УДК 621.039:004.9

А. Л. Клевцов, М. А. Ястребенецкий,
С. А. Трубчанинов

Государственный научно-технический центр по ядерной и радиационной безопасности, г. Киев, Украина

Компьютерная безопасность информационных и управляющих систем АЭС: нормативная база

Статья посвящена изучению нормативной базы в сфере компьютерной безопасности информационных и управляющих систем (ИУС) АЭС. Приведен краткий обзор серии публикаций МАГАТЭ по физической ядерной безопасности. Рассмотрены ключевое справочное руководство из этой серии и проект нового руководства по вопросам компьютерной безопасности ИУС ядерных установок. Изложены требования к информационной и компьютерной безопасности ИУС АЭС стандартов Международной электротехнической комиссии, в частности стандарта, регламентирующего требования к программе компьютерной безопасности ИУС АЭС. Дан анализ регулирующего руководства Комиссии ядерного регулирования США, содержащего требования к программе компьютерной безопасности ядерных установок. Подняты проблемные вопросы нормативного регулирования в данной сфере и обозначены задачи развития нормативной базы по компьютерной безопасности ядерных установок в Украине.

Ключевые слова: компьютерная безопасность, информационная и управляющая система, физическая защита, информационная безопасность, нормативная база.

О. Л. Клевцов, М.О. Ястребенецький, С.О.Трубчанінов

Комп'ютерна безпека інформаційних та керуючих систем АЕС: нормативна база

Стаття присвячена вивченню нормативної бази у сфері комп'ютерної безпеки інформаційних та керуючих систем (ІКС) АЕС. Наведено стислий огляд серії публікацій МАГАТЕ з фізичної ядерної безпеки. Розглянуто ключове довідкове керівництво з цієї серії та проект нового керівництва з питань комп'ютерної безпеки ІКС ядерних установок. Викладено вимоги щодо інформаційної та комп'ютерної безпеки ІКС АЕС стандартів Міжнародної електротехнічної комісії, зокрема стандарта, що регламентує вимоги до програми комп'ютерної безпеки ІКС АЕС. Надано аналіз регулюючого керівництва Комісії ядерного регулювання США, що містить вимоги до програми комп'ютерної безпеки ядерних установок. Піднято проблемні питання нормативного регулювання в цій сфері та позначено завдання розвитку нормативної бази з комп'ютерної безпеки ядерних установок в Україні.

Ключові слова: комп'ютерна безпека, інформаційна та керуюча система, физичний захист, інформаційна безпека, нормативна база.

Проблема обеспечения информационной и компьютерной безопасности ядерных установок, в том числе АЭС, приобретает в настоящее время все большую актуальность, особенно в свете имевшей место кибернетической атаки компьютерных систем двух АЭС в Южной Корее с реакторами «CANDU» в декабре 2014 года [1]. Помимо реализации различных практических мер защиты от кибернетических угроз, международное сообщество прилагает усилия по созданию соответствующей нормативной базы, охватывающей вопросы компьютерной безопасности. МАГАТЭ, МЭК, национальные органы регулирования ядерной и радиационной безопасности разных стран на сегодняшний день разработали и продолжают разрабатывать нормативные документы, которые покрывают различные аспекты обеспечения компьютерной безопасности (в том числе ИУС, важных для безопасности АЭС). Важность освещаемой темы подчеркнута на прошедшей в феврале 2015 года под эгидой Американского ядерного общества США 9-й Международной конференции «Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies» (которая традиционно является наиболее представительной международной конференцией по ИУС АЭС), где из 13 пленарных докладов четыре были посвящены компьютерной безопасности, включая доклад US NRC.

Настоящая статья входит в цикл статей по компьютерной безопасности ИУС АЭС журнала «Ядерна та радіаційна безпека», начатый публикацией [2]. Кроме того, в ней развивается описание нормативной базы по компьютерной безопасности ИУС, приведенное в [3, глава 7].

Отметим, что международная нормативная база по компьютерной безопасности ИУС АЭС формируется с учетом:

требований к ИУС АЭС, которые регламентируются стандартами МЭК серий «Атомные электростанции. Информационные и управляющие системы АЭС, важные для безопасности» и «Атомные электростанции. Информационные и управляющие системы»;

общепромышленных стандартов МЭК (из серии IEC 62443) по компьютерной безопасности сетей и систем;

стандартов и руководств МАГАТЭ по физической безопасности (поскольку компьютерная безопасность рассматривается как часть общей физической безопасности ядерных установок);

стандартов по информационной безопасности из серии ISO/IEC 27000 (поскольку компьютерная безопасность представляет собой специфический аспект информационной безопасности).

Акцент в данной статье сделан на рассмотрении международных стандартов, которые содержат требования к компьютерной безопасности ядерных установок.

Документы МАГАТЭ. МАГАТЭ рассматривает компьютерную безопасность как часть физической безопасности. Серия публикаций МАГАТЭ по физической ядерной безопасности (Nuclear Security Series) на сегодняшний день включает 23 документа, освещающих различные аспекты физической безопасности. Несколько новых документов данной серии находятся в процессе разработки (в частности глоссарий, в котором будут даны основные термины и определения в области ядерной физической безопасности).

