УДК 621.039:004.9

А. Л. Клевцов, С. А. Трубчанинов

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

Компьютерная безопасность информационных и управляющих систем АЭС: кибернетические угрозы

Статья посвящена изучению кибернетических угроз как одного из аспектов компьютерной безопасности информационных и управляющих систем АЭС. Кратко рассмотрены базовые понятия, термины и определения в области компьютерной безопасности. Дан анализ потенциальных кибернетических угроз на стадиях разработки и эксплуатации информационных и управляющих систем АЭС. Указаны основные типы угроз, среди которых вредоносные закладки в программном обеспечении и технических средствах (в частности покупных), компьютерные атаки по сетям передачи данных, внесение вредоносных программ с внешних носителей информации и портативных устройств. Особое внимание уделено влиянию программного обеспечения более низких классов безопасности на программное обеспечение более высоких классов безопасности. Приведены примеры реальных инцидентов на ядерных установках, вызванных умышленными кибернетическими атаками или неумышленными компьютерными ошибками при работе с программным обеспечением систем, важных для безопасности АЭС.

Ключевые слова: компьютерная безопасность, кибернетическая угроза, кибернетическая атака, информационная и управляющая система, программная закладка.

О. Л. Клевцов, С. О. Трубчанінов

Комп'ютерна безпека інформаційних та керуючих систем АЕС: кібернетичні загрози

Статтю присвячено вивченню кібернетичних загроз як одного з аспектів комп'ютерної безпеки інформаційних та керуючих систем АЕС. Коротко розглянуто базові поняття, терміни й визначення у сфері комп'ютерної безпеки. Дано аналіз потенційних кібернетичних загроз на стадіях розробки й експлуатації інформаційних та керуючих систем АЕС. Наведено основні типи загроз, серед яких шкідливі закладки в програмному забезпеченні й технічних засобах (зокрема покупних), комп'ютерні атаки по мережах передачі даних, внесення шкідливих програм із зовнішніх носіїв інформації та портативних пристроїв. Особливу увагу приділено впливу програмного забезпечення низьких класів безпеки на програмне забезпечення більш високих класів безпеки. Наведено приклади реальних інцидентів на ядерних установках, спричинених умисними кібернетичними атаками або ненавмисними комп'ютерними помилками під час роботи з програмним забезпеченням систем, важливих для безпеки АЕС.

Ключові слова: комп'ютерна безпека, кібернетична загроза, кібернетична атака, інформаційна та керуюча система, програмна закладка.

Международное агентство по атомной энергии (МАГАТЭ), Международная электротехническая комиссия (МЭК), национальные органы регулирования ядерной и радиационной безопасности разных стран (США, Германия и др.) уделяют значительное внимание вопросам исследования и регулирования компьютерной безопасности АЭС. Это вызвано тремя основными факторами: широкомасштабным переходом от аналоговых систем к цифровым информационным и управляющим системам (ИУС) АЭС, уязвимостью таких систем к кибернетическим (компьютерным) угрозам и увеличением количества случаев злоумышленного вмешательства в работу компьютерных систем с серьезными последствиями.

Обеспечение компьютерной безопасности — задача важная, поскольку кибернетические атаки могут негативно влиять как на физическую, так и на ядерную и радиационную безопасность АЭС и других ядерных установок. Многие страны уже более 10 лет занимаются реализацией соответствующих мероприятий по защите от компьютерных угроз, а также разработкой соответствующей нормативной базы, руководствуясь при этом рекомендациями, изложенными в документах МАГАТЭ (например, в [1]). В Украине же данной проблеме не уделяется достаточного внимания и наблюдается существенное отставание (по сравнению с другими странами) в вопросах нормативного регулирования и внедрения практических мер защиты от компьютерных угроз. Работы, проводимые АЭС и предприятиями-разработчиками ИУС по обеспечению компьютерной безопасности, не носят системного характера ввиду отсутствия единых подходов, методов и нормативной базы.

Данной публикацией авторы начинают цикл статей по компьютерной безопасности информационных и управляющих систем АЭС с целью всестороннего изучения этой проблематики. В статьях будут проанализированы различные аспекты компьютерной безопасности: виды компьютерных угроз, требования международных стандартов по компьютерной безопасности, средства обеспечения компьютерной безопасности на АЭС (в том числе на АЭС Украины) и на предприятиях-разработчиках ИУС, методы оценки компьютерной безопасности и др.

