КОМФОРТ И БЕЗОПАСНОСТЬ В ИНТЕЛЛЕКТУАЛЬНОМ ЗДАНИИ – ЗВЕНЬЯ ЕДИНОЙ ЦЕПИ!

С. Виноградов
д. т. н., академик Академии безопасности, обороны и правопорядка

В настоящее время много говорится и публикуется информации в тематических изданиях по теме "интеллектуальное здание" (ИЗ). Как правило, рассматривается достаточно большая группа тем по стандартизации, классификации, функциональным и техническим возможностям с позиции объединения систем автоматического управления и контроля (свет, вода, климат), диспетчеризации процессов (применение компьютеров, сетевые решения, программные средства), системы информационные, жизнеобеспечения и связи (программируемые контроллеры и системы, системные шины передачи данных, стандарты в протоколах обмена, варианты организации структур СКС) охранные (ОПС, ОС, пром. и охранное телевидение, СКУД), измерительные системы и многое другое, в зависимости от осведомленности специалистов в том или другом вопросе.

Интеллектуальная система есть совокупность или множество субъектов и объектов (систем), связанных между собой организационно, т.е. находящихся в состоянии активности и противостояния друг относительно друга и под воздействием внешнего мира.

Как правило, каждая из систем, в наше время, является интеллектуальной, состоящей из нескольких подсистем, и может претендовать на центральную роль в объединении остальных систем. Поэтому специалисты разных направлений и продвигают весьма привлекательную идею ИЗ с позиции своих знаний и корпоративных взглядов с привязкой к технической поддержке со стороны производителей и поставщиков оборудования и технологий, подходящих для решений таких, весьма непростых задач.

На основании произведенной оценки достаточно легко можно выделить технологии, исторически развивавшиеся независимо, с применением самых современных технических достижений, но сформировавшихся со временем до такой стадии, когда интеграция между ними стала возможна и полезна (см. рис.).