Публикации МАГАТЭ из серии физической ядерной безопасности изданы в четырех категориях (на рис. 1 приведены примеры публикаций [4—11], относящихся к разным категориям).

Рис. 1. Пирамида публикаций МАГАТЭ из серии физической ядерной безопасности

Остановимся подробнее на существующих и разрабатываемых документах МАГАТЭ, имеющих непосредственное отношение к компьютерной безопасности.

Документ NSS 17 [10] — важнейшее на сегодняшний день техническое руководство, в котором описаны принципы обеспечения компьютерной безопасности ядерной установки. Особое внимание акцентировано на важности описания предусмотренных мер по компьютерной безопасности в общем плане обеспечения физической безопасности ядерной установки.

Выделены три типа безопасности: безопасность персонала, физическая безопасность и компьютерная безопасность; четко очерчена роль компьютерной безопасности.

Сказано, что на всех ядерных установках должна осуществляться политика компьютерной безопасности, определяющая цели, основные задачи, а также соответствующий план обеспечения компьютерной безопасности на ядерной установке. Подчеркнута важность внедрения стратегии глубокоэшелонированной защиты от компьютерных угроз. Введены концепция и схема жизненного цикла управления безопасностью (новая концепция, требования, проект, внедрение, эксплуатация, обслуживание и дальнейшее усовершенствование / модернизация).

Показаны аспекты взаимодействия в обеспечении компьютерной безопасности, физической защиты и защиты персонала. Для того чтобы внедрить многоуровневый подход к безопасности, представлены структура возможных уровней безопасности (security level) и связи этих уровней с соответствующими мерами обеспечения безопасности, основные концепции безопасности и их взаимосвязь, в частности определены концепции контрмер, уязвимостей, рисков, ресурсов, угроз атакующих. Описаны основные подходы к оценке рисков, управлению рисками, выявлению и определению параметров уязвимостей.

МАГАТЭ начата разработка двух новых документов, которые должны заменить NSS 17 [10], предварительные названия которых — NST045 «Компьютерная безопасность для ядерной безопасности» и NST047 «Методы обеспечения компьютерной безопасности для ядерных установок».

Документ NSS 23-G [9] затрагивает вопросы информационной безопасности в ядерной отрасли. Основной тематикой данного документа является защита информации, критически важной для обеспечения ядерной безопасности. Рассматриваются аспекты идентификации, выявления, распространения, защиты конфиденциальной и критически важной ядерной информации, доступ к которой должен быть ограничен.

Документ NST036 (проект) [11] освещает вопросы компьютерной безопасности цифровых ИУС, которые выполняют функции безопасности или вспомогательные функции на ядерных установках. В нем затрагиваются три темы:

первая касается роли компьютерной безопасности в защите цифровых ИУС, мер обеспечения компьютерной безопасности, классификации систем по уровням и зонам компьютерной безопасности;

вторая — взаимосвязь между компьютерной и ядерной безопасностью. Приведены принципы оценки рисков с точки зрения компьютерной безопасности ИУС, проанализировано взаимное влияние ядерной и компьютерной безопасности, рассмотрены аспекты выбора мер обеспечения компьютерной безопасности с учетом предъявляемых к ИУС требований к ядерной безопасности;

третья — обеспечение компьютерной безопасности на всех этапах жизненного цикла ИУС, начиная с разработки требований к ИУС и заканчивая ее эксплуатацией, техническим обслуживанием и модификацией. При этом даются рекомендации по разработке основных документов, таких как политика компьютерной безопасности и план обеспечения компьютерной безопасности. Рассматривается ряд сопутствующих вопросов, важных с точки зрения компьютерной безопасности ИУС, например:

обеспечение компьютерной безопасности или ее компонентов (технических средств и программного обеспечения) основными и сторонними поставщиками ИУС;

безопасность архитектуры автоматизированной системы управления технологическим процессом (АСУТП) ядерной установки в целом;

верификация программного обеспечения и валидация ИУС с учетом требований к компьютерной безопасности;

мониторинг компьютерной безопасности.

В настоящее время ведется подготовка технических документов с предварительными названиями *NST037* «Оценки компьютерной безопасности» и *NST038* «Планирование реагирования на инциденты компьютерной безопасности».

В 2015 году планируется публикация разработанного при участии ГНТЦ ЯРБ документа МАГАТЭ *SSG-39* [12] — руководства по ядерной безопасности с установленными в нем требованиями к проектированию ИУС АЭС. В пп. 7.101—7.130 проекта этого документа приведен, в частности, ряд требований к компьютерной безопасности ИУС АЭС, затрагивающих:

взаимодействие между ядерной и компьютерной безопасностью;

управление доступом к цифровым ИУС, важным для безопасности АЭС;

защиту линий связи с аварийными центрами (такие линии связи должны быть защищены от вмешательства и исключать возможность негативного удаленного воздействия на ИУС);

функции обеспечения компьютерной безопасности в процессе эксплуатации (должны применяться средства выявления компьютерных угроз и смягчения их влияния);

необходимость разработки и реализации плана обеспечения компьютерной безопасности;

реализацию мер по предотвращению хакерских атак, умышленного или неумышленного искажения программного обеспечения или данных, внедрения вредоносного

программного кода, некорректного подключения к внешним сетям передачи данных.