В настоящей статье рассматриваются основные возможные кибернетические угрозы для ИУС АЭС. Подробный анализ мер защиты в данной статье не проводится, он будет представлен в одной из последующих статей.

Основные термины и определения

Поскольку среди принятых терминов и определений существует ряд неоднозначностей, сделаем ряд вводных комментариев.

Прежде всего, в английском языке слова *safety* и *security* имеют разное значение, однако переводятся на русский язык одним словом — *безопасность*, что может привести к некоторой путанице в терминах. Во избежание этого будем далее руководствоваться терминологией МАГАТЭ.

Согласно документу IAEA NSS No. 17 [1] (который официально издан как на английском, так и на русском языке), англоязычному термину *computer security* соответствует русскоязычный термин *компьютерная безопасность*, а термину *security* — *физическая безопасность*. Компьютерная безопасность определена в вышеупомянутом документе как специфический аспект информационной безопасности, относящийся к компьютерным системам, сетям

и цифровым системам. При этом компьютерная безопасность рассматривается как важная часть общей физической безопасности (*security*) ядерной установки. Целью компьютерной безопасности является защита характеристик конфиденциальности, целостности и доступности электронных данных или готовности компьютерных систем и процессов.

В некоторых международных стандартах, например в IEC 61513 [2], которому соответствуют ГОСТ Р МЭК 61513 [3] и ДСТУ IEC 61513 [4], термину *security* соответствует термин *защищенность* (однако в данной статье, как было сказано, используется терминология, принятая МАГАТЭ).

Вместо термина *компьютерная безопасность* (*computer security*) в некоторых международных стандартах приводятся термины *кибернетическая безопасность* (*cyber security*) или *безопасность информационных технологий* (*IT security*). МАГАТЭ, считая эти термины синонимами, в своих документах употребляет единый термин — *компьютерная безопасность* [1].

В свою очередь, под термином *безопасность* (*safety*) в документе IAEA SSS No. SF-1 [5] (и в данной статье) понимается защита людей и охрана окружающей среды от радиационных рисков, обеспечение безопасности установок и деятельности, связанной с радиационными рисками. Термин *безопасность* в стандартах МАГАТЭ включает безопасность ядерных установок, радиационную безопасность, безопасность обращения с радиоактивными отходами, безопасность перевозки радиоактивного материала, не затрагивая не связанных с радиацией аспектов безопасности.

В настоящей статье мы ограничиваемся только рассмотрением ИУС, непосредственно участвующих в управлении и мониторинге технологических процессов на АЭС (исключив системы физической защиты и прочие системы, не относящиеся непосредственно к технологическому процессу), и дифференцируем системы в зависимости от их классов безопасности согласно НП 306.2.141 [6]. Конечно, при рассмотрении вопросов компьютерной безопасности более корректно дифференцировать системы по уровням безопасности. Уровни безопасности, в соответствии с [1], определяют степени защиты физической безопасности, требуемые для различных компьютерных систем на ядерной установке. Согласно [1], строгость мер компьютерной безопасности зависит не от класса безопасности системы, а именно от установленного для нее уровня безопасности, поскольку некоторые системы АЭС не классифицируются по безопасности, но являются важными с точки зрения обеспечения физической безопасности и должны быть защищены от кибернетических угроз. Тем не менее, в настоящее время классификация по уровням безопасности в Украине не устанавливается, а авторы хотели бы обратить внимание на некоторые аспекты, которые зависят именно от классов безопасности ИУС АЭС. Принципы определения уровней безопасности будут рассмотрены в одной из последующих статей данной серии.

Виды кибернетических угроз

Кибернетические атаки, вирусы, программные закладки, несанкционированные модификации программного обеспечения и данных представляют угрозу для АЭС, поскольку могут опасно влиять на функционирование ИУС АЭС и на технологические процессы, которые реализуются под управлением этих ИУС. Ввиду этого предприятия-разработчики ИУС АЭС и эксплуатирующая организация (НАЭК «Энергоатом») должны применять меры защиты от кибернетических угроз при закупке элементной базы и комплектующих изделий, в процессе разработки ИУС и при эксплуатации ИУС на АЭС.