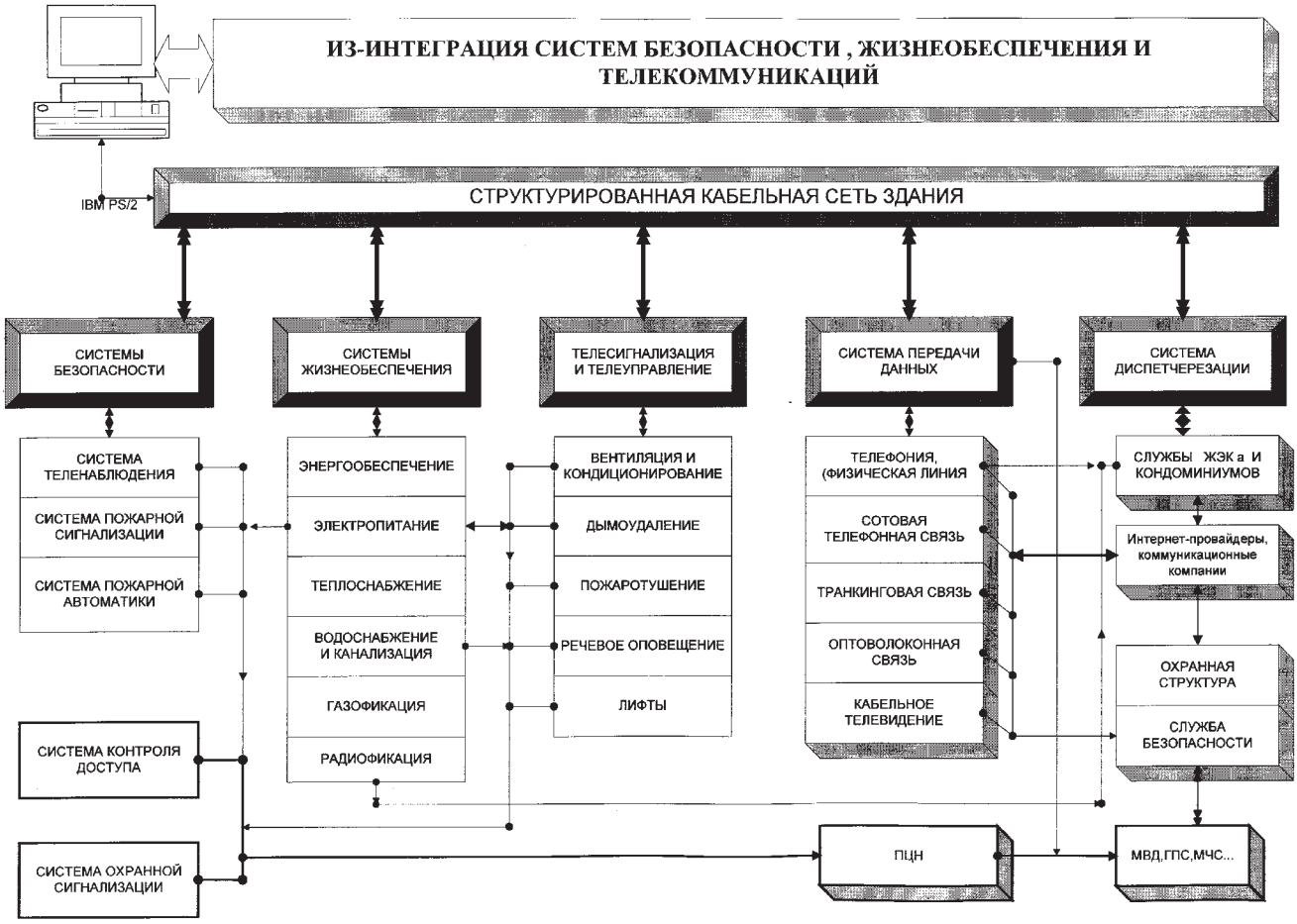
Например, концепция интеллектуального здания продвигалась исторически в первую очередь производителями СКС. Придя к концепции универсальной структурированной слаботочной кабельной системы здания, они вполне логично решили распространить этот подход с физической среды передачи данных и на другие системы, и подошли плотно к идее реализации ИЗ. К тому же, концепция ИЗ оказалась хорошим "локомотивом" для продвижения СКС, поскольку СКС может служить базой даже для весьма сложных решений, не говоря уже о более прозаических потребностях.

Вполне очевидно, что все серьезно занимающиеся кабельным бизнесом компании с энтузиазмом отнеслись к идее ТАКОЙ ИНТЕГРАЦИИ и активно начали ее продвигать на рынке услуг, естественным образом расширяя приложение и до уровня слаботочных систем в части охраны и комплексной безопасности. Концепция ИЗ стала продвигаться практически сразу, как только бизнес в области инсталляций СКС встал на ноги. С появлением кабельных подразделений у большинства сетевых интеграторов идея ИЗ получила массовую поддержку.

Отсутствие должного опыта у коммуникационщиков в данной сфере не замедлило сказаться, так как " безопасность" принадлежит другой плоскости организационных и нормативно-правовых аспектов регламентирующих деятельность в данном направлении, и нахрапом здесь ничего не решишь, ведь здесь речь идет уже не о технических вопросах и идеях, а о безопасности жизни людей и сохранности материальных ценностей.

Увлеченность ИЗ, (вкупе с естественным стремлением развивать бизнес) естественным образом, после накопления " шишек" привела к тому, что многие ведущие инсталляторы СКС в России, либо вывели свой бизнес на новый интеграторский уровень, активно привлекая опытных специалистов, для профессионального разрешения круга вопросов, связанных с обеспечением различных аспектов комплексной безопасности, либо кооперировались с организациями, профессионально занимающимися системной интеграцией в системах безопасности (либо и то и другое сразу).

