СИСТЕМЫ БЕЗОПАСНОСТИ И ЦИФРОВОЕ УПРАВЛЕНИЕ

Максименко Владимир Адамович
эксперт

LIGHT+BUILDING И INTERSEC FORUM 2018 – ЗНАКОВЫЕ СОБЫТИЯ РЫНКА АВТОМАТИЗАЦИИ ЗДАНИЙ И БЕЗОПАСНОСТИ

Говоря об использовании сетевых решений, облачных технологий и Интернета вещей в системах автоматизации зданий и безопасности, невозможно пройти мимо такого ключевого события, как выставка Light+Building 2018, недавно закончившаяся во Франкфурте-на-Майне. Второй раз выставке сопутствует конференция Intersec Forum 2018, в рамках которой тема конвергенции систем безопасности и систем автоматизации зданий, открытая на выставке в 2016 году, получила свое развитие.

В то время как на выставке Light+Building традиционно большое внимание уделялось системам освещения и достижениям в области автоматизации зданий, на конференции основное внимание уделялось вопросам неразрывной связи обеспечения защиты информации, используемой в сети современного здания, и применения для этого соответствующих стандартов. Не случайно открытие ключевой пятидневной конференции Intersec Forum 2018, посвященной этому вопросу, проходило под девизом «Оцифровка в основе безопасности данных!». Реализация глобальной задачи цифровизации (перехода к цифровому формату обмена данными и управления) зданий столкнулась с необходимостью обеспечения безопасности цифрового управления. Как отмечал представитель ZVEI (Немецкая ассоциация производителей электротехники и электроники, представляющая интересы 1600 компаний электротехнической промышленности и связанных с ними сервисных компаний в Германии) Майкл Зиесмер: «Именно данные делают цифровые технологии здания». Безопасное цифровое управление зданиями так же необходимо, как сбор и обработка данных здания на основе защиты информации. Недоверие в компаниях отрасли, а также у пользователей при проектировании, установке и эксплуатации может быть устранено, если безопасность данных будет гарантирована уже при создании продуктов и устройств в отрасли (безопасность при разработке). В этой статье сделана попытка осветить основные тенденции развития систем автоматизации зданий и систем безопасности, демонстрировавшиеся на выставке и конференции, и показать, как эти тенденции отражаются в отечественных нормативных документах и практических решениях.

СЕТИ И ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ И БЕЗОПАСНОСТИ – НЕРАЗРЫВНЫЕ ВОПРОСЫ СОЗДАНИЯ НОВЫХ ОБЪЕКТОВ

По словам технического директора Siemens доктора Роланда Буша проблема защиты данных – самое большое препятствие реализации концепции активного, гибкого здания в части автоматизации зданий. При этом он отметил:

- 41% мирового потребления энергии приходится на здания.
- Во время эксплуатации возникает 80% общих затрат на строительство – это должно планироваться с помощью BIM.
- 30% офисных площадей будут использоваться для гибкой практики работы.
- 50% рабочей силы в 2020 году будут так называемыми «Millennials» (поколение цифровых аборигенов, родившихся в новом тысячелетии).
- Для 80% зданий неясно, кому они будут принадлежать, поэтому аспекты планирования и безопасности делают этот факт заслуживающим внимания.

В качестве основных проблем перехода к цифровизации для проектировщиков и операторов современных зданий он выделил три основные проблемы: комфорт и безопасность продукта, эффективность энергии и имущества; эффективность пространства и пользователей.

Решать эти проблемы предлагается путем определения и соблюдения норм

и стандартов всеми участниками: разработчиками, производителями, техниками и строительными операторами. По данным доклада штаб-квартиры Siemens в Мюнхене 2016 года «Превышая самые высокие стандарты эффективности и устойчивости»: ежегодное сбережение по сравнению со старыми фондами составляет на 75% меньшее потребление воды, до 90% меньшее потребление энергии, до 90% меньший выброс CO_2, сертификацию по LEED и DGNB зеленым стандартам.

