PSIMом единым

Появление новых требований к антитеррористической защищенности совпало с повсеместным сокращением бюджетов, выделяемых для поддержания безопасности объектов транспортной инфраструктуры. В этих условиях владельцы объектов стоят перед задачей — более эффективно использовать уже существующие решения. Сделать это возможно с помощью технологии PSIM (Physical Security Information Management — система управления информацией о физической безопасности). В этом уверен генеральный директор ПСЦ «Электроника» **Николай Овченков**.

Беседовала: Марина Иванова

Как бы вы оценили состояние безопасности объектов транспорта в настоящий момент? Чем закончилась эпоха 40-х приказов Минтранса?

НИКОЛАЙ ОВЧЕНКОВ: Я считаю, что 40-е приказы свои задачи выполнили. По крайней мере уровень систем безопасности и, соответственно, защищенности объектов к настоящему моменту значительно вырос.

До появления этих приказов специалисты, обеспечивающие безопасность транспортных объектов, по большому счету, не задумывались ни о критических элементах, ни о потенциальных угрозах. Сейчас как минимум эти факторы анализируются, делаются попытки соотнести их с понятием уязвимости.

В последние годы существенно возросла нагрузка на объекты транспортной инфраструктуры, и на аэропорты в том числе. Требования законодательства по обеспечению безопасности становятся все более жесткими. Регулярное проведение плановых и внеплановых проверок прокуратуры и Ространснадзора привело к тому, что субъекты транспортной инфраструктуры уже не могут игнорировать эти требования и вынуждены их выполнять.

До сих пор отчасти это делается формально. Но фиктивного подхода, как было раньше, уже нет. В результате к настоящему моменту обеспечено базовое соответствие систем безопасности объектов оценке уязвимости. Это уже достижение.

Хорошо, что специалисты задумываются о том, где на объекте узкие места, от каких угроз следует защищаться и т. д. Предстоит еще проделать большую работу, чтобы обеспечить реальную безопасность транспортных объектов. Но ситуация уже на порядок лучше, чем 10 лет назад.

Какие проблемы могут возникнуть в ходе сертификации согласно требованиям нового 969-го постановления правительства?

Н. О.: Сам подход к тому, что необходим контроль соответствия систем заданным параметрам — абсолютно верный. В этом смысле сертификация может выступить средством осуществления такого контроля. Что касается оборудования, по отдельным его видам (например, досмотровому) сертификация давно существует. Требования, предъявляемые к оборудованию такого типа, понятны — обнаружительная способность и т. д. Но есть инженерно-технические средства, по которым не все так однозначно.

Not by PSIM alone. Interview with Nikolay Ovchenkov, CEO of PSC «Electronika» / By Marina Ivanova

Antiterrorist requirements for transport facilities appeared at the time of massive budget cutback. The next quest for facilities' owners is to make maximum use of installed security systems. Such opportunity gives PSIM technology (Physical Security Information Management). CEO of PSC «Electronika», Nikolay Ovchenkov, explaines, how to use PSIM at the best value.

Если рассматривать системы видеонаблюдения, контроля доступа, периметровой сигнализации, важно понимать, что оборудование представляет собой составляющие элементы конкретной системы. По аналогии с автомобилем — если сертифицировать все детали автомобиля, это не значит, что конкретный автомобиль поедет и в дальнейшем не будет проблем с его функционированием и техническим обслуживанием.

Еще один момент, который необходимо учесть, — некоторые требования к оборудованию (к разрешению камер, цвету, типу считывателей и т. д.) заведомо сформированы под параметры конкретных поставщиков.

> Необходимо сертифицировать не составляющие элементы системы безопасности, а систему в целом

Все это в совокупности позволяет говорить о том, что сертификация отдельных технических средств не решит проблему обеспечения безопасности объектов транспортной инфраструктуры. Это может быть первым, промежуточным этапом. Считаю, что в итоге необходимо сертифицировать не составляющие элементы системы безопасности, а систему в целом, на соответствие ее оценке уязвимости и критериям по минимизации рисков авиационной безопасности. Тогда будет понятно, насколько система способна противодействовать заданным видам угроз, которые могут нанести ущерб функционированию объекта, жизни или здоровью персонала, пассажиров и других лиц.

Какие основные технологические тренды в обеспечении транспортной безопасности будут востребованы, а какие вытеснены с рынка?

Н. О.: По сути, эти тренды мало отличаются от трендов систем физической защиты объектов. Системы (контроля доступа, охраны периметра и другие) становятся сложнее с технологической точки зрения. Это требует более высокого качества их исполнения и управления ими, интеграции на разных уровнях и перехода к PSIM-системам.

Один из ярких трендов — беспилотные летательные аппараты (БПЛА). Это палка о двух концах. С одной стороны, беспилотник может использоваться для контроля за протяженной территорией и ее периметром. С другой стороны, он или его груз может нести угрозу для стратегически важного объекта. Не случайно сейчас все чаще задумываются, как защитить объект от беспилотников.

Какие рекомендации вы даете по антитеррористической защищенности объектов в условиях сокращения бюджетов?

Н. О.: С учетом того, что на действующем объекте уже установлены системы безопасности, в той или иной комплектации, первоочередная задача в условиях ограниченного бюджета — добиться максимального результата от их работы. Необходима интеграция систем. Это позволит получать актуальную информацию о работе всего комплекса. Но и этого недостаточно — безопасность объекта необходимо не только отслеживать, но и управлять ею, что особенно актуально для объектов транспортной инфраструктуры.

Для решения этой задачи разработаны специализированные программно-аппаратные комплексы нового поколения, которые пришли на смену системам сбора и обработки информации — PSIM-системы.

Они предоставляют информацию о реальной защищенности объекта и снижают негативное воздействие человеческого фактора, за счет контроля работы оператора. А главное — позволяют проанализировать и оценить эффективность работы всей системы безопасности.

На отечественном рынке до последнего времени PSIM-системы были представлены зарубежными аналогами, качественными, но малодоступными по причине высокой стоимости. Сейчас появился продукт отечественной разработки — PSIM-система Electronika Security Manager (ESM) компании «Электроника».

Как показывает практика, даже небольшой ситуационный центр на базе такой системы позволяет повысить эффективность уже имеющихся систем и сэкономить на инвестициях в обеспечение безопасности объекта. А это немаловажно в условиях ограничения бюджета. Впоследствии выявленные «узкие места» можно будет «закрыть», докупив необходимое оборудование и нарастив систему.

Фото: ©Depositphotos.com/muhor

Объект внедрения ESM — международный аэропорт Сочи:
- более 600 камер видеонаблюдения
- видеоаналитика в терминалах и на привокзальной площади
- биометрические системы допуска, в том числе по 3D-снимку лица
- единое бюро пропусков
- пункт управления безопасностью