Также не стоит забывать, что ряд Западных производителей СКС (Lucent, Siemens, Alcatel) активно занимаются и сетевым, и телекоммуникационным бизнесом, они же



являются крупнейшими системными интеграторами и могут своими силами реализовывать решения для ИЗ.

Словосочетание "интеллектуальное здание" достаточно прочно утвердилось в лексиконе специалистов, но, в отличие от многих других концептуальных понятий, его еще рано считать устоявшимся термином, по крайней мере, в нашей стране. Поэтому цель данного обзорного материала, в подготовке которого мне помогали многие специалисты компаний системных интеграторов, акцентировать внимание наших потенциальных читателей-специалистов, занимающихся вопросами обеспечения безопасности, с позиции реализации возможностей технологий ИНТЕЛЛЕКТУАЛЬНОГО ЗДАНИЯ. Надеюсь, это поможет правильно оценивать ситуацию и рационально подходить к выбору технологических, технических, экономических решений при реализации таких проектов, а также позволит избежать досадных промахов и убережет от возможных ошибок и неблагоприятных последствий.

Основная технологическая идея ИЗ

В отличие от традиционно принятых схем оснащения зданий техническими средствами, в ИЗ предлагается построить систему коммуникаций, при которой создается так называемая информационная транспортная магистраль, внутри которой происходит передача информации и управляющих сигналов с центрального поста к периферийному оборудованию и наоборот. Поскольку в этом кольце присутствуют все сигналы, то создаются условия, при которых становится возможным централизованное управление всеми системами в комплексе.

Преимущества такого подхода

Подобное построение дает целый ряд преимуществ:

- имеется реальная возможность поставить действия каждой системы в зависимость от действий любой другой системы;
- получается очень гибкая схема, при которой технические средства внутри помещений можно менять. Так, если в какой-то кабинет приходит десять портов, то они могут быть заняты любой аппаратурой – телефонами, компьютерами, различными датчиками, телевизионными камерами. Все это оборудование можно установить одновременно;
- пропускная способность самой информационной транспортной магистрали может наращиваться без проведения каких-либо капитальных работ;
- при необходимости крупного расширения технических систем (строительство еще одного здания, пристройки к существующему, создания комплекса зданий) можно создать новые информационные кольца.

Соединив их с существующими, в новых помещениях появляются те же возможности, что и ранее;

- выбранные системы можно развивать и создавать новые, постепенно наращивая их, в зависимости от финансовых возможностей;
- обеспечение безопасности на предприятиях пойдет по пути реализации лучших достижений интегрированных комплексов технических систем, тем самым создавая условия для снижения затрат на их содержание.

Это означает, что само здание должно быть спроектировано так, что все сервисы могли бы интегрироваться друг с другом с минимальными затратами (с точки зрения финансов, времени и трудоемкости), а их обслуживание было бы организовано оптимальным образом.

Вместе с тем ИЗ должно отвечать задачам бизнеса, т. е., внедрение той или иной функциональности должно быть экономически оправдано.

Какие перспективы у технологий ИЗ (умного дома)?

По мере того как производители электронного оборудования будут налаживать отношения со строительными организациями, станет появляться все больше домов, подготовленных для раз-

вертывания широкополосных приложений. Наибольший интерес, скорее всего, вызовут развлекательные приложения, а не возможности управлять электроосвещением и функции обеспечения безопасности. Чем шире и быстрее продвигаются перспективные технологии глобальной информатизации и доступа, тем доступнее становятся и технологии вызывающие сбои и наносящие ущерб системам, обеспечивающим всеобщую глобальную информатизацию.

В таком широкомасштабном процессе неизбежен процесс формирования массового дилетантского подхода со стороны пользователей всемирными сетями к системам безопасности и их функциям в составе интеллектуальных технологических решений (например, применение сотового телефона в качестве устройства передачи кода для постановки или снятия объекта с охраны!!). Поэтому у специалистов компаний системных интеграторов по обеспечению безопасности таких объектов постоянно будет прибавляться работы.

