УДК 004.056.5

Леоненко Г.П., Юдин А.Ю.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ УКРАИНЫ

Анотація:

Стаття описує основні завдання державної політики в галузі забезпечення безпеки ключових систем інформаційної структури критично важливих об'єктів.

Аннотация:

Статья описывает основные задачи государственной политики в области обеспечения безопасности ключевых систем информационной структуры критически важных объектов.

Abstract:

This article describes the main goals of the state policy in the field of security of key systems information infrastructure of the critical facilities.

Актуальность проблемы

Актуальность проблемы обеспечения информационной безопасности (ИБ) ключевых систем, входящих в состав критически важной информационной инфраструктуры Украины (КСИИ), обуславливается такими современными условиями ведения деятельности на объектах информационной и телекоммуникационной инфраструктуры государства как: наличие растущей зависимости бизнес-процессов от инфокоммуникационных технологий, сложность используемых технологий, большое количество потенциальных угроз ИБ, как случайного, так и преднамеренного характера, включая терроризм. Реализация обозначенных угроз может приводить к значительным негативным последствиям для безопасности государства в информационной сфере и препятствовать реализации Украиной своих целей во внутренней/внешней политике.

Также следует отметить, что на сегодня на законодательном и нормативном уровне в Украине не даны определения критически важных объектов и ключевых систем информационной инфраструктуры. Учитывая это и используя анализ публикации специалистов из Российской Федерации, США, ряда стран Европы [1-6] дадим обобщенные определения критически важных объектов (КВО) и КСИИ.

Критически важный объект – объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок.

Ключевая система информационной инфраструктуры – это информационно-управляющая или информационно-телекоммуникационная система, которая отвечает одному из требований:

– осуществляет управление КВО (процессом);

– осуществляет информационное обеспечение управления КВО (процессом);
– осуществляет информирование граждан о чрезвычайных ситуациях.

В последние годы западные специалисты уделяют особое внимание оценке воздействия на жизненно важные объекты своих стран и возможные последствия этих воздействий для политической, экономической, экологической и других сфер деятельности государства. Очевидно, что в условиях современного чрезвычайно интенсивного развития инфраструктуры ведущих стран мира создается все большее количество КВО, таких, например, как крупные гидротехнические сооружения, нефте- и газопроводы, сети АЭС, пункты хранения стратегических запасов нефти и газа, химические производства, транспортные узлы, аэродромы и т.п., выведение из строя которых может привести к катастрофическим последствиям.

В связи с этим в США, Франции, Германии, Японии и других странах были проведены обширные исследования по выявлению объектов на их территории, представляющих угрозу для нормальной жизнедеятельности государства в случае воздействия на них безъядерного высокоточного оружия или в результате террористических (диверсионных) актов. Также прорабатывались варианты техногенных катастроф или разрушительных стихийных бедствий. В перечень выявленных КВО не включались традиционные типы военных объектов – ракетные базы и полигоны, авиационные базы, органы высшего военного управления, так как, по оценкам исследователей, эти объекты имеют достаточно высокую степень защищенности и практически являются малоуязвимыми от воздействия обычных средств поражения.

Кроме того, вывод из строя подобных объектов существенно не нарушает системы жизнеобеспечения государства и его управляемость.

По результатам исследований был сделан вывод, что главную угрозу для жизнедеятельности страны представляет выведение из строя объектов, приводящее к нарушению транспортных и энергетических систем, водоснабжения и др. в масштабах государства или отдельных районов. Так, на территории США и Канады выделено около 2 300 подобных объектов, в Германии - более 650, Франции - около 500, в Японии - до 700. При этом отмечается, что они обладают относительно низкой защищенностью и имеют большое количество уязвимых точек «несанкционированного доступа», воздействие на которые может привести фактически к полному параличу систем жизнедеятельности государства [7].

Защита КВО и их совокупности, которую принято называть критически важной инфраструктурой, или критической инфраструктурой, представляет собой одну из наиболее важных задач обеспечения национальной безопасности любой страны. Защита КВО включает проведение мероприятий, которые должны обеспечить их сохранение в случае различных воздействий природного или техногенного характера. Подтверждением этому являются события, получившие широкое освещение в СМИ, – обнаружение вируса Stuxnet, ориентированного на SCADA системы компании Siemens (Simatic WinCC), атака иранских объектов – 2010 год, внештатное аварийное выключение блока ядерной станции «Hatch» (США) после установки обновления программного обеспечения из-за нештатного сбоя программируемого логического контроллера при получении аномального выходного сетевого трафика из производственной сети – 2008 год, выявление силовыми структурами США проникновения в электроэнергетическую сеть и размещения в ней программных «закладок», направленных на внештатный останов ее функциональных элементов и нарушение корректной работы – 2009 год [2], а также публикация конфиденциальной дипло-

матической переписки сайтом WikiLeaks и массовая волна протестов в странах арабского Востока, получившая в прессе название «революции Facebook».

Нормативное обеспечение ИБ КСИИ

Для формирования формализованного научно-технического подхода к решению проблемы информационной безопасности КВО разрабатываются как ведомственные, так и общенациональные стандарты и нормативно-технические документы. Так, на сегодня в мире разработаны и используются:

1. Нормативные документы РФ:

– Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий, утверждена Секретарем Совета Безопасности от 08.11.2005;

– Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, утверждены ФСТЭК России от 18.05.2007;

– Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утверждена ФСТЭК России от 18.05.2007;

– Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утверждена ФСТЭК России от 18.05.2007;

– Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, утверждены ФСТЭК России от 19.11.2007;

– Положение о Реестре ключевых систем информационной инфраструктуры, утверждено приказом ФСТЭК России от 04.03.2009.