Стандарты МЭК. Стандарты МЭК можно классифицировать по трем признакам:

уровню, определяемому местом стандарта в иерархии стандартов серий «Атомные электростанции. Информационные и управляющие системы АЭС, важные для безопасности» и «Атомные электростанции. Информационные и управляющие системы»;

посвящен ли стандарт специально компьютерной безопасности или компьютерная безопасность является одним из предметов рассмотрения в стандарте;

утвержден ли и издан стандарт или находится в процессе разработки.

Структура стандартов МЭК, относящихся к компьютерной безопасности ИУС АЭС, приведена на рис. 2.

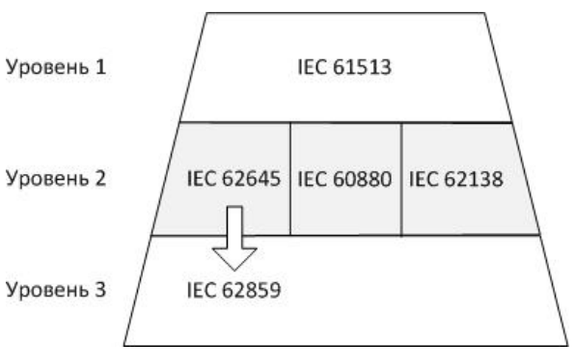

Рис. 2. Структура стандартов МЭК, относящихся к компьютерной безопасности ИУС АЭС

Стандарт IEC 61513 [13] — единственный стандарт 1-го уровня структуры. Компьютерная безопасность — один из аспектов рассмотрения. Содержит требования к физической безопасности (составной частью которой является компьютерная безопасность) на уровне АЭС в целом и на уровне отдельных систем, в частности — к общему плану обеспечения физической безопасности и к плану обеспечения физической безопасности системы. Приведено требование к наличию планов компьютерной безопасности как общего (Overall) для АСУТП блока, так и для отдельных ИУС.

Общий план определяет процедурные и технические меры по защите архитектуры ИУС от компьютерных атак, которые могут подвергать опасности функции, важные для безопасности:

систематическое управление риском от несанкционированного доступа и модификации на всех фазах жизненного цикла;

поддержание безопасности процедур интерфейса с административным и техническим персоналом, доступа, модификаций и технического облуживания, отчетности и аудита, обучения безопасности;

физическая защита от несанкционированного доступа;

запрет внешнего по отношению к АЭС доступа к ИУС, выполняющим функции категорий* A, B, и ограничение такого доступа к ИУС, выполняющим функции категории C;

документирование любого доступа к ИУС.

План для отдельных ИУС должен предусматривать трансформацию мер из общего плана в технические требования к проекту и документации на ИУС.

Стандарт IEC 62138 [15] — стандарт 2-го уровня. Компьютерная безопасность — один из аспектов рассмотрения. Развивает требования к компьютерной безопасности, приведенные в IEC 61513 [13], применительно к программному обеспечению (ПО) ИУС, выполняющих функции категорий B и C. Содержит два пункта, непосредственно посвященных компьютерной безопасности: п. 5.1.6 рассматривает компьютерную безопасность в числе общих требований к ПО ИУС, выполняющих функции категории C, а п. 6.1.6 — в числе общих требований к ПО ИУС, выполняющих функции категории B. В этих пунктах приведены требования к идентификации критических для компьютерной безопасности данных и функций; идентификации и аутентификации персонала; к контролю доступа к критическим для компьютерной безопасности данным и функциям; управлению критическими для компьютерной безопасности данными и функциями; прослеживаемости компьютерной безопасности в части действий персонала.

Стандарт IEC 60880 [16] — стандарт 2-го уровня. Компьютерная безопасность — один из аспектов рассмотрения. Развивает требования к компьютерной безопасности, приведенные в IEC 61513 [13], применительно к ПО ИУС, выполняющих функции категории A. Требования стандарта направлены на минимизацию уязвимостей ПО.

Стандарт содержит пп. 5.7 и 12.2, непосредственно посвященные компьютерной безопасности.

В п. 5.7 «Компьютерная безопасность программного обеспечения» рассматриваются:

анализ компьютерной безопасности ПО;

компьютерная безопасность при проектировании ПО (для оператора должна быть исключена возможность изменения хранящихся программ; в проектной документации определяются и описываются функции, критические для компьютерной безопасности; при верификации ПО подтверждается его компьютерная безопасность);

доступ пользователей (с требованиями к их аутентификации);

компьютерная безопасность при разработке ПО.

В п. 12.2 «Компьютерная безопасность на месте эксплуатации» говорится о необходимости оценки потенциальных угроз компьютерной безопасности с учетом их изменений при модернизации ПО. Приводятся меры обеспечения компьютерной безопасности при вводе ПО в эксплуатацию и при модернизации.