Базовая классификация злоумышленных действий, совершаемых в отношении компьютерных систем и затрагивающих физическую, ядерную и радиационную безопасность, приведена в [1]:

атаки для сбора информации с целью планирования и осуществления дальнейших преступных действий;

атаки, направленные на отключение или ухудшение работы одного или нескольких компьютеров (ИУС, технических средств), критически важных для физической защиты или безопасности ядерных установок;

нарушения нормальной работы одного или нескольких компьютеров (ИУС, технических средств) совместно с другими параллельными режимами атаки, такими как физическое вторжение на ядерную установку.

Представленная классификация носит общий характер. Для лучшего понимания масштаба решаемых задач по обеспечению компьютерной безопасности и последующей разработки мер по защите от этих угроз целесообразно разрабатывать более детальные классификации потенциальных угроз.

По результатам анализа, выполненного ГНТЦ ЯРБ, предлагается выделить две большие группы кибернетических угроз:

кибернетические угрозы на стадии разработки ИУС;

кибернетические угрозы на стадии эксплуатации ИУС на АЭС.

В свою очередь, в каждой из указанных групп можно выделить несколько основных типов кибернетических угроз по способу воздействия на ИУС, важные для безопасности АЭС.

Кибернетические угрозы на стадии разработки ИУС. В эту группу входят такие вредоносные воздействия, которые имеют место в процессе разработки ИУС и их компонентов (технических средств и программного обеспечения), а их результаты затем негативно сказываются при функционировании ИУС в период эксплуатации на АЭС. Рассмотрим подробнее возможные типы угроз данной группы.

Вредоносные закладки в программном обеспечении собственной разработки. Наличие в ПО собственной разработки определенного вредоносного программного кода, который может быть внесен кем-либо из группы разработчиков, представляет существенную опасность для последующей эксплуатации ИУС. Поэтому следует максимально контролировать программный код на всех этапах разработки ПО (разработка требований к ПО, проектирование ПО, кодирование ПО, интеграция ПО и технических средств). Одним из средств такого контроля является верификация, которая обязательна для ПО классов безопасности 2 и 3. Однако верификация, повышая вероятность выявления программных закладок, не гарантирует их полного отсутствия в ПО.

Поскольку в состав одной системы может входить ПО разных классов безопасности (например, ИУС класса безопасности 2 может включать в себя ПО классов безопасности 2, 3 и 4), возможно негативное влияние ПО более низкого класса безопасности на ПО более высокого класса безопасности. Верификация ПО класса безопасности 4 не обязательна в Украине; таким образом, данное

ПО становится удобным объектом для внедрения в него определенного вредоносного программного кода, который впоследствии может оказать негативное влияние на другие используемые в той же системе компоненты ПО более высоких классов безопасности и, как следствие, на работу системы в целом. Такому ПО должно быть уделено определенное внимание с точки зрения компьютерной безопасности, так как именно это ПО является наиболее уязвимым.

Вредоносные закладки в покупном программном обеспечении. В настоящее время в любой ИУС, важной для безопасности АЭС, используется то или иное покупное ПО. При этом вероятность наличия вредоносных программных закладок в нем не исключается. Имея дело с готовым продуктом, разработчик ИУС не может контролировать процесс разработки ПО на всех этапах (разработка требований, проектирование, кодирование, интеграция) и анализировать исходный код ПО. Анализ имеющегося в распоряжении разработчиков ИУС исполняемого кода — сложнейшая задача.

Негативное воздействие на программное обеспечение ИУС со стороны средств разработки ПО. Различные средства разработки ПО (генераторы кода, компиляторы, трансляторы и т. д.) могут формировать некорректный исходный или исполняемый программный код — как из-за непреднамеренных внутренних ошибок в этих инструментах, так и в результате умышленно заложенных в них вредоносных функций. Поэтому необходимы контроль правильности функционирования самих средств разработки и детальная проверка автоматически сгенерированного исходного и исполняемого кода.

Угрозы объектно-ориентированного программирования. В случае применения объектно-ориентированного программирования для разработки ПО ИУС АЭС необходимо учитывать, что в программном коде, как правило, будет использоваться существенное количество стандартных объектов, предлагаемых разработчиком языка программирования или сторонними разработчиками. Проблема состоит в том, что код стандартных объектов теоретически может содержать вредоносные команды, которые в определенных условиях могут негативно влиять на работу системы. Анализ кода стандартных объектов — достаточно сложная задача.

