Безопасность систем безопасности: защита информации IP-видеонаблюдения

Индустрия видеонаблюдения планомерно мигрирует с аналоговых технологий на цифровые, а именно - на IP-камеры в рамках общей тенденции All-over-IP. При этом трафик IP-видеонаблюдения содержит чувствительную к атакам информацию, например, о критических производственных процессах и объектах и др. Подобные данные должны быть защищены от угроз навязывания, искажения, перехвата и др. Обратная ситуация, когда к средствам информационной безопасности применяют меры физической защиты, является вполне типичной - например, технические устройства (системы видеонаблюдения, СКУД, сигнализация, решетки на окна и т.д.) контролируемой зоны, в которой размещаются средства криптографической защиты информации (СКЗИ). То есть системы физической защиты позволяют обеспечить качественное функционирование средств защиты информации. По этой же логике должен быть повышен общий уровень защищенности путем обеспечения информационной безопасности системы видеонаблюдения. Такой подход, нацеленный на максимальную комплексную защиту востребован на всех объектах массового скопления людей. Также стоит учитывать геополитическую ситуацию, а именно курс на импортозамещение. Видеокамер казахстанского производства пока на рынке нет. Все оборудование создается полностью на иностранной элементной базе. Абстрагируясь от страны производства IP-камер, используются средства защиты информации, соответствующие требованиям казахстанского законодательства и национальным стандартам в области ИБ.

Правительство РК утвердило требования, предъявляемые к виду деятельности по разработке и реализации (в том числе иной передаче) средств криптографической защиты информации (Постановление Правительства Республики Казахстан от 10 апреля 2012 года № 440