Отметим, что рассмотренные выше стандарты МЭК содержат лишь некоторые общие требования, которые относятся к компьютерной безопасности.

Стандарт IEC 62645 [17] — стандарт 2-го уровня. Компьютерная безопасность — основной объект рассмотрения: стандарт полностью посвящен вопросам компьютерной безопасности (причем всех ИУС АЭС, а не только важных для безопасности), устанавливает требования к разработке и реализации программы компьютерной безопасности для ИУС АЭС, определяет жизненный цикл и описывает основные меры обеспечения компьютерной безопасности ИУС АЭС. Сфокусирован на определении требований к программе компьютерной безопасности и к процессу разработки ИУС АЭС для предупреждения или минимизации влияния атак на компьютерные системы; ориентирован на применение в течение всего жизненного цикла при модернизации существующих и проектировании новых АЭС; представляет подход к установке требований, правил разработки, управлению эффективной

* Категории функций определяются согласно стандарту IEC 61226 [14].

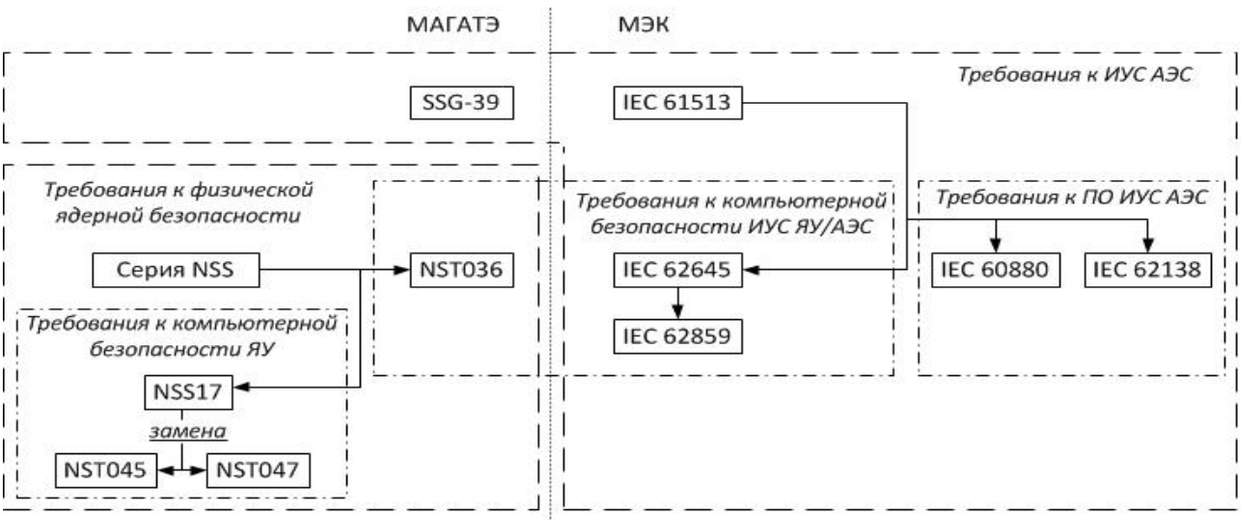

Рис. 3. Взаимосвязи между документами МАГАТЭ и стандартами МЭК

программой безопасности для ИУС АЭС и реализации жизненного цикла защищенности ИУС.

В IEC 62645 установлены основные требования к управлению защищенностью, в частности: к политике защищенности; организационной защищенности; управлению ресурсами (техническими, программными, информационными); защищенности человеческих ресурсов; физической защищенности и защищенности окружающей среды; управлению доступом.

Важным аспектом, рассмотренным в [17], является определение трех степеней компьютерной безопасности (security degree*) ИУС, в зависимости от которых устанавливается жесткость требований к компьютерной безопасности конкретной ИУС (только для ИУС, участвующих в управлении технологическим процессом; прочие компьютерные системы, действующие на АЭС, не рассматриваются). Даны предложения по установлению взаимосвязи между степенями компьютерной безопасности и категориями функций, выполняемых ИУС (такая взаимосвязь в определенном смысле является взаимосвязью между компьютерной и ядерной безопасностью). Установлены требования к мерам компьютерной безопасности как общего характера, так и для разных степеней компьютерной безопасности ИУС АЭС (более подробно степени компьютерной безопасности ИУС АЭС будут рассмотрены в одной из следующих публикаций).

Несмотря на то что IEC 62645 издан в 2014 году, уже начата разработка второй редакции стандарта. Это демонстрирует, насколько активно в мире развивается область компьютерной безопасности ИУС АЭС.

Стандарт IEC 62859 [18] (проект) — стандарт 3-го уровня, прямо подчиненный стандарту IEC 62645 [17]. Компьютерная безопасность — основной объект рассмотрения. Как и IEC 62645 [17], распространяется на все ИУС АЭС, а не только на важные для безопасности. Содержит принципы оптимизации учета требований к компьютерной безопасности при формировании архитектуры ИУС АЭС (которая ранее была нацелена на соответствие требованиям ядерной безопасности), предотвращения конфликтов между обеспечением ядерной и компьютерной безопасности, оказания помощи в достижении синергии между ядерной и компьютерной безопасностью.

