При использовании маскируемого оборудования или его элементов в рубежах охраны СФЗ, скрытии принципов функционирования инженерно-технических средств системы должны быть обеспечены меры их защиты от фотографических и оптико-электронных средств разведки.

Эффективность принимаемых мер защиты должна соответствовать действующим нормативным документам по противодействию фотографическим и оптико-электронным средствам разведки.

Основными мероприятиями по защите информации в СФЗ от таких средств являются: использование маскирующих свойств местности, условий ограниченной видимости; применение ложных сооружений и маскировочных конструкций; пространственные ограничения, направленные на исключение контакта между средствами разведки и защищаемым объектом.

Все вышеперечисленные мероприятия используются на различных этапах жизненного цикла системы физической защиты АЭС.

УДК 34:002

А.Н. Лепёхин, Д.В. Перевалов

НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

В рамках регулирования информационных правоотношений, в частности правовой регламентации функционирования критически важных объектов информатизации, авторским коллективом разрабатывается целостный пакет проектов нормативных правовых актов в данной сфере. Предполагается, что принятие и реализация актов законодательства, направленных на регулирование информационных правоотношений, обеспечит повышение качества принимаемых нормативных правовых актов в сфере информационной безопасности, защищенность информационных интересов граждан, общества и государства придаст адресность государственной информационной политике, что, в свою очередь, повысит эффективность ее реализации.

Основу указанного пакета нормативных правовых актов составляет проект модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры» (далее – законопроект), который разрабатывается в соответствии с Межгосударственной программой совместных мер борьбы с преступностью на 2014–2018 годы, утвержденной решением Совета глав государств СНГ 25 октября 2013 г.

Законопроект непосредственно основывается на Модельном информационном кодексе для государств – участников СНГ, модельных

законах «Об информации, информатизации и защите информации» и «О международном информационном обмене», Рекомендациях по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности, а также учитывает положения нормативных правовых актов государств – участников СНГ: закона Азербайджанской Республики от 3 апреля 1998 г. № 460-IQ «Об информации, информатизации и защите информации»; закона Республики Армения от 17 февраля 1998 г. «О телекоммуникации»; закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»; закона Республики Казахстан от 5 июля 2004 г. № 567-II «О связи»; законов Республики Молдова от 22 июня 2000 г. «Об информатике» и от 3 февраля 2009 г. «О предупреждении и борьбе с преступностью в сфере компьютерной информации»; федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», законов Украины от 5 июля 1994 г. № 80/94-ВР «О защите информации в информационно-телекоммуникационных системах» и от 18 ноября 2003 г. № 1280-IV «О телекоммуникациях»; указа Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»; указа Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Необходимость разработки законопроекта обусловлена, во-первых, увеличением числа критически важных объектов в системе объектов информационно-коммуникационной инфраструктуры государств – участников СНГ; во-вторых, повышением уровня опасности последствий для государства, общества и отдельных лиц в случае нарушения (прекращения) нормального функционирования критически важных объектов информационно-коммуникационной инфраструктуры; в-третьих, расширением спектра угроз безопасности таких объектов, изменением их характера и интенсивности, в-четвертых, отсутствием в большинстве государств – участников СНГ нормативно закрепленных основ деятельности по обеспечению нормального функционирования критически важных объектам информационно-коммуникационной инфраструктуры, а также по предупреждению, выявлению и локализации угроз их безопасности.

Основной целью подготовки законопроекта является выработка новой согласованной политики на пространстве СНГ в сфере информационной безопасности, гармонизация законодательных решений государств – участников СНГ в области обеспечения безопасности крити-

чески важных объектов информационно-коммуникационной инфраструктуры. Основными задачами при этом являются:

установление единых (общих) основных положений законодательства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры, обеспечивающих регулятивную мобильность уполномоченных государственных органов государств – участников СНГ;

определение общих положений правового статуса субъектов обеспечения безопасности таких объектов;

выработка механизма установления эквивалентности и взаимного согласования систем обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры в государствах – участниках СНГ;

формирование единой, скоординированной и сопряженной системы правовых, организационных, инженерно-технических, программно-аппаратных и специальных мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры в государствах – участниках СНГ.

Таким образом, принятие законопроекта позволит создать эффективные организационно-правовые механизмы, обеспечивающие формирование и развитие системы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры. Кроме того, данное действие позволит обеспечить комплексную реализацию положений Стратегии сотрудничества государств – участников СНГ в построении и развитии информационного общества, а также предусмотреть действенную систему мер интеграционного сотрудничества государств – участников СНГ в рамках сближения законодательства в сфере обеспечения информационной безопасности.

УДК 681.51

А.А. Матвеев

ПРОБЛЕМНЫЕ ВОПРОСЫ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Повсеместное внедрение широкого спектра информационных технологий в системы управления производственными и технологическими процессами обеспечивает развитие всех сфер государственной и экономической жизни страны. В то же время безопасность коммуникационных сетей и информационных систем, особенно их работоспособность и отказоустойчивость, стала крайне актуальной темой для общества. Эта тревога объясняется риском появления проблем в критически важных информационных системах, которые могут возникнуть из-за их сложности, а также из-за атак на инфраструктуры, предоставляющие критические сервисы. В четверку наиболее опасных и подверженных угрозам отраслей входят энергетика, нефтегазовая сфера, транспорт и водоснабжение. на безопасность критически важных объектов информатизации (КВОИ) являются:

интеграция в единые комплексы автоматизированных систем управления (АСУ) информационных систем, используемых в управлении производственными и транспортными структурами, административными и финансовыми ресурсами;

рост числа противоправных деяний с использованием информационных и коммуникационных технологий;

постоянное усложнение программного обеспечения и оборудования, используемых в АСУ;

вынужденная технологическая зависимость от иностранных компаний-производителей и поставщиков программно-аппаратных средств обработки, хранения и передачи информации, привлекаемых к созданию АСУ КВОИ;

стремление организаций – разработчиков программного обеспечения АС к снижению издержек и, как следствие, к использованию типовых решений и заимствованного программного обеспечения;

отсутствие достаточного нормативно-правового регулирования процессов обеспечения безопасности АСУ КВОИ, в том числе в части определения уровня их реальной защищенности и ответственности за нарушение требований по обеспечению безопасности КВОИ.

Кроме того, требования нормативных правовых актов предоставляют право владельцам объектов информатизации отнесения их к критически важным на основе отраслевых критериев. Это связано с тем, что в каждой отрасли существует своя специфика задач обеспечения безопасности. В то же время анализ сведений об имеющихся в структуре государственных органов и иных организаций объектах информатизации показывает, что значительную часть данных объектов не представляется возможным отнести к критически важным в соответствии с существующей процедурой, хотя они оказывают существенное влияние на отдельные отрасли Республики Беларусь (системы управления технологическими процессами банковской сферы, транспортной системы и др.). Владелец такого объекта нередко просто не понимает, что его система критически важная, а иногда старается самоустраниться по причине нежелания вкладывать средства в обеспечение необходимого уровня защищенности.