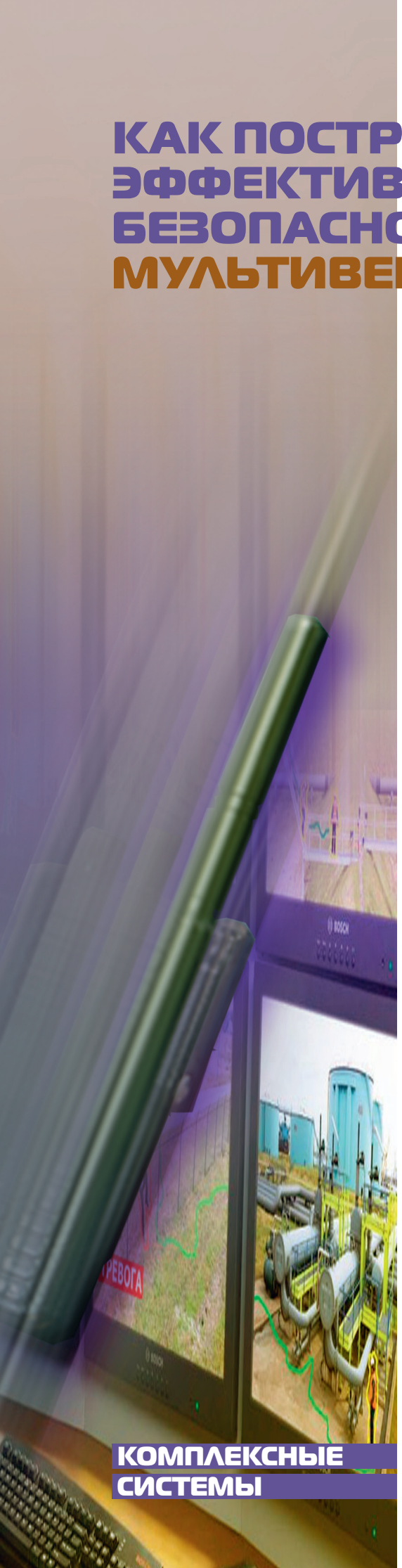
КАК ПОСТРОИТЬ ЭФФЕКТИВНУЮ СИСТЕМУ БЕЗОПАСНОСТИ В УСЛОВИЯХ МУЛЬТИВЕНДОРНОСТИ?

Скворцов Андрей Викторович
директор по развитию ПСЦ «Электроника»



КОМПЛЕКСНЫЕ СИСТЕМЫ

Эффективная система безопасности предприятия – система, выстроенная «с нуля», – утверждение верно лишь при идеальных условиях. В реальности же заказчики сталкиваются с ситуацией, когда необходимо построить комплексную систему безопасности на объекте с множеством уже установленных технических средств в арсенале. Ниже разбираем – как?

МУЛЬТИВЕНДОРНОСТЬ: ОПРЕДЕЛЯЕМ ПОНЯТИЕ

В своем развитии предприятие проходит несколько этапов: сменяются руководители, расширяется структура, изменяются потребности в защите от угроз – идет наращивание систем безопасности. Помимо внутренних изменений происходят и внешние: меняется законодательство, появляются новые требования к безопасности объектов. Добавим к этому желание каждого нового управленца угнаться за технологическими новинками, которые обещают максимальный эффект. В результате за годы существования предприятия на нем скапливается множество разнобрендовых систем защиты, которые и составляют в итоге систему безопасности. И подобная ситуация мультивендорности наблюдается на многих крупных предприятиях промышленной сферы, банковской, транспортной отрасли, государственного сектора.

ЗАДАЧИ ДЛЯ РЕШЕНИЯ

В условиях мультивендорности у заказчика постепенно возникает потребность в интеграции оборудования и построения комплексной системы безопасности, которая будет полностью отвечать требованиям по защите предприятия от внешних и внутренних угроз.

Одной из задач, с которой заказчик обращается к производителю, может являться интеграция подсистем (например, СКУД, видеонаблюдения, систем охраны периметра) для оптимизации работы технических средств на нижнем уровне. В этом случае интеграция СКУД, например, поможет создать единое бюро пропусков, автоматизировать заказ и выдачу заявок на пропуска, своевременно выявлять нарушения пропускного и внутриобъектового режима и т. д.

Вторая задача – интеграция всех подсистем предприятия в единый комплекс с целью сведения поступающей информации, отслеживания нештатных ситуаций, автоматизации и контроля за работой подсистем безопасности объекта, формирования аналитических данных.

Третьей задачей может стать желание руководителя не только интегрировать имеющееся оборудование, но и иметь возможность управлять безопасностью на объекте. В настоящее время данный уровень интеграции востребован и имеет широкие перспективы развития. В этом случае мы говорим о создании ситуационных центров, которые позволяют управлять ситуацией на всех этапах обеспечения безопасности: от обнаружения угрозы до ликвидации и предоставления отчета по нештатной ситуации руководителю.

При том нельзя забывать об экономическом эффекте – заказчику интересно решение проблемы в приемлемые сроки без значительных финансовых затрат, сократить которые, в нашем случае, возможно за счет интеграции уже имеющихся на предприятии подсистем на любом уровне.