2. Нормативные документы Республики Беларусь:

– Указ Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации», который утверждает Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации.

3. Регламентирующие документы США:

– Административный указ 13636 «О мерах по укреплению кибербезопасности критических инфраструктур» (Executive Order — Improving Critical Infrastructure Cybersecurity);

– Директива 21 от 12.02.2013 «Об обеспечении безопасности и устойчивости критических инфраструктур» (Presidential Policy Directive 21 — Critical Infrastructure Security and Resilience).

– Административный указ 13636 вместе с Директивой 21 заменил Директиву 2003 года «Homeland Security Presidential Directive 7» (HSPD-7).

4. Международные нормативные документы:

– ISA-SP99, Manufacturing and Control Systems Security;

– NERC CEO Announces Plan to Improve Response to Cyber and Critical Infrastructure Protection;

– PCSRF - Security Capabilities profile for industrial control;

– IEC 61784-4. Industrial Communications - Fieldbus Profile - Part 4: Profiles for secure communications in industrial networks;

– - Cisco SAFE for PCN (ProcessControlNetwork) для защиты систем управления технологическими производствами и процессами АСУ ТП (SCADA).

В тоже время следует отметить, что в Украине отсутствуют национальные или ведомственные стандарты, а также нормативно-методические документы, регламентирующие аспекты обеспечения информационной безопасности КВО. Следовательно, можно констатировать отсутствие государственной политики в области обеспечения безопасности КСИИ КВО инфраструктуры государства.

Выводы

Исходя из проведенного анализа стандартов и нормативных документов ряда стран Европы, США и РФ можно сделать вывод, что решение основных задач государственной политики в области обеспечения безопасности КСИИ КВО должно осуществляться по следующим направлениям:

1. Фундаментальная и прикладная наука, технологии и средства обеспечения безопасности КСИИ КВО;
2. Совершенствование нормативно-правовой базы;
3. Промышленная и научно-техническая политика;
4. Повышение квалификации кадров в области обеспечения безопасности КСИИ КВО.

Попытаемся сформулировать основные задачи государственной политики по первым двум направлениям.

Основные задачи в области развития **фундаментальной и прикладной науки, технологий и средств** обеспечения безопасности КСИИ КВО и критической информационной инфраструктуры могут быть представлены следующим образом:

а) аналитический обзор исследований, связанных с использованием стандартов и нормативно-методических документов по информационной безопасности для оценки эффективности защиты КСИИ КВО;

б) исследование методов и средств своевременного выявления угроз и оценки их опасности для КСИИ КВО;

в) развитие исследований в области математического моделирования процессов обеспечения безопасности КСИИ КВО, направленных на выработку вероятных сценариев развития ситуации и поддержку управленческих решений;

г) моделирование комплексных систем защиты и обеспечения безопасности КСИИ КВО, отвечающих современному уровню развития информационных технологий и минимизирующих участие обслуживающего персонала в настройке и эксплуатации входящих в их состав программно-аппаратных средств;

д) моделирование, разработка и внедрение специализированных информационно-аналитических систем КВО.

Основные задачи, касающиеся **разработки (совершенствования) нормативно-правовой базы** в области обеспечения безопасности КСИИ КВО могут быть представлены следующим образом:

а) законодательное определение и закрепление прав и обязанностей собственников КСИИ КВО и иных объектов критической информационной инфраструктуры и эксплуатирующих их организаций в области обеспечения безопасности КСИИ КВО;

б) определение порядка:

- разработки, ввода в действие, эксплуатации и модернизации КСИИ КВО и иных элементов критической информационной инфраструктуры;

- получения органом исполнительной власти, регулирующим вопросы обеспечения безопасности информации, сведений о КСИИ КВО и иных элементах критической информационной инфраструктуры;

- использования сил и средств обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру;

- использования сил и средств ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;

- действий должностных лиц, персонала и владельцев КСИИ КВО и иных элементов критической информационной инфраструктуры при обнаружении попыток или фактов нарушения штатного функционирования этих объектов в случае компьютерных инцидентов;

а) нормативно-методическое обеспечение функционирования единой государственной системы обнаружения компьютерных атак на критическую информационную инфраструктуру и мониторинга уровня ее реальной защищенности;

б) оптимизация законодательства Украины в части лицензирования деятельности, связанной с разработкой, производством, эксплуатацией и техническим обслуживанием КСИИ КВО.

Литература:

1. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах / А. Кондратьев / Зарубежное военное обозрение. № 1. -2012.

2. The Cybersecurity Executive Order. Exploiting Emerging Cyber Technologies and Practices for Collaborative Success [Электронный ресурс] / M. McConnell, S. Labarre, D. Sulek, M. McGowan. – Режим доступа: http://www.boozallen.com/media/file/BA13-051CybersecurityEOVP.pdf. - Название с экрана.

3. Ключевые системы информационной инфраструктуры [Электронный ресурс]. – Режим доступа: http://ispdn.narod.ru/ksii.pdf. - Название с экрана.

4. System of Systems Engineerings / Keating, C, Rogers, R., Unal. R., Dryer, D., Sousa-Poza, A., Safford. R.. Peterson, W., Rabadi, G. //Engineering Management Journal, Vol. 15, No. 3, -2003.

5. In the Dark. Crucial Industries Confront Cyberattacks. McAfee second annual critical infrastructure protection report [Электронный ресурс].- Режим доступа: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf. - Название с экрана.

6. Критически важные объекты информатизации. [Электронный ресурс].- Режим доступа: http://oac.gov.by/tzi/kvoi.html. - Название с экрана.