, что проектно-монтажным организациям (которые выступают в роли покупателей оборудования ИСБ) необходимы специалисты более высокой квалификации в области знания IP-технологий. Это будет влиять на стоимость системы для заказчика в целом.
Возможно также, что вопросами внедрения ИСБ будут заниматься организации, ранее специализировавшиеся исключительно на IP-системах.
5. Более удобными внедрение и эксплуатация ИСБ для инсталляторов становятся только в том случае, если имеются специалисты высшей квалификации. О выгоде инсталляторов трудно судить, поскольку она зависит от многих факторов.
Преимущества для заказчиков, как я уже говорил, будут выражаться только в экономии средств на безопасность при соблюдении заданного уровня защиты.
6. Перспективы развития ИСБ:

- расширение возможностей по защите от более широкого класса угроз (технологических, экологических, информационных и др.);
- интеграция с технологическим оборудованием. Управление устройством зданий позволит получить экономический эффект за счет внедрения энергосберегающих технологий, сокращения персонала, снижения расходов на обслуживание и т.д., что позволит перевести задачу обеспечения безопасности из области затратных расходов на самоокупаемость;
- расширение возможностей ИСБ для построения систем мониторинга безопасности территориально распределенных объектов.

С.И. Корчагин
Заведующий базовой кафедрой "Системы безопасности" МФТИ

1. Произошел переход от интеграции "на уровне проволочек", то есть релейной интеграции, к программно-аппаратной (уровень локальных процессоров и контроллеров) и программной интеграции.
Стало возможным реализовать не только жесткие алгоритмы взаимодействия систем, но и более гибкие, а также неалгоритмизованные реакции систем на события.
С 2000 г. явно прослеживается тенденция укрупнения систем, интегрирующих в своем составе десятки тысяч устройств.
2. Развитие объединяющей среды ИСБ за последние 10 лет, что обусловлено совершенствованием электроники в целом и, как следствие, информационных технологий.
Применение в индустрии безопасности прогрессивных технологий, ранее там не использовавшихся.
Совершенствование технологий подсистем: например, активное внедрение охранно-пожарной сигнализации с распределенной архитектурой, с адресными и адресно-аналоговыми извещателями и т.п.
3. Стало возможно управление большими базами данных и создание прогрессивных алгоритмов их обработки. Повысилась скорость и достоверность передачи информации. Произошел переход систем телевизионного наблюдения на сетевые решения.
4. Изменились предпочтения в основном мелких и средних заказчиков ИСБ в сторону "коробочных" IP-решений. Причина – простота инсталляции, создание разработчиками дружественных, привычных пользователю интерфейсов, сниженные требования к сервису и невысокие – к качеству телевизионного изображения, с одной стороны, и дополнительные возможности, как, например, получение более полной и комплексной информации о тревожном событии, учет рабочего времени и применение встроенной, хотя и упрощенной, видеоаналитики, с другой стороны.
В то же время некоторые крупные заказчики, настаивая на программной интеграции, выдвигают повышенные требования к защите информации, циркулирующей в системе, то есть охране сетей, и, кроме того, остаются приверженцами аналоговой формы видеоизображения. Действительно, IP-телевидение с исходным изображением формата PAL не оправдало ожиданий по разрешению, чувствительности, отношению сигнал/шум. К тому же оно часто требует большого трафика. Для повышения качества картинки стало возможным применение сетевых мегапиксельных камер, но такое решение предъявляет дополнительные требования к организации сети высокой пропускной способности и обязательному наличию охранного освещения, интегрированного в ИСБ.
5. Сократился объем монтажных работ, но, с другой стороны, увеличился масштаб пусконаладочных и шеф-монтажных работ, потребовалось значительное число новых специалистов по сетевым технологиям. Систему усложнили, получилось, что включить просто, а настроить и реализовать все функции трудно.
Иногда препятствием для внедрения ИСБ становится стремление заказчика из ложных соображений экономии использовать уже имеющуюся корпоративную IP-сеть как основу для интегрированной системы безопасности, а не прокладывать новую, несмотря на ограничение пропускной способности уже имеющейся, что зачастую приводит к задержке передачи изображения и, как следствие, потере актуальности видеоинформации.
Усложнилась политика ценообразования предложения.
6. IP-технологии развиваются самостоятельно и независимо от индустрии систем безопасности и как среда для передачи данных будут востребованы в ИСБ. Применительно к ИСБ актуально создание защищенных объектовых беспроводных сетей (возможно, и с использованием спутниковой связи).
В то же время должны развиваться сами интегрированные системы безопасности. Можно выделить желательные и наиболее перспективные направления продвижения:

- Повышение обнаружительной способности извещателей с более эффективной и точной локализацией места тревожного события, возможно, на новых физических принципах.
- Получение видеоизображения с более высокими характеристиками по передаче низкого контраста, при слабых освещенностях сцены.
- Применение спектральной фильтрации для повышения воспринимаемого контраста изображений.
- Более плотное взаимодействие систем путем увеличения объема передачи информации от системы к системе, что приведет к высокой

периферийных контроллеров системы), резервирования линий связи и т.д.

Так или иначе вопрос интеграции систем возникает все чаще, и применение интегрированных решений будет со временем расширяться, потому что такова логика развития технологий.

2. Потребности заказчиков и ответные инициативы разработчиков. По большому счету задача для каждого объекта всегда одна – создать эффективный инструмент, с помощью которого какая-то часть угроз будет отсечена, а остальные станут прозрачными и видимыми раньше, чем нанесут ущерб. И вся эволюция технологий – движение к тому, чтобы решить эту проблему как можно лучше. И вот здесь уже возникают различия в подходах. На наш взгляд, эффективность системы или решения во многом определяется его устойчивостью к человеческому фактору и соответственно способностью минимизировать его негативные влияния на ту или иную ситуацию. Эта логика прослеживается и в развитии технологий: сегодня при работе с системой безопасности требуется все меньше человеческих навыков и все больше задач решается техникой, заданными алгоритмами и сценариями.

3. IP-технологии создали предпосылку и техническую возможность для того, чтобы ИСБ получили широкое распространение. Во-первых, возросла надежность и скорость сетевых интерфейсов. Во-вторых, снизилась стоимость сетевого оборудования. Это подтолкнуло разработчиков и производителей выпускать больше продуктов с сетевыми интерфейсами. С IP стало удобнее и проще работать, легче обслуживать. И самое главное, у IP-систем значительно больше возможностей.

4. Предпочтения и подход меняются. Пока не каждый заказчик готов инвестировать свое время и средства в построение мощной интегрированной системы, которая заработает в полную силу через какое-то время. У многих крупных заказчиков есть свои стандарты и требования к системам безопасности, которые разработаны достаточно давно и меняются довольно редко. Они зачастую взаимодействуют с конкретными интеграторами, в положениях указаны определенные программно-аппаратные комплексы. И здесь не всегда есть соответствие между возможностями тех систем, которые включены в стандарты, и задачами, которые необходимо решать.

Но практический интерес к интеграции, в том числе с использованием IP-технологий, заметно возрос. При выборе систем клиенты стали интересоваться наличием IP-технологий в предлагаемых решениях. В некоторых случаях узнают о возможности построения системы безопасности, используя существующую IP-сеть предприятия с целью экономии.

Когда именно на рынке произойдет окончательная смена предпочтений, сказать сложно, поскольку это зависит от многих факторов: и от тактико-технических характеристик систем, и от стоимости внедрения, и от совокупной цены владения, и от конкретных людей, которые оценивают технологии, готовят технические задания и принимают решения о том, что и зачем будет внедряться. У нас есть и такие заказчики, которых не нужно убеждать в полезности интегрированных решений и преимуществах IP. Они прекрасно разбираются во всех данных аспектах и ставят задачи по верхней планке.

5. И внедрение, и эксплуатация ИСБ с развитием IP стали привлекательнее, поскольку это все-таки единый стандарт с общим протоколом взаимодействия. Для клиента выбор такой системы логичен и по экономическим причинам, и по технологическим. Инсталлятору IP дает возможность расширить свое предложение и в конечном итоге больше зарабатывать.

6. 10 лет – большой срок, учитывая сегодняшние темпы развития технологий. Думаю, что будет разработан единый открытый стандарт, который станет определять протоколы сетевого взаимодействия оборудования. Сейчас уже на рынке IP-видео успешно зарекомендовал себя ONVIF. Следующий шаг – за интегрированными системами. Общая тенденция такова: больше возможностей, выше надежность, проще взаимодействие, прозрачнее границы. В обозримой перспективе само содержание термина ИСБ существенно изменится: во-первых, за счет усложнения задач, во-вторых, за счет пересечения со смежными областями, например с ИТ и т.д.