Сегодня упомянутые выше вопросы эффективности оказались неразрывно связаны с вопросами безопасности сетей управления и обмена данными. Еще десять лет назад были широко известны и использовались сетевые технологии автоматизации зданий, такие как KNX, LonWorks, BacNet, ModBus, однако ввиду высокой профессиональной планки, необходимой для работы с этими технологиями, больших проблем в части безопасности таких сетей практически не возникало. Только с активным переходом к работе через IT-приложения и шлюзы особенно остро встала проблема кибербезопасности. Ведущие специалисты европейских компаний большое внимание уделили вопросам кибербезопасности в цифровизации. Так, президент Федерального ведомства по информационной безопасности Германии (BSI) сказал о новом понимании безопасности информации и данных как в компаниях, так и в обществе в целом: «Мы должны по умолчанию реализовать реальное и рациональное управление рисками для кибербезопасности. Кибербезопасность является предпосылкой для оцифровки и должна быть вопросом для руководства». Очередной шаг для этого уже сегодня – стандарты безопасности данных.

С 2012 года BSI создала на европейском уровне успешную платформу через инициативу «Сети защиты сетей», которая позволяет управляющим и менеджерам компаний сообщать и обмениваться опытом, сертифицированными партнерами, решениями и рисками: www.allianz-fuer-cybersicherheit.de.

Представляют интерес результаты опроса, проведенного ZVEI среди более чем 100 компаний-членов из 21 различных промышленных секторов (в основном, производителей компонентов):

- 42% опрошенных компаний-членов ZVEI хотят увеличить свои бюджеты в области IT-безопасности в течение следующих 12-18 месяцев, причем первичные инвестиции предназначены для использования в аппаратном и программном обеспечении, а также в процессах.
- 87% компаний несут основную ответственность за безопасность IT.
- 88% заявляют, что кибербезопасность является главной темой управления бизнесом.
- Инциденты, в основном, были вызваны троянами или вымогательством (60% опрошенных компаний).
- Слабые стороны используемого программного обеспечения и человеческая ошибка являются основными факторами, которые приводят к возникновению инцидента с безопасностью.
- Стандарты безопасности для окружающей среды производства – VDI/VDE стандарт 2182, стандарты ISO/IEC 27009/27019 прежде всего полезны для производителей, интеграторов и операторов. Стандарт IEC62443 ранее применялся только очень ограниченно (5-7% респондентов) и полностью неизвестен более чем половине респондентов.

В качестве выхода из сложившейся ситуации в Германии рекомендуется взаимодействие с упомянутой сетью BSI www.allianz-fuer-cybersicherheit.de.

НОВАЯ НОРМАТИВНАЯ БАЗА – ФУНДАМЕНТ ВНЕДРЕНИЯ НОВЫХ ПОДХОДОВ

Таким образом, появление реальных проблем использования сетевых решений в АСУЗ вызвало появление новых нормативных документов, регламентирующих правила безопасной работы в сетях. В докладе представителя компании dhpg, в частности, упоминались:

- DIN EN 50132 «Системы сигнализации. Наблюдение за системами видеонаблюдения для использования в приложениях безопасности. Руководство по применению».
- DIN EN 14676 «Устройства сигнализации о дыме для использования в жилом здании, квартирах и комнатах с аналогичными целями».
- VDMA 24774 «IT-безопасность для автоматизации зданий и систем управления».
- Доклад Gartner: «8,4 миллиарда

Рис. 1. Категории требований цифровизации

Рис. 2. DIN VDE 0826-2. Системное проектирование: противопожарные системы с системными компонентами: Приложение A (информативное)

подключенных «вещей» будут использоваться в 2017 году». (Gartner, 2017).

В докладе представителя hagergroup рассматривались вопросы системного проектирования пожароохранных систем со всеми системными компонентами DIN VDE V 0826-2. По сути, здесь рассмотрена структурная схема организации пожароохранной системы, т. е. внутрисистемные коммуникации, и для каждого компонента системы указаны соответствующие нормативные документы, регламентирующие их использование в системе и обеспечивающие внутрисистемную интеграцию.

Новые нормативные документы по сетям оповещения продемонстрировала Ассоциация ZVEI.