Стандарты в ИЗ

Все современные более-менее развитые системы имеют интерфейсы для электронного управления, так что разработать средства для их интеграции не составляет особого труда. Проблема в том, что производители этого оборудования, естественно, не рассчитывают, что оно будет подключаться в сеть, да еще по витой паре, а тем более по волоконной оптике. В результате попытки перевести охранную или пожарную сигнализацию на трассы СКС, существующие стандарты и нормы для ОПС, вступают в противоречие с концепцией универсальной проводки. Проблема на первый взгляд кажется неразрешимой. К счастью, у отрасли наконец-то стали появляться открытые стандарты на сети контроля и управления различными устройствами.

На сегодняшний день, наиболее широкое распространение получили стандарты: BACNet и LonWorks. (Building Automation Control Network). Стандарт предусматривает использование программируемых контроллеров, причем они могут быть объединены в сеть при помощи различных сред. Таким образом, контроллеры выступают промежуточным звеном между практически любыми устройствами, к которым они подключаются по нестандартным интерфейсам. Связь же между контроллерами и системой управления осуществляется по общей сети.

Некоторые трудности субъективного свойства

Специалисты признают, что при реализации проектов интеллектуального здания им пока удается достичь "уровня интеллектуализации" приблизительно процентов в 30-60 от реально возможного. Одна из причин такого положения дел, как правило кроется в нехватке средств у заказчика (или нежелании их пока тратить на перспективные идеи), для внедрения концепции ИЗ в России.

Уже отмечалась важная роль стандартов при построении ИЗ. С точки зрения технологии и технических решений систем путь к реализации проекта интеллектуального здания в российской строительной индустрии открыт. В техническом отношении все подготовлено и решено. Сложнее обстоит дело с нормативной базой и российской ментальностью.

Приведем лишь несколько примеров. Так, реализации идеи объединенной кабельной системы препятствуют существующие нормативные акты, регламентирующие способы прокладки силовых и слаботочных кабельных сетей. Несмотря на очевидные преимущества объединения кабельных каналов, в нормативном плане этот вопрос пока до конца не отрегулирован, хотя и наметилось некоторое оживление.

Актуальна и проблема интеграции систем жизнеобеспечения и безопасности, в частности, использование современных адресно-аналоговых систем пожарной сигнализации (ПС) и адресных систем охранной сигнализации (ОС) в составе единой автоматизированной системы управления – АСУ ИЗ.

Типовые варианты реализации проектов интеллектуального здания

Реализация проекта интеллектуального здания (ИЗ), существенным образом отличается от традиционной схемы построения здания. Главной и определяющей составляющей организационно-технических мероприятий, проводимых заказчиком на этапе принятия решения о строительстве ИЗ, является выбор генерального подрядчика по строительству и инженерным системам. При традиционной схеме "строительный" генподрядчик имеет дело с большим количеством субподрядчиков, отвечающих за одну-две инженерные системы. Каждый из субподрядчиков стремится сузить круг своей ответственности. Он заинтересован лишь в скорейшем выполнении своей части работ и не заинтересован в конечном результате.

Иначе обстоит дело при построении интеллектуального здания. Здесь заказчик "работает" с одним подрядчиком - системным интегратором, который реализует технические решения по всему комплексу систем инженерного оборудования ИЗ. У заказчика вместо "головной боли" – общение с представителем ведущей компании, решающей весь комплекс вопросов.

Такая компания – системный интегратор – не только оснащает объект всем необходимым инженерным оборудованием, но и осуществляет его обслуживание на всех этапах "жизни". Поэтому системный интегратор "кровно" заинтересован в оснащении здания надежным и эффективным оборудованием, "правильно" структурированными, взаимодействующими по заданным алгоритмам комплексами систем. Вместо многочисленных разрозненных служб эксплуатации в ИЗ функционирует одна (или несколько) диспетчерских служб, контролирующих состояние всех систем и осуществляющих координацию работы специализированных бригад. Обслуживание всего комплекса систем осуществляет одна компания – как правило, именно та, которая проектировала ИЗ и выполняла пусконаладочные работы.