Закладки в технических средствах (hardware trojans). Закладки в технических средствах представляют собой вредоносные и умышленно скрытые модификации электронных устройств (например, микросхемы или ее внутренней программируемой конфигурации). Такая модификация может изменять функциональность модулей, которые содержат программируемые компоненты или базируются на технологии программируемых логических интегральных схем (ПЛИС), что ведет к нарушению их функционирования (например, в результате непредсказуемых отказов или дефектов) и, таким образом, может негативно влиять на работу системы, использующей это устройство. Подробный анализ закладок в технических средствах представлен в [7].

Внедрение закладок в технические средства возможно на стадиях разработки и производства самих электронных устройств или построенной на базе этих устройств системы в целом.

Закладки в технических средствах в зависимости от расположения могут прямо влиять на следующие компоненты:

процессор (изменять порядок выполнения команд);

память, включая ее интерфейсы (изменять значения, хранимые в памяти; блокировать операции чтения/записи для определенных областей памяти);

систему ввода-вывода (влиять на внутрисистемные связи или связи с внешними компонентами);

контур электропитания (изменять напряжение и силу тока, питающего микросхему или модуль, вызывая тем самым отказы);

временной контур (влиять на синхронизацию функционирования различных модулей, приводя тем самым к ошибкам и отказам системы).

Влияние закладок в технических средствах может варьироваться от незначительных нарушений в работе устройств, содержащих такую закладку, до опасных отказов системы, которая содержит такие устройства (например, если такая закладка будет внедрена в систему аварийной защиты). Возможные последствия можно разделить на следующие группы:

изменение функциональности устройства (путем добавления дополнительной логики или удаления части существующей логики), что обычно приводит к малозаметным ошибкам, которые практически непредсказуемы;

снижение производительности в результате умышленного изменения технических характеристик устройства с помощью закладки;

утечка информации через открытые или скрытые каналы;

отказ в выполнении операций устройством, который препятствует выполнению функций системы и обычно бывает вызван неожиданным недостатком ширины полосы пропускания, вычислительной мощности или мощности электропитания;

физическое повреждение, отключение устройства или изменение его конфигурации.

Кибернетические угрозы на стадии эксплуатации ИУС. Данная группа угроз включает в себя вредоносные воздействия, которые реализуются в процессе эксплуатации ИУС на АЭС и негативно влияют на ее функционирование. Перечислим основные типы угроз на этой стадии.

Негативное воздействие по сетям передачи данных (Интернет или локальные вычислительные сети). К таким воздействиям могут относиться как внедрение обычных вирусов, которые не направлены на конкретную систему, так и целенаправленные спланированные атаки на конкретную ИУС или конкретную АЭС. Первый тип угроз достаточно успешно нейтрализуется применением антивирусных программ и межсетевых экранов. Однако это лишь снижает риски и не гарантирует полную защиту, поскольку не защищает от проникновения с использованием уязвимостей самого ПО. В частности, угрозу представляют новые вирусы, информация о которых в определенные моменты времени отсутствуют в базах антивирусных программ. Кроме того, указанные средства недостаточно эффективны для защиты от угроз, когда атака имеет конкретную цель, хорошо спланирована и использует уязвимости ПО.

В связи с этим ПО систем, важных для безопасности АЭС, должно разрабатываться таким образом, чтобы исключить или минимизировать уязвимости. Целесообразно полностью исключить связь систем, важных для безопасности АЭС, с сетью Интернет. Для систем класса безопасности 2, согласно НП 306.2.141 [6], должна быть реализована только односторонняя (исходящая) передача

информации в системы более низких классов безопасности по сетям передачи данных. Для систем класса безопасности 3 нужно ограничить обмен данными с системами класса безопасности 4 и применять межсетевые экраны. Целесообразно разработать специальные требования к компьютерной безопасности систем класса безопасности 4 с целью недопущения негативного влияния на системы, важные для безопасности.

Необходимо оценить влияние средств защиты (антивирусных программ, межсетевых экранов и пр.) на пропускную способность каналов связи и на производительность систем, важных для безопасности АЭС, поскольку сами средства защиты не должны негативно влиять на работу систем.

Отметим, что сети передачи данных могут также использоваться злоумышленниками для получения важной закрытой информации и привилегированного удаленного доступа в качестве подготовки для последующих атак. Предотвращение таких действий является важной составляющей общей системы защиты от компьютерных атак.