ТЕНДЕНЦИИ

Среди тенденций можно отметить работу по разработке стандарта fieldbus в мире IP-протокола IoT (предназначенного для создания единой инфраструктуры IP для всех продуктов автоматизации зданий независимо от их технического происхождения или экосистемы), упомянутую в докладе Дж. Демареста из ассоциации KNX.

Следует отметить, что тема Интернета вещей (IoT) в том или ином виде отражалась в большинстве докладов как существующая реальность: это использование облачных технологий и больших данных, глубокая интеграция и конвергенция управления инженерными системами зданий и безопасностью, использование информации систем нижнего уровня для принятия решений после ее обработки на верхних уровнях и т. п.

По словам Д-р Хилко Хоффманн «Никто не знает, какие стандарты у нас будут в течение десяти или двадцати лет. Но мы уже можем создать основу для их взаимодействия сегодня». Эта основа – семантические веб-технологии для автоматизации зданий.

Платформа нейтральной интеграции поставщиков основывается на том, что «нет ни одного правильного интерфейса. Независимая от поставщика платформа интеграции должна поддерживать как можно больше существующих интерфейсов, протоколов и стандартов и поддерживать их в актуальном состоянии. Будущие системы безопасности предлагаются только системами, которые действительно открыты, что означает, что они не поддерживают ни фирменное решение, ни один стандарт: открытая архитектура является ключом к будущему».

НОВЫЕ ИНИЦИАТИВЫ КАК ОТРАЖЕНИЕ НОВОЙ ИДЕОЛОГИИ СТРОИТЕЛЬСТВА

Озвученные конкретные решения и предложения, продемонстрированные в ходе конференции, логически вписываются в идеологию, представленную на Intersec Forum 2018 рядом организаций, инициатив и сообществ. Так, Питер Боровски, генеральный директор Инициативы Smart Home Germany, отметил, что инвестиции клиентов в интеллектуальные домашние установки сегодня мотивированы растущей потребностью в безопасности в 60% случаев, по соображениям комфорта в 30% и по соображениям энергоэффективности – в 10%. При этом «нет необходимости использовать единый всеобъемлющий протокол автоматизации зданий. Сила умной автоматизации обычно основана не на технологии, а на навыках проектировщиков и интеграторов-исполнителей проекта. Протестированные и сертифицированные технологии безопасности будут огромным конкурентным преимуществом, по крайней мере, в Германии».

Экономическая инициатива Smart Living, представляющая более 60 крупнейших немецких компаний-производителей и ассоциаций представила общий подход немецких компаний к ускорению перехода инноваций на рынок, устранению существующих