Таким образом, выбор подрядчика, способного предложить интегрированное решение по инженерному оборудованию здания, становится важнейшей составляющей при построении ИЗ независимо от того, проектируется ли небольшой загородный дом или многоэтажный гостиничный комплекс. В этом, так сказать, основной организационный принцип построения интеллектуального здания.

Важной структурной единицей ИЗ является единый центр диспетчеризации, осуществляющий контроль за состоянием всего комплекса и управление системами жизнеобеспечения здания. Для правильного его функционирования необходимо предусмотреть всевозможные взаимосвязи между отдельными системами, степень их интеграции и структуру аппаратно-программного обеспечения центра.

Поэтому при проектировании ИЗ одним из определяющих принципов является формирование единого подхода при построении всех систем различных комплексов:

- комплекс систем безопасности;
- комплекс систем жизнеобеспечения;
- комплекс систем информатизации;
- структурированная кабельная система;
- единый центр мониторинга, диспетчеризации и управления (АСУ зданием).

Такой унифицированный подход к формированию многофункционального комплекса систем проще достичь, если "дело" по созданию интеллектуального здания поручить одной фирме – системному интегратору, который берет на себя всю ответственность за конечный результат.

Новые горизонты функциональных возможностей

Интеллектуальность здания напрямую будет зависеть от того, какие функции будут выполняться автоматически без участия человека: в ЕГО отсутствие охранять дом и сообщать ЕМУ и на пост вневедомственной охраны о несанкционированном доступе (либо возгорании, и т.д.), контролировать микроклимат в помещениях и поддерживать его на заданном уровне, включать и выключать бытовые приборы в нужное время, отключать освещение в пустых помещениях и включать его при появлении или с наступлением сумерек и т.д. В данном случае следует представлять необходимый перечень подсистем "интеллектуального здания", определяющий и возможности "Вашего" ИЗ – "умного здания".

К таковым подсистемам можно отнести:

- Автоматизированная система управления эксплуатацией здания.
- Кабельная канализация и механические конструктивы.
- Единая структурированная кабельная система.
- Система сбалансированного электропитания.
- Система жизнеобеспечения:
  - *управление вентиляцией и кондиционированием воздуха:*
    - регулирование температуры и влажности воздуха;
    - поддержание заданных параметров воздуха;
    - перевод систем в энергосберегающие режимы работы в часы пониженных нагрузок;
    - отработка заданных алгоритмов включения/выключения местных вентиляционно-кондиционирующих установок;
    - перевод систем в аварийные режимы работы (например, удаление дыма).
  - *управление тепло- и водоснабжением:*
    - управление режимами работы локальной котельной;
    - стабилизация тепловых режимов системы;
    - стабилизация гидравлических режимов работы систем;
    - перевод систем в аварийные режимы работы
  - *управление электросбережением:*
    - контроль параметров сети и положения коммутационных узлов;
    - обнаружение аварийных и предаварийных ситуаций по отклонению параметров (провалы и выбросы напряжения, отключения, высоковольтные пики, шумы и импульсные помехи, отклонения от частоты) и положению коммутационных узлов;
    - автоматическое переключение на резервное или автономное энергоснабжение;
    - дистанционное управление коммутационными узлами энергосистемы;
    - контроль энергопотребления с учетом и регистрацией как по зданию в целом, так и по конкретным потребителям;
  - *управление освещением:*
    - плавная регулировка освещения в зависимости от времени суток, погоды, присутствия людей в помещении;
    - режимы освещения (ночной, дежурный, аварийный, рабочий, имитация присутствия и проч.);
    - управление жалюзи и шторами;
- Локальная вычислительная сеть.
- Автоматические телефонные станции.
- Система коллективного приема телевизионных сигналов и КТВ.
- Автоматизированная система лифтового оборудования.
- Система электрочасы.
- Комплексная Система безопасности (КСБ):

КСБ обеспечивает защиту жизни и здоровья обитателей здания, защиту материальных и информационных ценностей, защиту собственных ресурсов комплекса и технических средств и т.д.