Внесение вредоносных программ или данных с портативных устройств (мобильные телефоны, планшеты, ноутбуки и т. д.) либо с внешних носителей данных (CD, DVD, флэш-накопители, карты памяти, портативные жесткие диски и др.) в процессе эксплуатации. Портативные устройства могут использоваться с целью повреждения информации или внедрения вредоносного ПО в различные компьютерные системы АЭС через беспроводные соединения (Wi-Fi, Bluetooth), а также путем подключения таких устройств к компьютерам через USB-порты. В связи с этим использование портативных устройств следует ограничивать, реализуя, в частности, соответствующую защиту беспроводных соединений и их изоляцию от сетей, к которым подключены ИУС, важные для безопасности.

Наиболее яркий пример негативного воздействия с применением внешнего носителя данных — широкоизвестный Stuxnet, который был непреднамеренно внесен в систему с персонального флэш-накопителя сотрудника компании Siemens. Это первый известный компьютерный червь, перехватывающий и модифицирующий информационный поток между программируемыми логическими контроллерами марки Simatic S7 и рабочими станциями SCADA-системы Simatic WinCC фирмы Siemens. Уникальность вируса заключалась в том, что он был рассчитан строго на определенную конфигурацию аппаратных средств (т. е. запускался в конкретной системе) и впервые в истории кибернетических атак физически разрушал инфраструктуру (выводил из строя уранообогатительные центрифуги путем внезапных изменений скорости их вращения). Данный (или аналогичный) компьютерный червь потенциально может быть использован в качестве средства несанкционированного сбора данных (шпионажа) и диверсий в других АСУТП промышленных предприятий, электростанций, аэропортов. Существование такого пути внесения вредоносных программ требует того, чтобы организации устанавливали правила и реализовывали специальные процедуры по использованию внешних носителей информации и портативных устройств.

Негативное воздействие со стороны контрольно-проверочной аппаратуры. Контрольно-проверочная аппаратура подключается к системам, важным для безопасности АЭС, в процессе их испытаний, восстановления или технического обслуживания. Взаимодействуя с техническими средствами и программным обеспечением системы, данная аппаратура служит потенциальным источником (или путем распространения) вредоносного влияния на системы, важные для безопасности АЭС.

При взаимодействии контрольно-проверочной аппаратуры с ИУС АЭС необходимо исключить возможность искажения данных или ПО системы, а также возможность внесения вредоносных программ или данных в систему.

Контрольно-проверочная аппаратура может иметь в своем составе собственное ПО, которое должно контролироваться на предмет отсутствия в нем вредоносных функций, вирусов или программных закладок, способных оказать негативное влияние на ИУС, важные для безопасности АЭС.

Вредоносные действия, осуществляемые непосредственно персоналом АЭС или сторонних организаций. Такие действия могут быть как непреднамеренными, так и преднамеренными. В свою очередь, преднамеренные действия могут варьироваться от мелкого вредительства или саботажа отдельно взятого сотрудника до хорошо спланированной диверсии.

Если для выполнения работ по монтажу, наладке или ремонту ИУС АЭС привлекаются специалисты сторонних организаций, то их действия должны строго контролироваться во избежание нарушения ими конфиденциальности, целостности и пригодности технических средств, программного обеспечения и данных системы.

Искажение информации, поступающей от датчиков. Некорректная информация, поступающая от датчиков, может в конечном итоге привести к нарушению технологического процесса. Безусловно, внимание должно быть уделено проверке самих датчиков. Однако, кроме этого, нужно учитывать, что датчики, как правило, находятся на значительном удалении от центральной части ИУС (например, некоторые датчики АСРК расположены за пределами АЭС), и это упрощает возможность несанкционированного доступа к ним с целью повреждения или искажения передаваемой ими информации. Следовательно, необходимо предусматривать средства защиты и средства контроля за несанкционированным доступом к датчикам и средства проверки достоверности данных, получаемых от датчиков.

Некорректное обновление программного обеспечения ИУС АЭС. Нередко возникают ситуации, когда в процессе эксплуатации ИУС нужны доработка, модификация или обновление программного обеспечения. При этом существует риск внесения в систему вредоносного ПО или непреднамеренных ошибок. Известен инцидент, который произошел на энергоблоке № 2 АЭС «Хэтч» (Hatch) в штате Джорджия (США) и заключался в том, что реактор был аварийно остановлен на 48 ч после некорректного обновления ПО на одном компьютере. Компьютер использовался для наблюдения за химическими и диагностическими данными, получаемыми от основной системы управления. Программное обеспечение в компьютере было доработано с целью синхронизации хранимых в нем данных с данными в системе управления. При перезапуске компьютера после обновления ПО произошло удаление всех данных как в нем самом, так и в связанной с ним системе управления. В свою очередь, система безопасности интерпретировала отсутствие данных как потерю охлаждающей воды и в результате инициировала аварийный останов реактора.