ШАГ ЗА ШАГОМ

После того, как мы определили потребности заказчика, приступаем к предпроектному обследованию объекта.

В качестве примера рассмотрим ситуацию на объекте заказчика, у которо-

го есть множество технических средств охраны различных производителей, требующих интеграции в комплексную систему безопасности с единым интерфейсом, аналитикой, управлением.

С точки зрения законодательства на данном объекте уже должны быть соблюдены требования к техническим средствам охраны, при необходимости произведено категорирование объекта, определены алгоритмы действий оператора, функционирования системы охраны периметра, контрольно-пропускного режима, инструкции сил реагирования.

Огромный пласт работы на подготовительном этапе ложится на плечи технических специалистов и руководителей проектов. В ходе общения с заказчиком и предпроектного обследования предприятия собирается информация и анализируются данные о периметре, прилегающих внешних и внутренних территориях, уязвимых мест в ограждении, наличии инженерных коммуникаций, проверяется наличие на ограждении элементов ОТС, СКУД, ТСОН, освещения, систем контроля и управления доступом, учитывается количество бюро пропусков и другие моменты.

Далее решается вопрос о том, какое оборудование подлежит интегрирации, будет ли оно заменено или дополнено, прорабатываются схемы интеграции. Интегратору следует учитывать тот факт, что заказчик ранее уже вложил деньги в систему безопасности и важно сохранить его вложения за счет оптимального решения.

Отметим, что сегодня интеграция установленного оборудования все же возможна без его замены. Производители технических систем безопасности заинтересованы в широком использовании своих продуктов, поэтому, как правило, используют открытые (универсальные) протоколы обмена данными (например, ONVIF и другие), которые позволяют без труда интегрировать технические устройства. От возможностей протокола будет зависеть глубина интеграции. В случае, если протокол закрытый (защищенный), есть три пути решения. В первом случае заказчик может оставить одну из подсистем в автономном режиме и не подвергать интеграции, но данный способ не обеспечит полноценное решение задачи. Второй вариант – заменить данное оборудование, чтобы выполнить интеграцию всех подсистем, без исключений. Третий – интеграция технических средств на аппаратном уровне (метод «сухих контактов»).

Важно учитывать и разрозненную структуру предприятия, на котором создается интеграция. Так, ситуационные центры могут выстраиваться как в рамках одного объекта (на местном уровне), так и выходить на уровень федеральный – то есть объединять несколько территориально удаленных объектов в единой информационной среде. Многоуровневая архитектура ситуационных центров позволяет держать под контролем предприятия в масштабах города, региона, страны.

Завершающим этапом работы с заказчиком является предложение концепции будущей системы безопасности объектов и утверждение проекта в работу.

ТЕХНОЛОГИИ БУДУЩЕГО: ЗДЕСЬ И СЕЙЧАС

Мы выявили потребности заказчика, определили модель интеграции, оценили возможности установленного на объекте оборудования, сформулировали задачи по выполнению проекта. Но что позволит нам реализовать интеграцию на практике?

Осуществить интеграцию системы безопасности предприятия наиболее эффективным образом сегодня позволяют интеллектуальные платформы.

Полная прозрачность, управление безопасностью предприятия 24/7, автоматизация процессов, обработка огромного количества событий, минимизация влияния человеческого фактора, снижение времени реагирования на угрозу, логичная система отчетных данных с возможностью последующего анализа – далеко не весь функционал платформ нового поколения. Эти возможности обеспечиваются за счет «умного» ПО управленческого класса PSIM (Physical Security Information Management). Программное обеспечение PSIM-класса интегрирует все подсистемы безопасности в единый комплекс, собирает и обрабатывает информацию, поступающую от них, выявляет связь между событиями и отражает ее в требуемом виде. Система помогает принимать правильные решения, беря на себя большую часть нагрузки на оператора, что значительно снижает вероятность возникновения ошибки при ликвидации нештатных ситуаций.

Это в теории, а что на практике? При возникновении тревожных событий оператору, ответственному за их верификацию, выводится вся доступная по событию информация и инструкция, которая помогает оценить событие и выбрать правильный сценарий его обработки. В случае, если оператор действует некорректно или не столь оперативно, как этого требует ситуация, сигнал передается на уровень выше. Таким образом, руководитель обладает прозрачной и достоверной информацией о происходящем на объекте и может в режиме реального времени контролировать любые отклонения.

МУЛЬТИВЕНДОРНОСТЬ И СВОБОДА ДЕЙСТВИЙ

Мы рассмотрели возможную схему построения мультивендорной системы безопасности на объекте. Конечная цель нашего проекта в заданном формате – обеспечить качественное решение поставленных заказчиком задач, а также возможности дальнейшего усовершенствования системы безопасности без зависимости от бренда разработчика и поставщика. После реализации проекта заказчик должен иметь свободу в самостоятельном развитии и наращивании системы безопасности.

Резюмируя, можно сказать, что построение систем управления безопасностью в рамках мультивендорности приобретает трендовое звучание в современных условиях, и задача интеграторов – услышать его, реализовать на практике наиболее эффективным образом, удовлетворить все пожелания заказчика, предоставив ему дальнейшую свободу выбора и действий.