В состав КСБ, обычно включают следующие составляющие:

- система охранно-тревожной сигнализации;
- система управления доступом;
- система телевизионного наблюдения;
- система сбора и обработки информации;
- системы пожарной сигнализации и оповещения о пожаре;
- система автоматического пожаротушения.

В России уже появились системы охранной и пожарной сигнализации, построенные в соответствии со стандартом "открытых систем" (по технологии LonWorks), что кардинально изменит ситуацию с интеграцией КСБ.

- Телекоммуникационная подсистема.
- Радиовещание, оповещение, система управления эвакуацией людей при чрезвычайных обстоятельствах.

Это далеко не весь перечень возможности систем, предназначенных для функционирования в составе комплексов для интеллектуальных зданий. Структура ИЗ выполняется таким образом, что функционально ее возможности можно нарастить по мере необходимости.

Преимущества перспективных технологий интеллектуального здания

Интеллектуальное здание – это здание или комплекс зданий, в проектировании, строительстве и эксплуатации которого использованы современные технологии, позволяющие управлять всем жизненным циклом здания и его подсистемами как единым целым:

- Единое управление инженерными системами здания позволяет отслеживать сроки замены оборудования, прогнозировать и оптимизировать расходы на поддержание систем в рабочем состоянии. Также системы обеспечивают комфорт людей, находящихся в здании, и определяют уровень престижности объекта.
- Автоматизированный учет коммунальных услуг позволяет учитывать и прогнозировать все расходы на электроэнергию и теплоносители, выбирать оптимальные режимы энергопотребления, принимать меры по экономии энергии.
- Интегрированное управление безопасностью упрощает процесс страхования имущества и обеспечивает защиту людей и собственности. Корректная работа систем безопасности также определяет уровень престижности объекта.
- Автоматизация управления бизнес-процессами позволяет учитывать и анализировать расходы по эксплуатации здания в целом, разграничивать расходы между арендаторами за использование электричества, парковки или других ресурсов, своевременно выставлять счета арендаторам и эффективно управлять всеми ресурсами здания через единую систему.

По сравнению с автономными системами комплексная система имеет следующие преимущества:

- существенная экономия на кабельных сетях и сетевом оборудовании;
- снижение энергопотребления и повышение надежности всей системы;
- повышение оперативности управления объектом;
- графическое представление информации о состоянии систем и оборудования на различных уровнях (объектовом, зональном, адресном);
- снижение трудозатрат эксплуатационных и диспетчерских служб;
- обеспечение необходимого взаимодействия систем;
- снижение вероятности возникновения страховых случаев;
- "открытость" комплекса, обеспечивающая возможность его наращивания и использования оборудования разных производителей.

Формирование в здании инженерной инфраструктуры типа ИЗ существенно повышает его ликвидность. ИЗ - это эффективное инвестиционное решение, позволяющее существенно снизить расходы на обслуживание и развитие. Такое здание соответствует современным международным требованиям и является привлекательным рыночным товаром.

Подводя некоторый итог, хотелось бы отметить следующее:

ПРОФЕССИОНАЛАМ, объединившим, наконец, свои усилия по продвижению технологий ИЗ, прежде всего, нужно определиться не в том какие системы и устройства, элементы систем, датчики и извещатели относятся к представлениям об интеллектуальном здании, а как правильно и рационально их скомпоновать, на каком уровне и в каком объеме будет происходить обмен информационными потоками, и с применением каких технологий защиты информации по каждому уровню интеграции в составе комплекса АСУ ИЗ.

