Обеспечение комплексной безопасности критически важных объектов информатизации

Маликов Владимир Викторович, начальник цикла технических и специальных дисциплин УО «Учебный центр Департамента охраны» МВД Республики Беларусь, майор милиции, кандидат технических наук.

В настоящее время обеспечение комплексной защиты критически важных объектов информатизации (КВОИ) является одной из приоритетных задач современного общества.

Данная проблема приобретает сегодня особую значимость и для Республики Беларусь в связи с необходимостью разработки и внедрения современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Согласно п. 14 Концепции национальной безопасности Республики Беларусь: обеспечение надежности и устойчивости функционирования КВОИ является одним из основных национальных интересов в информационной сфере Республики Беларусь.

Следует отметить то, что публикуемые в открытых источниках информации материалы по методикам создания и функционирования КВОИ имеют общий характер, а почти все статистические данные по безопасности данных объектов являются закрытыми. Однако, учитывая то, что функционирование КВОИ осуществляется в рамках единого административно-территориального и экономического пространства государства, то можно предположить для указанных объектов в той или иной мере будут применимы общие подходы по выделению данных, связанных с построением их информационной и инженерно-технической защиты.

Основу современных систем обеспечения информационной и инженерно-технической защиты КВОИ от несанкционированного доступа составляют нормативно-правовые и организационно-технические методы защиты информации, позволяющие сформировать необходимое нормативное и организационное обеспечение для организации инфраструктуры таких систем, а также реализовать поддержку принятия соответствующих управленческих решений в вопросах безопасности объектов.

В настоящее время на территории стран СНГ идет активный процесс по формированию национального нормативно-правового обеспечения в области защиты КВОИ от несанкционированного доступа. Однако, принятые (разрабатываемые) нормативно-правовые акты в большинстве случаев носят ведомственный характер, что приводит к снижению эффективности взаимодействия между различными органами управления и ведомствами, так как при наличии их большого количества уровень и качество связей остается низким. Также следует отметить, что в области информационного права остро стоят вопросы о развитии и применении международного законодательства, международного частного права, гармонизации правовых норм. Данные проблемы также особенно актуальны для национального законодательства стран СНГ.

Одним из основных принципов противодействия угрозам безопасности КВОИ будем считать превентивность принимаемых мер защиты, так как устранение последствий проявления угроз требует значительных финансовых, временных и материальных затрат.

С учетом того, что в системах защиты КВОИ используются аппаратно-программные средства охраны, существуют угрозы, связанные с возможным внедрением в изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия, а также программного обеспечения, нарушающего функционирование системы защиты. Анализ организационно-технического обеспечения при построении систем защиты КВОИ позволяет определить комплекс мероприятий по их защите на стадии проектирования системы, обеспечив оптимальное сочетание организационных и технических мер защиты информации.

Обеспечение комплексной безопасности КВОИ неразрывно связано с инженерно-техническими средствами и системами защиты, позволяющими обеспечить защиту от несанкционированного физического доступа к объекту / ресурсам объекта. Причинами возникновения угроз инженерно-технической защите КВОИ могут быть действия человека, форс-мажорные обстоятельства, отказ оборудования и внутренних систем жизнеобеспечения. Однако, основной причиной таких угроз является, как правило, преднамеренное или случайное действие человека (нарушителя). Потенциальный нарушитель для реализации своих замыслов руководствуется определенной мотивацией и намерениями, владеет совокупностью знаний, умений и навыков (способов) совершения противоправных действий.

Продолжение см. стр. 60

Начало см. стр. 51

Следует отметить, что факты практической реализации угроз инженерно-технической защите КВОИ, связанные с несанкционированным физическим доступом к объекту / ресурсам объекта, как правило, направлены на нарушение свойств целостности, доступности и конфиденциальности средств и систем обработки информации, каналов телекоммуникации таких объектов.

На основании изложенного выше, современные системы обеспечения безопасности КВОИ, как правило, представляют собой многоуровневые, территориально распределенные, автоматизированные информационные системы, осуществляющие мониторинг состояния безопасности, как отдельных объектов, так и их территориально-административных объединений. Основу построения таких систем составляют аппаратно-программные средства и методы обеспечения комплексной безопасности КВОИ, задачей которых является практическая реализация информационной и инженерно-технической защиты с учетом специфики возникающих угроз. В свою очередь основой аппаратно-программных средств и методов обеспечения информационной и инженерно-технической безопасности являются:

1. Технологии передачи данных.
2. Программное обеспечение средств и систем защиты.
3. Аппаратно-программные средства и системы защиты информации.
4. Интегрированные системы технических средств охраны.
5. Автоматизированные системы передачи извещений.
6. Системы управления рисками.

Очевидно, что системы обеспечения комплексной безопасности КВОИ должны проектироваться с учетом принципов равнопрочности средств защиты, согласованности критериев безопасности и информационного единства.

Основные направления исследований по совершенствованию комплексной безопасности КВОИ.

1. Разработанные системы защиты и управления рисками для КВОИ по нормативно-правовым, организационно-техническим и физическим факторам имеют множество недостатков и уязвимостей, а также значительную (во многих случаях избыточную) стоимость и низкую функциональность. Необходимо формирование нового системообразующего документа для реализации комплексного подхода в области безопасности КВОИ для решения проблем согласованного взаимодействия заинтересованных структур, централизации управления при обеспечении защиты КВОИ.

2. Имеющаяся классификация КВОИ не имеет категорирования по признакам информационной и инженерно-технической безопасности с учетом особенностей доступа. Существующие критерии не учитывают в полном объеме вопросы организационной структуры управления объектом, функционально-экономического организацию процесса деятельности объекта, оценки риска. Необходимо проведение классификации угроз безопасности не только для защищаемого КВОИ, но и для системы защиты с учетом жизненного цикла последней.

3. При использовании технологий передачи данных в системах защиты необходимо учитывать как категорию защищаемого объекта, так и пропускную способность каналов связи, параметры их надежности и помехоустойчивости. Существующие в настоящее время аппаратно-программные системы защиты информации и инженерно-технической безопасности КВОИ имеют низкий уровень унификации, проблему совместимости используемых средств безопасности при работе с различными системами защиты объектов.

4. Существующие методы оценки эффективности систем защиты КВОИ не позволяют проводить полный анализ и динамическую коррекцию результатов оценки.

5. Эксплуатируемые в рамках СПИ средства и системы охраны обеспечивают отражение только части программно-технических и физических угроз КВОИ и, в целом, не всегда отвечает современным требованиям к комплексным системам защиты объектов. ■

Президент Республики Беларусь Александр Лукашенко 25 октября 2011 года подписал Указ № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»

Согласно Указу создается Государственный реестр критически важных объектов информатизации (далее — КВОИ).

Указом также утверждено Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации, согласно которому отнесение объекта информатизации к критически важным объектам информатизации осуществляется на основании отраслевых критериев и с учетом уровня ущерба национальным интересам в политической, экономической, социальной, информационной, экологической и иных сферах, причинение которого возможно в случае возникновения угроз различного характера в отношении объекта информатизации (его составляющих элементов).

Обеспечение безопасности КВОИ включает комплекс мероприятий по созданию системы безопасности КВОИ правового, организационного и технического характера, в том числе по мониторингу угроз безопасности КВОИ и принятию мер реагирования на угрозы безопасности КВОИ. ■

http://oac.gov.by/news/26.html

Интервью с регуляторами, комментарии специалистов планируются в следующих номерах журнала «Технологии безопасности»