Рассмотрена координация ядерной и компьютерной безопасности как на уровне общей архитектуры АСУТП, так и на уровне отдельных ИУС. Указана необходимость анализа полезности обеспечивающих ядерную безопасность мер по предотвращению отказов по общей причине, физического разделения, диверсности для компьютерной безопасности. Обращено внимание на то, что применение мер по компьютерной безопасности может усложнить ИУС и ввести новые источники отказов. Отмечено, что реализация мер по обеспечению компьютерной безопасности не должна снижать характеристики ИУС (надежность, быстродействие, эффективность и др.). Предусмотрено, что меры по обеспечению компьютерной безопасности реализуются на всех этапах жизненного цикла ИУС (этапах разработки требований, проектирования, валидации, внедрения, испытаний, эксплуатации, модификации).

Сформулировано требование к выделению зон компьютерной безопасности (более подробно такие зоны будут рассмотрены в одной из следующих публикаций).

Приведены требования к техническим мероприятиям по обеспечению: компьютерной безопасности в части управления доступом для операторов на щитах управления; использования принципов криптографии для защиты важной информации; модификации программного обеспечения и др.

Взаимосвязь между документами МАГАТЭ и МЭК. Рассмотренные действующие и разрабатываемые документы МАГАТЭ и стандарты МЭК относятся к различным областям знаний, однако все содержат (частично или полностью) требования к компьютерной безопасности, находящиеся на стыке этих областей знаний (рис. 3). Поэтому вопросы компьютерной безопасности нельзя рассматривать без учета общих требований к ИУС АЭС и требований к физической ядерной безопасности.

Документы US NRC. Ядерная регулирующая комиссия США (US NRC) выпустила в 2010 году регулирующее руководство RG 5.71 [19], которое определяет требования к программе компьютерной безопасности ядерных

* Термин «security degree» аналогичен принятому в публикациях МАГАТЭ термину «security level», однако считается более предпочтительным в настоящее время.

установок, а также предусматривает разработку, внедрение (с описанием соответствующих стадий) и реализацию плана обеспечения компьютерной безопасности.

В этом основном документе США по компьютерной безопасности ядерных установок описаны структура жизненного цикла процесса обеспечения компьютерной безопасности: проектирование программы компьютерной безопасности, ее внедрение на установках, постоянный мониторинг программы, периодический пересмотр программы, управление изменениями и сохранение документации.

Для разработки, внедрения и обслуживания программы компьютерной безопасности предполагается реализация следующих действий:

анализ цифровых систем и сетей ядерных установок;

выявление и оценка критических ресурсов с точки зрения безопасности;

внедрение безопасной архитектуры в соответствии с определенными нормативами;

анализ потенциальных рисков нарушений компьютерной безопасности;

реализация деятельности по обслуживанию программы компьютерной безопасности.

В RG 5.71 [19] введены уровни компьютерной безопасности*, представлена диаграмма взаимодействия этих уровней и их описание. Кроме того, документ содержит описание групп технических, эксплуатационных и управленческих методов обеспечения безопасности по каждому ресурсу, критическому для безопасности, и подходы к внедрению методов.

Нормативная база Украины. В Украине в настоящее время существует развитая законодательная база в сфере информационной безопасности и ядерной защищенности, одним из компонентов которой есть компьютерная безопасность. Ряд действующих в Украине норм и правил (например, НП 306.2.141-2008 [20], ГНД 306.7.02/2.041-2000 [21]) содержит общие требования к физической безопасности, к защите от несанкционированного доступа к ИУС АЭС и к безопасности ПО ИУС АЭС, охватывая отдельные элементы компьютерной безопасности. Однако нормативные документы, которые содержали бы более полные и детальные требования к компьютерной безопасности ИУС АЭС, представлены недостаточно, не гармонизированы с современными международными стандартами и требуют развития.

Одним из первых шагов в направлении развития требований к компьютерной безопасности ИУС АЭС является планируемый в 2015 году ввод в действие нового нормативного документа Государственной инспекции ядерного регулирования Украины — «Требования по ядерной и радиационной безопасности информационных и управляющих систем, важных для безопасности атомных станций». По аналогии с IEC 61226 [14], указанным документом вводится классификация функций ИУС АЭС по категориям A, B, C в зависимости от их роли в обеспечении и поддержании безопасности, а также от возможных последствий, вызванных невыполнением или ошибочным выполнением функций. Регламентируются требования по ядерной и радиационной безопасности ИУС АЭС, а также некоторые требования, касающиеся компьютерной безопасности ИУС АЭС. Согласно этим требованиям, ПО, которое участвует в выполнении функций категорий A, B и C, должно быть защищено от нежелательного и опасного вмешательства в его работу, а также от несанкционированного изменения через внешние компьютерные сети и/или при использовании внешних носителей данных. ПО, которое участвует в выполнении функций, относящихся к категории A, полностью изолируется от взаимодействия с внешними компьютерными сетями. ПО, которое принимает участие в выполнение функций, относящихся к категориям B и C, изолируется от доступа к сети Интернет.