Необходимо четко определиться, что относится к строительной части при проектировании и строительстве объектов с такой инфраструктурой, а что относится к приоритетам компаний-системным интеграторам, в части формирования организационно технических и технологических решений применительно к объекту ИЗ.

Если речь идет только об инсталляции ИЗ с применением технологии СКС, то главенство на объекте (и в проекте) принадлежит, как правило (вполне оправданно), "строителям" уже накопившим ранее "необходимый" опыт.

В случае если инициатива реализации ИЗ с самого начала проекта идет со стороны системного интегратора, приоритет в решениях, очевидно, должен быть за ним, но и в том и в другом случае предлагаемые решения должны быть технологически и технически совместимы и взаимозаменяемы.

В отечественной строительной индустрии существуют свои традиции. Это, конечно же, неплохо, если бы только отдельные привычки не мешали новым подходам. Дело в том, что технологии и принципы построения ИЗ, должны учитываться уже на этапе архитектурного проектирования. У нас же довольно распространенной является ситуация, когда об инженерной "начинке" вспоминают уже после возведения коробки здания (а иногда и перед началом отделочных работ).

Развиваются информационные технологии, "жизнь" настоятельно требует не только интеграции систем, но и обновления некоторых "особенностей национальных подходов". Поэтому нельзя, например, не учитывать, в части обеспечения вопросов безопасности в составе ИЗ, обязательно необходимо взвешенно учитывать, как минимум, две ветви организационно технических решений:

- безопасность жизнедеятельности объекта (нормированное функционирование систем жизнеобеспечения объекта),
- обеспечение территориальной безопасности, защита имущества, собственности от несанкционированного воздействия и проникновения с целью нанесения личностного и имущественного ущерба.

Эти две, на первый взгляд, объединенные лишь общей технологической целью составляющие должны иметь весьма разные подходы при формировании требований по уровню доступа к потокам информации со стороны непосредственных пользователей и обслуживающих структур, в разветвленной структуре ИЗ.

Некоторые компании стремятся, прежде всего, учесть свой коммерческий интерес при создании ИЗ, и зачастую при формировании технических заданий "упускают" такие деликатные вопросы, оставляя право решать заказчику, как и на каком уровне будут решены эти проблемы, а ведь он нередко далек от правильных представлений, как это должно быть правильно реализовано в составе ИЗ. Под техническими мероприятиями в концепции безопасности понимается комплексная система безопасности (КСБ).

На основе анализа многолетней практической деятельности, можно сделать некоторые интересные выводы:

- У нас в России сейчас больше отдают предпочтение интегрированным системам и не хотят иметь в пользовании разрозненные системы охранно-пожарной сигнализации, телевизионного наблюдения, управления доступом, управления микроклиматом и освещением, управления лифтами и другими системами.
- Для решения проблемы обеспечения безопасности деятельности необходимо синтезировать интегрированные системы безопасности, а не ограничиваться простым объединением независимых систем.
- Дальнейшим развитием процесса интеграции интеллектуальных систем безопасности и жизнеобеспечения объекта или здания (системы интеллектуального здания) можно считать объединение их с системами автоматизации и управления функционированием объекта. Такие системы могут применяться не только в жилых или офисных зданиях, но и на производственных и промышленных объектах.

Реализация систем данного типа требует тщательной проработки по определению функций и задач для ядра системы, а также способы технических решений и отработки алгоритмов в информационных потоках для периферийных устройств. Впрочем, эти проблемы не принципиальны, решить их совместными усилиями вполне возможно.

Многофункциональная, гибкая логическая взаимосвязь систем безопасности с системами жизнеобеспечения в этом случае позволяет эффективно и экономично выполнять многофункциональные задачи контроля и управления.

