УГРОЗЫ ПРИМЕНЕНИЯ НЕДЕКЛАРИРОВАННЫХ ЗАКЛАДНЫХ УСТРОЙСТВ НА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

О.К. БАРАНОВСКИЙ

В современных условиях информатизация процессов в области национальной безопасности, автоматизация управления объектами, нарушение функционирования которых может привести к чрезвычайным ситуациям техногенного характера или нарушению жизнедеятельности населения, актуализировало требования к безопасности критически важных объектов информатизации (КВОИ), поддерживающих эти процессы. Специфика проблем безопасности КВОИ состоит в том, что повсеместно используемые популярные импортные продукты и системы не рассчитаны или не прошли процедуру подтверждения соответствия для применения в тех ситуациях, когда безопасность имеет существенное значение.

К основным угрозам безопасности на КВОИ относят:

– нарушение целостности, доступности, конфиденциальности и сохранности информации;

– нарушение функционирования оборудования или программного обеспечения, от которых зависит выполнение миссии объектом критической инфраструктуры.

Учитывая, что известные методы поиска недокументированных возможностей являются весьма трудоемкими и не позволяют обеспечить высокое доверие к функционированию КВОИ, необходимо также предусматривать меры по перекрытию скрытых (неразрешенных) каналов передачи данных между отдельными агентами.

В связи с этим, обеспечение заданного уровня доверия к используемым на КВОИ продуктам и системам информационных технологий импортного производства должно выполняться в рамках действующих процедур подтверждения соответствия в устанавливаемых с учетом степени критичности КВОИ объемах и соотношениях работ, включающих поиск недокументированных возможностей и перекрытие скрытых каналов передачи данных как внутри КВОИ, так и за их пределы.