Любые изменения в ПО могут вноситься только после соответствующей авторизации; возможность несанкционированного изменения ПО вручную или с использованием внешних носителей данных должна быть исключена.

Должна быть исключена и возможность негативного влияния принятых мер защиты от кибернетических угроз на выполнение программ и/или на характеристики выполнения функций, которые реализуются с использованием программных средств.

Поскольку данный документ содержит требования к ядерной и радиационной безопасности ИУС АЭС и не относится непосредственно к компьютерной безопасности ИУС АЭС, приведенные в нем требования к компьютерной безопасности имеют общий характер. Важной задачей для Украины является разработка нормативного документа с детальными требованиями к компьютерной безопасности ИУС АЭС, в котором должны быть учтены существующие и разрабатываемые документы МАГАТЭ (в том числе NSS17 [10], NST036 [11]) и международные стандарты (в частности, IEC 62645 [17]).

Выводы

По результатам краткого анализа существующей нормативной базы по компьютерной безопасности ядерных установок и ИУС АЭС следует констатировать, что ее разработка чрезвычайно актуальна как для международных организаций, так и национальных регулирующих органов (наиболее активно проводится в США).

В настоящее время проблемы нормативного регулирования компьютерной безопасности ИУС, важных для безопасности АЭС, не решены в полной мере. В существующих документах не рассмотрены многие специфические технические аспекты компьютерной безопасности ИУС АЭС (например, защита от вредоносных программных закладок). Отсутствует единство принятых подходов (например, по определению уровней компьютерной безопасности).

Отметим, что кроме нормативных документов с регулирующими требованиями по компьютерной безопасности целесообразно также разрабатывать документы, где будут рассматриваться технические аспекты, проводиться анализ потенциальных кибернетических угроз и даваться конкретные методические рекомендации по мерам обеспечения компьютерной безопасности ИУС АЭС на разных стадиях жизненного цикла с учетом особенностей применяемых технологий.

В Украине при дальнейшей разработке нормативных документов с детальными требованиями к компьютерной безопасности ИУС АЭС целесообразно рассматривать последние в комплексе с требованиями к ядерной безопасности, а также с учетом требований международных стандартов.

* Нумерация уровней компьютерной безопасности в RG 5.71 [18] обратна нумерации, приведенной в рекомендациях МАГАТЭ и МЭК.

Список использованной литературы

1. South Korea's nuclear plant operator hacked // Nuclear News. — February 2015. — P. 30-31.

2. *Клевцов А. Л.* Компьютерная безопасность информационных и управляющих систем АЭС: кибернетические угрозы / А. Л. Клевцов, С. А. Трубчанинов // Ядерна та радіаційна безпека. — 2015. — № 1 (65). — С. 54—58.

3. Nuclear Power Plant Instrumentation and Control Systems for Safety and Security / Edited by Yastrebenetsky M., Kharchenko V. — USA, Hershey, IGI Global, 2014. — 450 p.

4. Objective and essential elements of a State's nuclear security regime : nuclear security fundamentals. — Vienna : International Atomic Energy Agency, 2013. — (IAEA nuclear security series, ISSN 1816-9317; No. 20). — ISBN 978-92-0-137810-1.

5. Nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INFCIRC/225/Revision 5) : recommendations. — Vienna : International Atomic Energy Agency, 2010. — (IAEA nuclear security series, ISSN 1816-9317; No. 13). — ISBN 978-92-0-111110-4.

6. Nuclear security recommendations on radioactive material and associated facilities : recommendations. — Vienna : International Atomic Energy Agency, 2011. — (IAEA nuclear security series, ISSN 1816-9317; No. 14). — ISBN 978-92-0-112110-3.

7. Nuclear security culture : implementing guide. — Vienna : International Atomic Energy Agency, 2008. — (IAEA nuclear security series, ISSN 1816-9317; No. 7). — ISBN 978-92-0-107808-7.

8. Preventive and protective measures against insider threats : implementing guide. — Vienna : International Atomic Energy Agency, 2008. — (IAEA nuclear security series, ISSN 1816-9317; No. 8). — ISBN 978-92-0-109908-2.

9. Security of nuclear information. — Vienna : International Atomic Energy Agency, 2015. — (IAEA nuclear security series, ISSN 1816-9317; No. 23-G). — ISBN 978-92-0-110614-8.

10. Computer security at nuclear facilities : reference manual : technical guidance. — Vienna : International Atomic Energy Agency, 2011. — (IAEA nuclear security series, ISSN 1816-9317; No. 17). — ISBN 978-92-0-120110-2.

11. Computer security of instrumentation and control systems at nuclear facilities (Draft). — Vienna : International Atomic Energy Agency. 2014. — (IAEA nuclear security series, NST036). — 47 p.

12. Design of Instrumentation and Control Systems for Nuclear Power Plants (Draft). — Vienna : International Atomic Energy Agency. 2015. — (Specific Safety Guide, SSG-39). — 88 p.

13. *IEC 61513.* Nuclear power plants — instrumentation and control important to safety — General requirements for systems. — Geneva : International Electrotechnical Commission, 2011. — ISBN 978-2-88912-663-7.