Рис. 3. Совместимость шинных систем

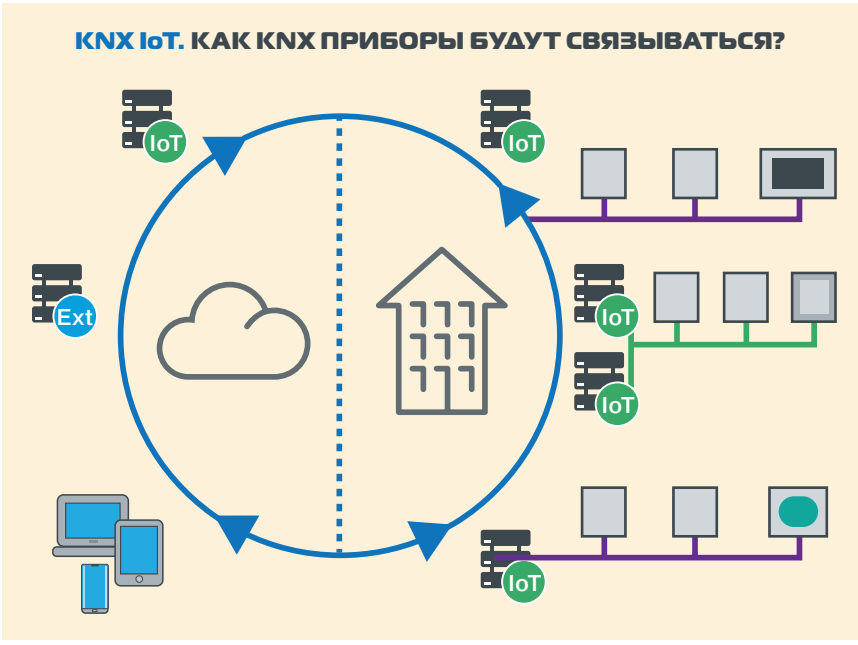
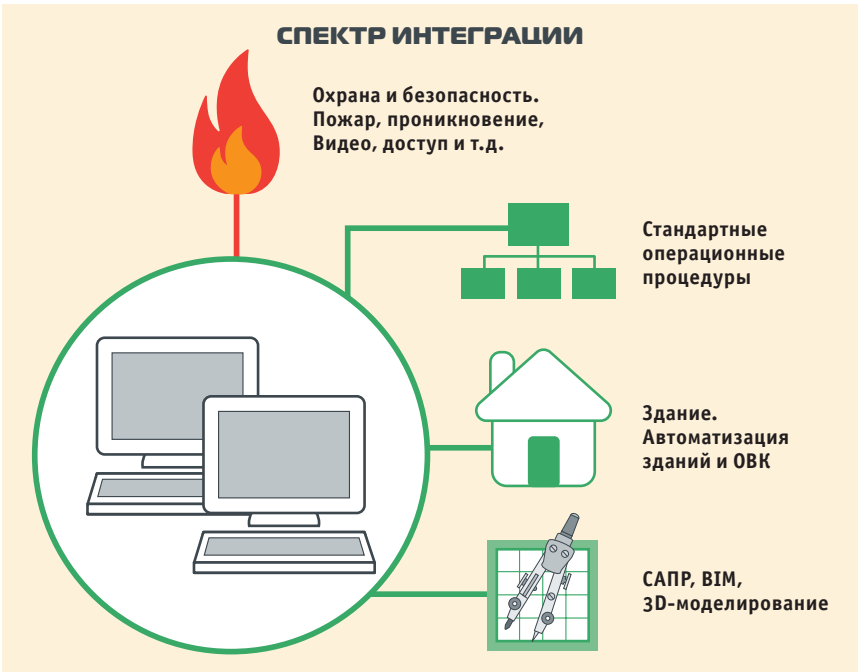


Рис. 4. Платформа нейтральной интеграции



барьеров и разработке устойчивых рыночных стратегий. В части инициатив, стандартов и разных платформ с апреля 2017 года отдел Smart Living координирует и поддерживает деятельность этой инициативы от имени Федерального министерства экономики и энергетики (BMWi) и выступает в качестве контактного лица для заинтересованных компаний и инициатив, политиков и общественности.

Таким образом, вопросы внедрения цифровизации в Германии глубоко проработаны как на уровне технологий и сетевых решений, так и на уровне нормативных документов, обеспечивающих безопасность процессов. Практическая реализация новых проектов обеспечена соответствующей квалификацией интеграторов, поддерживающейся в рамках работы рабочих групп соответствующих национальных инициатив.

РОССИЙСКИЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ В ОБЛАСТИ АСУЗ И ОТРАЖАЮЩИЕ ИХ РЕШЕНИЯ НА ОТЕЧЕСТВЕННОМ РЫНКЕ

Несмотря на то, что сравнивать уровень продвижения, государственной и профессиональной поддержки и сопутствующей нормативной базы в Европе и России сложно, тем не менее, в последнее время вопросам автоматизации зданий, энергоэффективности, цифровизации и кибербезопасности стало уделяться гораздо больше внимания.

Так, по данным исследований J'son & Partners Consulting прошлого года за пять лет доля домохозяйств, использующих подобные технологии, увеличится с 1% до 5%. В абсолютном выражении их число вырастет до 2,8 миллиона.

