БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ: КОМПЛЕКСНЫЙ ПОДХОД

Красов Алексей Алексеевич
начальник проектного отдела дирекции комплексной безопасности, группа «Астерос»

КОМПЛЕКСНЫЕ СИСТЕМЫ

Сегодня, в связи с осложнившейся обстановкой на мировой политической арене, активизацией террористических организаций, в том числе ведущих пропаганду через Интернет, вопросы оснащения критически важных объектов городской инфраструктуры современными комплексами физической безопасности представляются наиболее актуальными. Основной задачей любого террористического акта является нанесение максимального ущерба городу или определенной организации в материальном аспекте либо в плане человеческих потерь. Если говорить об объектах ТЭК, ГЭС, АЭС, то здесь преступники часто преследуют единственную цель: остановить технологические процессы либо вывести из строя оборудование предприятия, что может привести к возникновению техногенных катастроф, человеческим жертвам, финансовым и репутационным потерям.

ЗАКОНОДАТЕЛЬНАЯ БАЗА

Нормативы по оснащению системами безопасности и антитеррористической защиты существуют для всех критически важных городских объектов: транспортных, ТЭК, АЭС, ГЭС, стадионов, комплексов для проведения культурно-массовых мероприятий и так далее. Данные требования регламентируются ведомственными нормативно-правовыми актами или закрепляются отдельными постановлениями правительства. Например, для транспортных объектов существуют постановления в сфере безопасности Минтранспорта РФ, а также ФЗ «О транспортной безопасности». С точки зрения обеспечения защиты объектов ТЭК основным документом является Постановление Правительства Российской Федерации от 5.05.2012 № 458 «Об утверждении Правил по обеспечению безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса». Если министерские и правительственные нормативы отсутствуют, то применяются, как правило, общие ГОСТы либо близкие по содержанию ведомственные требования (МВД России и другие).

КАК ПРОВЕРЯЮТ И КТО ВИНОВАТ?

Всегда конечную ответственность за безопасность объекта несет руководитель либо собственник предприятия. Обычно это прописано во всех ведомственных и отраслевых документах и является общепринятой практикой. На правоохранительные органы и гражданские службы, как правило, возложена контролирующая функция: они могут посетить объект с плановой или внеплановой проверкой выполнения всех требований по антитеррору. То же самое относится к административным органам федерального и территориального управления: каждый из них на своем уровне осуществляет контроль антитеррористической защищенности. Существуют проверки на уровне района, города, области, страны.

В большинстве случаев на предприятиях проходят стандартные плановые проверки. При этом на стратегически важных объектах могут быть организованы различные варианты межведомственных учений, в том числе внеплановых, с имитацией захвата заложников, закладывания взрывных устройств и так далее.

БЕЗОПАСНОСТЬ ОБЪЕКТОВ: ГОРОДСКИЕ/ЗАГОРОДНЫЕ

Законодательством не предусмотрены отдельные нормативы по антитеррористической защищенности объектов, расположенных за чертой города. Однако в результате строительства могут возникать дополнительные требования, например, касающиеся регулирования застройки. Предприятия, находящиеся «в чистом поле», имеют возможность построить «полосу отчуждения» и установить на ней, скажем, радиоволновые датчики, реагирующие на движения. На данной территории по умолчанию никто не может находиться, в противном случае лицо, нарушающее рубеж безопасности, расценивается как лазутчик.

Городские объекты, как правило, расположены в условиях тесной застройки и не имеют возможности расширять свои границы и выделять отдельные «мертвые зоны» для построения охранных систем. Кроме того, при создании систем защиты для таких предприятий следует учитывать их влияние на прилегающие постройки, особенно это касается жилого сектора. Представим, что на периметре объекта установлены системы охранного освещения и оповещения, которые включаются по срабатыванию сигнализации. В свою

очередь, сигнализация может среагировать на пролетающую птицу, пробегающую кошку или сработать ложно – в результате сбоя датчиков. И вот система запустилась: зажглись яркие прожекторы, включились пронзительные звуковые сигналы. Все это, особенно в ночное время, доставляет дискомфорт жителям прилегающих районов. С такими моментами приходится считаться при построении систем безопасности критически важных городских объектов.

АНАЛИЗ УЯЗВИМОСТИ И МОДЕЛЬ НАРУШИТЕЛЯ

В основе системы антитеррористической защиты любого критически важного объекта лежат два документа: анализ уязвимости и модель нарушителя. Именно на их основании вырабатывается техническое решение по оснащению организации комплексом безопасности.

Практика показывает: намного проще проводить анализ уязвимости уже действующего объекта, чем строящегося. Причина лежит на поверхности: все точки, которые так или иначе попадают под подозрение в системе защиты, можно обойти пешком, оценить визуально, вплоть до проведения натурных испытаний. К тому же руководство и служба безопасности знают слабые стороны уже функционирующего объекта.

Анализ уязвимости осуществляется по следующему сценарию: в первую очередь проводится обследование объекта и намечаются потенциальные «точки уязвимости». Затем происходит их ранжирование по важности и рассчитывается вероятность нарушения безопасности этих узлов предприятия.

Параллельно разрабатывается модель нарушителя. Кто является преступником – одиночный террорист-смертник или группа специально подготовленных вооруженных лиц? Возможно, ему или им может оказывать содействие сотрудник предприятия (рядовой либо высокопоставленный, специалист службы безопасности и т. д.). Все эти варианты развития событий несут в себе различные типы угроз, и соответственно, в каждом из перечисленных случаев предусматриваются свои подходы к созданию систем защиты.