14. *IEC 61226.* Nuclear power plants − Instrumentation and control important to safety — Classification of instrumentation and control functions. — Geneva : International Electrotechnical Commission, 2009. − ISBN 978-2-88910-448-2.

15. *IEC 62138.* Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions. — Geneva : International Electrotechnical Commission, 2004. — 95 p.

16. *IEC 60880.* Nuclear power plants — Instrumentation and control systems important to safety — Software aspects for computer-based systems performing category A functions. — Geneva : International Electrotechnical Commission, 2006. — 217 p.

17. *IEC 62645.* Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based system. — Geneva : International Electrotechnical Commission, 2014. — ISBN 978-2-8322-1810-5.

18. *IEC 62859.* Nuclear power plants — Instrumentation and control systems — Requirements for coordinating safety and cybersecurity. (Draft) — Geneva : International Electrotechnical Commission, 2014. — 19 p.

19. *RG 5.71.* Cyber security programs for nuclear facilities. — Washington : U.S. Nuclear Regulatory Commission, 2010. — 105 p.

20. *НП 306.2.141-2008.* Загальні положення безпеки атомних станцій. — К. : Державний комітет ядерного регулювання України, 2008. — 59 с.

21. *ГНД 306.7.02/2.041-2000.* Методика оцінки відповідності інформаційних і керуючих систем, важливих для безпеки атомних станцій, вимогам з ядерної та радіаційної безпеки. — К. : М-во екології та природних ресурсів України, 2008. — 45 с.

References

1. South Korea's Nuclear Plant Operator Hacked (2015), Nuclear News, No. 2 (58), pp. 30-31.

2. *Klevtsov, A. L., Trubchaninov, S. A.* (2015), "Computer Security of NPP Instrumentation and Control Systems: Cyber Threats" [Kompiuternaia bezopasnost' informatsionnykh i upravliaiushchikh sistem AES: kiberneticheskie ugrozy], Nuclear and Radiation Safety, No. 1 (65), pp. 54—58. (Rus)

3. *Yastrebenetsky, M., Kharchenko, V.* (2014), "Nuclear Power Plant Instrumentation and Control Systems for Safety and Security", IGI Global, Hershey, USA, 450 p.

4. IAEA Nuclear Security Series, No. 20 (2013), Objective and Essential Elements of a State's Nuclear Security Regime: Nuclear Security Fundamentals, International Atomic Energy Agency, Vienna, 32 p. (IAEA Nuclear Security Series, ISSN 1816-9317; No. 20), ISBN 978-92-0-137810-1.

5. IAEA Nuclear Security Series, No. 13 (2010), Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, International Atomic Energy Agency, Vienna, 76 p. (IAEA nuclear security series, ISSN 1816-9317; No. 13), ISBN 978-92-0-111110-4.

6. IAEA Nuclear Security Series, No. 14 (2011), Nuclear Security Recommendations on Radioactive Material and Associated Facilities: Recommendations, International Atomic Energy Agency, Vienna, 44 p. (IAEA Nuclear Security Series, ISSN 1816-9317; No. 14), ISBN 978-92-0-112110-3.

7. IAEA Nuclear Security Series, No. 7 (2008), Nuclear Security Culture: Implementing Guide, International Atomic Energy Agency, Vienna, 48 p. (IAEA Nuclear Security Series, ISSN 1816-9317; No. 7), ISBN 978-92-0-107808-7.

8. IAEA Nuclear Security Series, No. 8 (2008), Preventive and Protective Measures against Insider Threats: Implementing Guide, International Atomic Energy Agency, Vienna, 36 p. (IAEA Nuclear Security Series, ISSN 1816-9317; No. 8), ISBN 978-92-0-109908-2.

9. IAEA Nuclear Security Series, No. 23-G (2015), Security of Nuclear Information, International Atomic Energy Agency, Vienna, 68 p. (IAEA nuclear security series, ISSN 1816-9317; No. 23-G), ISBN 978-92-0-110614-8.

10. IAEA Nuclear Security Series, No. 17 (2011), Computer Security at Nuclear Facilities: Reference Manual: Technical Guidance, International Atomic Energy Agency, Vienna, 88 p. (IAEA nuclear security series, ISSN 1816-9317; No. 17), ISBN 978-92-0-120110-2.

11. IAEA Nuclear Security Series, NST036 (2014), Computer Security of Instrumentation and Control Systems at Nuclear Facilities (Draft), International Atomic Energy Agency, Vienna, 47 p.

12. Specific Safety Guide, SSG-39 (2015), Design of Instrumentation and Control Systems for Nuclear Power Plants (Draft), International Atomic Energy Agency, Vienna, 88 p.

13. *IEC 61513* (2011), Nuclear Power Plants — Instrumentation and Control Important to Safety — General Requirements for Systems, International Electrotechnical Commission, Geneva, 205 p. (ISBN 978-2-88912-663-7)

14. *IEC 61226* (2009), Nuclear Power Plants — Instrumentation and Control Important to Safety — Classification of Instrumentation and Control Functions, International Electrotechnical Commission, Geneva, 64 p. (ISBN 978-2-88910-448-2)

15. *IEC 62138* (2004), Nuclear Power Plants — Instrumentation and Control Important to Safety — Software Aspects for Computer-Based Systems Performing Category B or C Functions, International Electrotechnical Commission, Geneva, 95 p.