А.М. Омельянчук
Начальник конструкторского бюро
ООО "Сигма-ИС"

1–2. 2000 год был вообще довольно специфическим: недавно "громыхнул" август 1998 г., началось активное импортозамещение, да и вертикали власти тогда не было, а соответственно существовал совсем другой состав платежеспособных покупателей.

С тех пор произошло многое. С чисто технической точки зрения в 2000 г. бедные заказчики предпочитали интегрировать системы "проводочками", а богатые хотели компьютерную систему. Сейчас ситуация почти обратная: малоимущие покупатели берут компьютерную систему, а богатые спрашивают, насколько надежно и насколько "интегрированно" система будет работать при выходе из строя компьютера, или говорят: "Хорошо, пусть интеграция будет на компьютерах, но нельзя ли на рабочих местах персонала обойтись без них?"

Второе существенное отличие связано со смещением денежных потоков. Ныне основные заказчики интегрированных систем – государственные ведомства и полугосударственные монополии. Положительной стороной такого смещения является пункт в тендерной документации о предпочтительности отечественного оборудования. В начале 2000-х гг. оно занимало довольно узкую нишу "крайне дешевого оборудования" (устанавливаемого, например, для защиты не от пожара, а от пожарника), а также довольно низкую нишу "оборудования для вневедомственной охраны" благодаря протекционистской политике этой организации. Про интегрированные системы в них никто и не заикался.

Теперь же существует довольно много отечественных производителей оборудования и программных средств, ориентированных на создание сложных интегрированных систем для крупных объектов. Как правило, это не массовое оборудование, так что, хотя качественные параметры совсем немного превышают его характеристики, цена отличается значительно сильнее.

Наконец, производители устройства, изначально ориентированного на заказчиков, вовсе не требующих интеграции, также сместились в сторону интегрированных систем. По мере развития опыта инсталляторов оказалось, что "немножко интеграции" совсем не дорого. Поэтому возникли и получили широкое распространение интегрированные системы, основу которых составляет оборудование, предназначенное для самых простых объектов, зато широко известное и привычное.

5. Наверное, в вопросе имелось в виду не развитие IP как такового. Появление IPv6 – конечно, важный момент, но заказчики систем безопасности в большинстве своем, наверное, о нем даже не знают. Видимо, речь идет о распространении так называемых IP-систем, к которым обычно относят любое оборудование с Ethernet-разъемом. Должен сказать, что в этом отношении ничего особого для интегрированных систем не произошло. Революционным стал переход (точнее, его начало) от коаксиального кабеля к Ethernet в системах видеонаблюдения. Что же касается интегрированных систем в целом, то Ethernet-ориентированное оборудование для них – до сих пор редкость и оно является скорее вспомогательным способом для подключения компьютеров, но не основным естественным интерфейсом внутрисистемной связи. Более того, в пожарных системах ныне фактически запрещено использование Ethernet, поскольку главное его преимущество – применение существующей инфраструктуры СКС – невозможно. Даже если вы готовы проложить для пожарной сигнализации огнестойкий кабель, вряд ли вы намерены проложить им всю сеть в здании – дороговато, да и с точки зрения собственно Ethernet такие кабели значительно хуже обыкновенных.

Кроме того, наличие Ethernet-разъема вовсе не облегчает интеграцию подсистем. Даже если помимо возможности подключения на физическом уровне в оборудовании реализована (а пока это осуществлено в основном в устройствах видеонаблюдения, да и то не в любых) возможность управления им из обычного Web-браузера, это вовсе не означает, что его легко интегрировать.

6. Тем не менее, несмотря на высказанный выше пессимизм по поводу IP-систем, я предполагаю, что в дальнейшем интеграция будет приходить на основе IP-каналов, а кроме того, она будет шире – затронет такие смежные области, как управление зданием, контроль энергоресурсов, экономика, учет и управление производством. Соответственно способы объединения будут активно заимствоваться из этих смежных областей, в которых значительно дальше продвинулась стандартизация межсистемных интерфейсов.