В существующих системах редко учитывается полный набор угроз, поэтому, на момент ввода системы в эксплуатацию в ней имеется много "пробелов". Кроме этого, часто не учитываются статистические данные, характерные для конкретного региона России и для конкретного типа объекта. Это, конечно, проявится потом, и тем серьезнее могут быть последствия, чем менее тщательно этому вопросу было уделено внимания на этапе проектирования.

Приведем основные, наиболее важные позиции и составляющие алгоритмического анализа, определяющие уровень и качество принимаемых технологических решений:

- правильный учет норм, правил, действующих стандартов,
- оценка составляющих систем безопасности ресурсов коммерческого предприятия,
- оценка организационно-технических мер по физической защите (безопасность) материальных объектов и финансовых ресурсов,
- анализ системности предусматриваемых охранных мер,
- оценка и разработка системы мер по обеспечению сохранности материальных ценностей разработка требований к организации объектовой службе безопасности,
- разработка системы мер по обеспечению безопасности информационных ресурсов.

Обеспечение качества работ системе безопасности

Необходимой составляющей системы безопасности должно быть обеспечение высокого качества работ и надежности используемых средств и мер защиты, на основе действующей системы стандартов и руководящих нормативно-технических и методических документов по безопасности, утвержденных федеральными органами государственного управления в соответ-

ствии с их компетенцией. В соответствии с этими требованиями и должны производиться предпроектное обследование и проектирование информационных систем, заказ средств защиты информации и контроля, предполагаемых к использованию в этих системах, аттестация объектов информатики, а также контроль защищенности информационных ресурсов.

Заключение

Реализация проектов ИЗ - бизнес в большей части интеллектуальный, многогранный..!!!!

Им должны заниматься либо крупные строительные компании, имеющие в своем составе специализированные подразделения, которые занимаются кабельными системами (электроснабжение, слаботочные системы, охранная и пожарная сигнализация и т. д.), либо работающие в тесном контакте со строительными организациями самостоятельные компании системные интеграторы.

В процесс революционных преобразований в сфере создания интеллектуальных систем вовлечены четыре группы - каждая со своими интересами и в то же время заинтересованная в двух других. Это строители, производители СКС, системные интеграторы и конечные пользователи. Для каждой группы основной целью являются экономия денежных средств на затратном этапе и увеличение доходов в процессе профессиональной деятельности (в бизнесе). Так, например, в нашем случае, медленное, но верное принятие новой технологии управления сетями оказалось выгодным для всех.

Богатый практический опыт работы с Заказчиком, показывает, что выполнение этих требований, важных для обеих сторон, возможно только при условии, что Заказчик и Исполнитель правильно учтут все необходимые требования при разработке Технического задания и Проектировании, а в процессе выполнения работ не допустят принципиальных отклонений от принятых и согласованных на этапе проектирования организационно-технических решений при создании ИЗ.

P.S. Возможно многим покажется, что в данном материале опять чрезмерно заостряется внимание на составляющих безопасности, в то время как основная идея ИЗ – это прежде всего в высшей степени надежность инженерных коммуникаций, автоматизация процессов управления и их эксплуатации, минимизация затрат, и конечно удобство и комфорт для пользователя. Но в том и заключается главная проблема, что увлекшись красивой терминологией умного, комфортного здания и перспективами в части предоставления пользовательских функций и перспективой автоматизации по житейски рутинных процессов обеспечения нашей жизнедеятельности, комплекс вопросов по обеспечению безопасности, опять оставили на заднем плане, что в целом вполне естественно, так как это отражает сложившуюся, сформировавшуюся систему отношений к специалистам слаботочникам на рынке строительства и реконструкции зданий.

Предполагаю, что специалистам необходимы более активные совместные действия для преодоления имеющихся несоответствий, настало время активной интеграции в данном направлении. Возможно, при таком подходе к комплексному решению и потенциальные заказчики, на проекты такого класса, будут увереннее себя чувствовать, как это произошло, например, на рынке интегрированных систем безопасности.