Таким образом, комплексная система безопасности и антитеррористической защиты должна быть построена с применением риск-ориентированного подхода. Необходимо определить, какие потенциальные потери может понести предприятие либо город в случае реализации угроз, оценить их вероятность и сопоставить с конечной стоимостью систем.

ВЫБОР ТЕХНИЧЕСКИХ РЕШЕНИЙ

При выборе оборудования для обеспечения безопасности стратегически важных объектов в первую очередь стоит учитывать специфику предприятия. Например, для объектов ГЭС, располагающихся на воде, АЭС, имеющих пруды-охладители, необходимо применять продукты, стойкие к коррозии. Для предприятий ТЭК, расположенных в черте города неподалеку от транспортных магистралей, которые подвергаются обработке реагентами, предпочтение также стоит отдать оборудованию, стойкому к агрессивным средам. Кроме того, в каждом сегменте рынка безопасности существуют продукты и решения, которые являются золотым стандартом в части ПО, охранной сигнализации, СКУД и т. д.

Что касается выбора ПО для обеспечения безопасности, то для стратегически важных объектов и госструктур существует Единый реестр российского программного обеспечения Минкомсвязи РФ. В него входят отечественные решения, полностью соответствующие всем требованиям регулятора и разрешенные для закупок госучреждениями и предприятиями с госучастием.

ИНТЕГРАЦИЯ – ВСЕМУ ГОЛОВА

Получение и передача оператору данных о текущем состоянии объекта является основной задачей мониторинговых центров безопасности. В идеале информация должна поступать не только от классических (контроля доступа, видеонаблюдения, охранной сигнализации), но и от смежных систем – инженерных, контролирующих технологические процессы предприятия, строительных конструкций и т. д. Эти «побочные» системы могут быть источником ценной информации для комплекса КСБ. К примеру, нарушители приводят в действие пожарную сигнализацию, имитируя пожар или действительно вызывая его. Пока поднимается пожарная тревога, у них появляется возможность преодолеть рубежи безопасности предприятия. Поэтому для обеспечения комплексной защиты необходимо владеть полной информацией о текущем состоянии объекта. Одно дело – когда оператор видит срабатывание конкретного датчика, другое – когда он фиксирует, что после автоматического включения пожарной сигнализации произошла активация детекторов движения на видеокамерах, периметральной охранной сигнализации, взломана дверь. В этом случае станет ясно, что происходит диверсия с целью проникновения на объект. Именно поэтому на стратегически важных объектах необходимо уделять особое внимание интеграции классических систем безопасности с инженерными и архитектурными решениями здания, в части СМИС и СМИК.

Кроме того, на некоторых критически важных городских объектах обязательна интеграция СМИК и СМИС с общегородскими комплексами безопасности. Данные системы автоматически оповещают структуры МЧС о серьезных неполадках в «инженерке» либо нарушениях в конструктивной целостности зданий. Свод правил 132.13330.2011 «Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования» регламентирует, что каждый объект должен быть категорирован с точки зрения потенциальной угрозы и оснащаться либо полным, либо частичным набором систем. Например, объекты для проведения спортивных или культурно-массовых мероприятий в зависимости от вместимости обязаны предусматривать СМИК и СМИС и объединять их с городскими системами безопасности. К таким объектам относятся, например, БСА «Лужники», стадион «Динамо». К тому же сегодня на территории Москвы создана система видеонаблюдения на базе Единого центра хранения и обработки данных (ЕЦХД). В него «стекаются» видеопотоки со всех подведомственным городским структурам предприятий. Полагаю, следующим шагом в развитии защиты критически важных городских объектов станет подготовка нормативных актов о дополнительной интеграции систем охранной сигнализации, контроля доступа в АПК «Безопасный город».

ОРГАНИЗАЦИЯ СЛУЖБЫ КОНТРОЛЯ И РЕАГИРОВАНИЯ

Эволюция систем безопасности в комплексы принятия решений – это рыночный тренд, который наблюдается на протяжении последних лет. В идеале служба контроля и реагирования предприятия должна быть построена именно на базе системы принятия решений. Ее основным отличием от любого комплекса безопасности является то, что в случае возникновения нештатной ситуации она «подсказывает» оператору его дальнейшие шаги. При срабатывании определенных датчиков человек видит сообщение, что в первую очередь необходимо оповестить группу быстрого реагирования, затем руководство и так далее. Такие оповещения могут осуществляться и в автоматическом режиме – с помощью рассылок по SMS, e-mail, пейджинговых служб. Таким образом, с помощью системы принятия решений оператор сможет правильно и быстро среагировать на инцидент, что в критической ситуации бывает порой затруднительно.

Кроме того, нюансы организации службы контроля и реагирования зависят от того, кто несет охрану на объекте – ЧОП, вневедомственная охрана, внутренние войска, Росгвардия и т. д. У каждой из организаций, которые занимаются охранной деятельностью, могут быть свои дополнительные требования по организации караула, мониторинга, дежурства и реагирования. Существуют и соответствующие ограничения: для задержания нарушителей сотрудники ЧОП не могут применять силовые методы, они лишь вправе предупредить преступников о незаконности действий и вызвать полицию. У Росгвардии, к примеру, с этим не возникнет проблем.