16. *IEC 60880* (2006), Nuclear Power Plants — Instrumentation and Control Systems Important to safety — Software Aspects for Computer-Based Systems Performing Category A Functions, International Electrotechnical Commission, Geneva, 217 p.

17. *IEC 62645* (2014), Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Security Programmes for Computer-Based System, International Electrotechnical Commission, Geneva, 93 p. (ISBN 978-2-8322-1810-5)

18. *IEC 62859* (2014), Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Coordinating Safety and Cybersecurity. (Draft), International Electrotechnical Commission, Geneva, 19 p.

19. *RG 5.71* (2010), Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, Washington, 105 p.

20. *NP 306.2.141* (2008), "General Safety Provisions for Nuclear Power Plants" [Zahalni polozhennia bezpeky atomnykh stantsii], State Nuclear Regulatory Committee of Ukraine, Kyiv, 59 p. (Ukr)

21. *GND 306.7.02/2.041* (2000), "Methodology to Assess Compliance of Instrumentation and Control Systems Important to Safety with Requirements for Nuclear and Radiation Safety" [Metodyka otsinky vidpovidnosti informatsiinykh ta keruiuchykh system, vazhlyvykh dlia bezpeky atomnykh stantsii, vymoham z yadernoi ta radiatsiinoi bezpeky], Ministry of Ecology and Natural Resources of Ukraine, Kyiv, 45 p. (Ukr)

Получено 02.06.2015.

Правила для авторів

1. Рукопис статті журналу подається у вигляді твердої копії з підписами всіх авторів на останній сторінці, а також електронної версії (на електронному носії або електронною поштою). До публікації приймаються лише оригінальні твори, присвячені проблемам ядерної та радіаційної безпеки.

2. Стаття має містити УДК. Українською, російською та англійською мовами наводяться анотація, назва статті, ключові слова, прізвище, ім'я та по батькові автора, назва організації, де працює автор.

3. Загальний обсяг статті разом з графічними матеріалами не повинен перевищувати 18 сторінок формату А4. На одній сторінці може бути не більш як 30 рядків та до 60 знаків (з урахуванням розділових знаків і проміжків між словами) у кожному рядку. Розмір шрифту підготовленого на комп'ютері матеріалу — 14; міжрядковий інтервал — 1,5. Розміри полів, мм: зліва — 30, справа —10, зверху — 20, знизу — 25.

4. Текст набирається шрифтом Times New Roman у редакторі Microsoft Word. Графічний матеріал (чорно-білий) подається у форматі EPS, TIFF або JPG-файлів з густиною точок на дюйм 300–600 dpi. Ілюстрації подаються окремо від тексту.

5. Статті, які є результатами робіт, проведених в організаціях, повинні мати супровідний документ від цих організацій.

6. Разом зі статтею до редакції журналу має бути поданий документ про можливість відкритої публікації матеріалів, а також про згоду на поширення їх через мережу Інтернет.

7. До авторського оригіналу статті на окремому аркуші додаються: прізвище, ім'я, по батькові (повністю) автора, організація, в якій він працює, посада, вчений ступінь, звання, мобільний, службовий і домашній номери телефону, службова та домашня адреси.

8. Скорочення слів, словосполучень, назв, термінів, за винятком загальноприйнятих, можливе тільки після їх повного першого згадування в тексті.

9. Зміст наукових статей будується за такою структурою:

коротка анотація – стислі відомості про статтю (до 10 рядків);

вступ — постановка наукової проблеми, її актуальність, зв'язок з державними науковими та практичними програмами, значення вирішення проблеми;

основні дослідження і публікації — аналітичний огляд останніх досліджень і публікацій з даної проблеми, виокремлення не розв'язаних раніше питань;

формування мети статті — опис головної ідеї даної публікації, чим вона відрізняється, доповнює та поглиблює вже відомі підходи, які нові факти, закономірності висвітлює (до 15 рядків);

викладення основного змісту проведеного дослідження — головна частина статті, де висвітлюються основні положення дослідження, програма і методика експерименту, отримані результати та їх обгрунтування, виявлені закономірності, аналіз результатів, особистий внесок автора;

висновки — основні підсумки, рекомендації, значення для теорії й практики, перспективи подальших досліджень;

список літератури — перелік літературних джерел, на які є посилання в тексті статті; вказати автора та назву твору, місце публікації (для книжки — місто та видавництво, для статті — назву збірника чи журналу, його номер або випуск), дату публікації, кількість сторінок у книжці або сторінки, на яких вміщено статтю.

10. Матеріали, які неохайно оформлені і не відповідають зазначеним вимогам, редакцією не розглядаються.

11. Для скорочення витрат на видання журналу виплата авторського гонорару не передбачається.

12. Матеріали, що надійшли до редакції, авторам не повертаються.