В данном инциденте проявилось сразу несколько важных недостатков:

ошибка разработчика, который не предусмотрел возможность подобного развития событий;

неподготовленность техника, непосредственно осуществляющего обновление ПО, поскольку он не был осведомлен о влиянии данного ПО на работу других систем;

негативное влияние менее важной для безопасности системы на более важную;

некорректное проектирование обеих систем и реализация их ПО без учета принципов компьютерной безопасности.

Описанный случай наглядно демонстрирует, какие опасности может нести в себе модификация ПО в процессе эксплуатации ИУС и как ошибки в одной системе могут негативно влиять на работу других систем. При этом следует быть готовым к тому, что подобные угрозы могут носить не только непреднамеренный характер (как в рассмотренном примере), но и являться результатом умышленной вредоносной атаки.

Представленный перечень видов угроз не является абсолютно полным и может быть в дальнейшем расширен или уточнен. Однако выполненный анализ показывает основные возможные пути компьютерных атак, демонстрирует их разнообразие и позволяет оценить сложность защиты от всех возможных угроз.

Выводы

Обеспечение компьютерной безопасности ИУС АЭС, а также разработка соответствующей нормативной базы актуальны во многих странах, в том числе в Украине. С этой целью должно быть проведено всестороннее исследование разнообразных аспектов компьютерной безопасности. Первым шагом в данном направлении стало изучение возможных кибернетических угроз.

Проведенный анализ видов кибернетических угроз показывает, что обеспечение компьютерной безопасности — одна из сложных комплексных задач, при решении которой надо учитывать множество разнообразных факторов и различных видов компьютерных атак. Адекватные защитные меры должны охватывать все этапы жизненного цикла ИУС АЭС и предусматривать комплекс организационных, технических и программных средств защиты. Возможные способы защиты будут рассмотрены в последующих публикациях

Список использованной литературы

1. 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.

2. *IEC 61513*. Nuclear power plants — instrumentation and control important to safety — General requirements for systems. — Geneva : International Electrotechnical Commission, 2001.

3. *ГОСТ Р МЭК 61513*. Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования. — М. : Стандартинформ, 2012.

4. *ДСТУ IEC 61513:2009*. Атомні електростанції. Інформаційні та керуючі системи, важливі для безпеки. Загальні вимоги до систем (IEC 61513:2001, IDT). — К. : Держспоживстандарт України, 2014.

5. Fundamental safety principles : safety fundamentals. — Vienna : International Atomic Energy Agency, 2006. — (IAEA safety standards series, ISSN 1020–525X; No. SF-1). — ISBN 92–0–110706–4.

6. *НП 306.2.141–2008*. Загальні положення безпеки атомних станцій. — К. : Державний комітет ядерного регулювання України, 2008.

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

References

1. Computer Security at Nuclear Facilities: Reference Manual: Technical Guidance, IAEA, Vienna (2011).

2. *IEC 61513*, Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements for Systems, International Electrotechnical Commission, Geneva (2001).

3. *GOST IEC 61513***.** Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements [Atomnyie stantsii. Sistemy kontrolya i upravleniya, vazhnyie dlya bezopasnosti. Obschiie trebovaniia], Standartinform, Moscow (2012). (Rus)

4. *DSTU IEC 61513:2009***.** Nuclear Power Plants. Instrumentation and Control Systems Important to Safety. General Requirements for Systems [Atomnyie stantsii. Sistemy kontrolya i upravleniya, vazhnyie dlya bezopasnosti], Derzhspozhyvstandart, Kyiv (2014). (Ukr)

5. Fundamental Safety Principles: Safety Fundamentals, Safety Standards Series No. SF-1, IAEA, Vienna (2006).

6. *NP 306.2.141–2008*, General Safety Provisions for Nuclear Power Plants [Obschiie polozheniya bezopasnotsi atomnykh stantsii], Ofitsiinyi visnyk Ukrainy (2008), No. 9, 226 p. (Rus)

7. *M. Yastrebenetsky, V. Kharfchenko (eds.)*, Nuclear Power Plant Instrumentation and Control Systems for Safety and Security, IGI Global, Hershey, SA (2014), 450 p.

Получено 02.02.2015.