Согласно приказу № 1550/пр «Об утверждении Требований энергетической эффективности зданий, строений, сооружений» от 17.11.2017: «Предусматривается поэтапное уменьшение удельного расхода тепловой энергии на отопление и вентиляцию для вновь строящихся зданий, в том числе многоквартирных домов. Объем тепла и энергии, необходимый для отопления новостроек, должен будет снизиться с 1 июля 2018 года – на 20%, с 1 января 2023 года – на 40%, с 1 января 2028 года – на 50%». Документ также предполагает введение новых обязательных требований энергетической эффективности: установку систем «умного освещения» и «умного отопления». «Умное отопление» должно появиться во всех административных и общественных зданиях площадью более 1 тыс. м^2.

По данным Russia Internet of Things Market 2016-2020 Forecast рынок технологий Интернета вещей в России (куда входит и «Умный дом») будет увеличиваться в среднем на 21,3% в год и к 2020-му достигнет 9 млрд долл. Эта информация создает определенные позитивные предпосылки.

В этой связи изложенный выше зарубежный опыт и, тем более, разрабатываемая нормативная база может быть весьма полезна при внедрении технологий цифровизации в России. Сегодня можно наблюдать, как отечественные производители предлагают новые конвергентные решения, востребованные при реализации задач цифровизации. Так на выставке MIPS/Securika Moscow можно было увидеть, как в программе конференций, так и на стенде, новое решение, отражающее и конвергенцию систем безопасности и автоматизации зданий, и имеющее в своей основе сетевую структуру, отвечающую требованиям, сформулированным на конференции Intersec Forum 2018.

Дальнейшее развитие этого направления можно будет увидеть в программе XI Специализированной выставки-форума «Передовые Технологии Автоматизации. ПТА – Санкт-Петербург 2018», которая пройдет в Санкт-Петербурге в начале июня.

Рис. 5. Структура комплексного решения управления складом

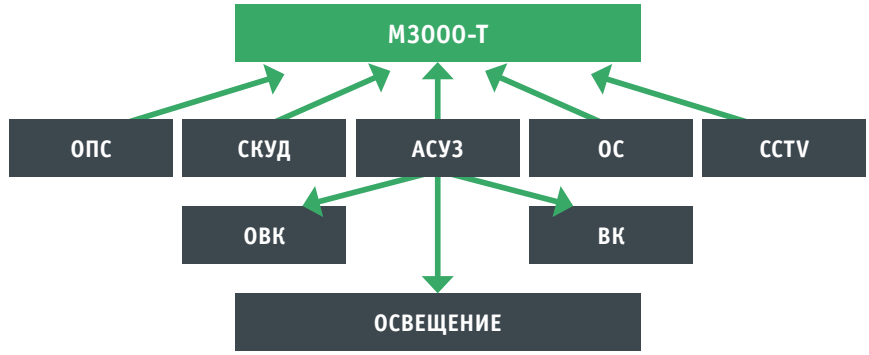


Рис. 6. Управление светом с использованием сетевых решений

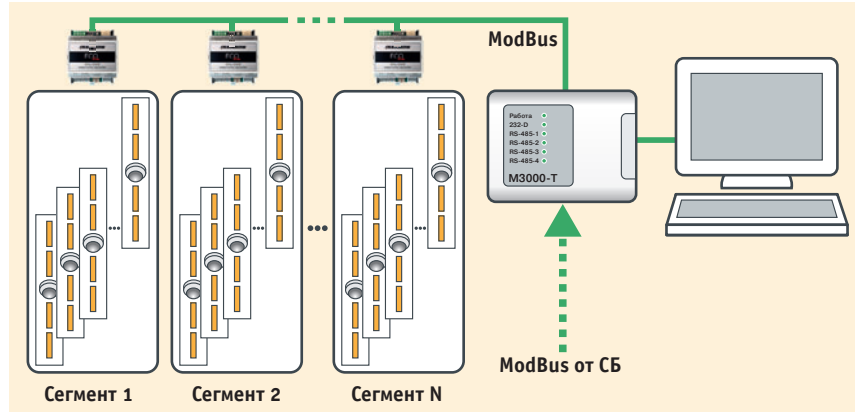


Рис. 7. Мезонинный склад с управлением светом на DALI-ModBus