УДК 621.039:004.9

А. Л. Клевцов, А. А. Симонов, С. А. Трубчанинов

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

Компьютерная безопасность информационных и управляющих систем АЭС: категоризация

Рассмотрены уровни и зоны компьютерной безопасности, принятые в Международном агентстве по атомной энергии (МАГАТЭ). Описаны степени и зоны компьютерной безопасности, регламентированные стандартом Международной электротехнической комиссии (МЭК). Представлена категоризация систем по компьютерной безопасности, используемая Комиссией ядерного регулирования (КЯР) США. Проведен краткий анализ основных отличий в категоризациях систем по компьютерной безопасности, принятых МАГАТЭ, МЭК и КЯР США. Предложены подходы к категоризации, которые целесообразно применять в Украине при разработке нормативного документа по компьютерной безопасности ИУС АЭС.

Ключевые слова: компьютерная безопасность, информационная и управляющая система, категоризация, уровень, степень, зона.

О. Л. Клевцов, А. А. Симонов, С. О. Трубчанінов

Комп'ютерна безпека інформаційних та керуючих систем АЕС: категоризація

Розглянуто рівні та зони комп'ютерної безпеки, прийняті в Міжнародній агенції з атомної енергії (МАГАТЕ). Описано ступені та зони комп'ютерної безпеки, регламентовані стандартом Міжнародної електротехнічної комісії (МЕК). Представлено категоризацію систем з комп'ютерної безпеки, яка використовується Комісією ядерного регулювання (КЯР) США. Проведено стислий аналіз основних відмінностей у категоризаціях систем з комп'ютерної безпеки, прийнятих МАГАТЕ, МЕК та КЯР США. Запропоновано підходи до категоризації, які доцільно застосовувати в Україні, розробляючи нормативний документ з комп'ютерної безпеки ІКС АЕС.

Ключові слова: комп'ютерна безпека, інформаційна та керуюча система, категоризація, рівень, ступінь, зона.

Данная статья продолжает цикл публикаций [1, 2] по компьютерной безопасности ИУС АЭС в журнале «Ядерна та радіаційна безпека». Обзор нормативных документов МАГАТЭ, МЭК и КЯР США по компьютерной безопасности ядерных установок приведен в [2]. Требования, установленные в этих документах, зависят от принятой категоризации систем по компьютерной безопасности, но во всех случаях при их разработке использован дифференцированный подход к компьютерной безопасности — меры защиты применяются пропорционально потенциальным последствиям компьютерных атак. В частности, дифференцированный подход заключается в разбиении компьютерных систем на уровни/степени и зоны в зависимости от их значимости для безопасности. Для разных уровней/степеней и зон компьютерной безопасности применяются меры защиты различной жесткости (чем важнее система для безопасности, тем более строгая защита должна быть для нее обеспечена).

Категоризации систем по компьютерной безопасности, принятые в МАГАТЭ, МЭК и КЯР США, имеют как общие черты, так и определенные отличия. С учетом стоящей перед Государственным научно-техническим центром по ядерной и радиационной безопасности (ГНТЦ ЯРБ) задачей по разработке нормативного документа, касающегося компьютерной безопасности ИУС АЭС, необходимо провести анализ существующих категоризаций по компьютерной безопасности и предложить собственные подходы к такой категоризации.

Категоризация систем по компьютерной безопасности, принятая МАГАТЭ. Структура возможных уровней безопасности (security level) и связи этих уровней с соответствующими мерами обеспечения безопасности представлены в **NSS 17** [3]. В соответствии с указанным документом под уровнем безопасности понимается абстракция, определяющая степень защиты, требуемой для различных компьютерных систем (не только ИУС, непосредственно участвующих в процессе управления технологическими процессами, но также компьютерных систем физической безопасности, систем делопроизводства и др.) на ядерной установке (в том числе на АЭС). Основная цель введения уровней безопасности заключается в упрощении определения набора защитных мер для различных компьютерных систем на основе их категоризации (отнесения к определенному уровню).

Для каждого уровня нужно реализовать различный набор защитных мер, удовлетворяющих требованиям безопасности данного уровня. При этом часть защитных мер применяется ко всем системам на всех уровнях, а некоторые меры являются специфическими для определенного уровня.

Связь между критической важностью систем и применяемыми к ним мерами компьютерной безопасности показана на рис. 1. Должны быть предусмотрены защитные меры базового уровня, применяемые в отношении всех компьютерных систем. Кроме того, для каждого уровня компьютерной безопасности должны применяться специальные меры защиты: для уровня 5 необходима минимальная защита, а для уровня 1 — максимальная защита*. При этом некоторые защитные меры могут повторяться для нескольких уровней.

Отметим, что в [3] приведены *примерные* перечни базовых и дифференцированных (для разных уровней) защитных мер; точный выбор уровней и связанных с ними мер защиты следует делать в соответствии с конкретной

* Критерии отнесения систем к тому или иному уровню компьютерной безопасности в NSS 17 отсутствуют.

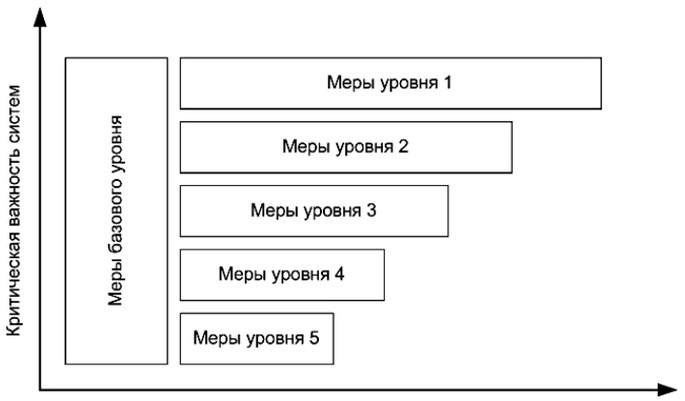

Рис. 1. Уровень физической безопасности/строгость мер

средой, спецификой установки и результатами анализа рисков компьютерной безопасности.

NSS 17 вводится понятие «зона компьютерной безопасности», которая представляет собой логическое и физическое понятие, позволяющее группировать компьютерные системы, имеющие одинаковую важность для безопасности, с целью обеспечения удобства административного управления, коммуникации и применения защитных мер.

Согласно [3], при применении зональной модели следует соблюдать следующие рекомендации:

каждая зона должна включать системы, имеющие одинаковую или сопоставимую важность для физической безопасности, а также для ядерной и радиационной безопасности установки;

по отношению к системам, относящимся к одной зоне, применяются аналогичные защитные меры;

компьютерные системы в пределах одной зоны образуют область надежной связи, не требующей применения дополнительных мер защиты;

на границах зон реализуются механизмы развязки потоков данных с целью предотвращения несанкционированного доступа и распространения ошибок из зоны с более низкими требованиями защиты в зону с более высокими требованиями.

Технические и административные меры, обеспечивающие разделение зон, должны учитывать требования защитных уровней. Не допускается прямой канал соединения, проходящий через несколько зон.

Поскольку зоны состоят из систем с одинаковой или сопоставимой значимостью, каждой зоне может быть присвоен уровень компьютерной безопасности, определяющий защитные меры по отношению к компьютерным системам в этой зоне.

Связь между зонами и уровнями не взаимно однозначна. Если для нескольких зон требуется одинаковая степень защиты, им может быть присвоен одинаковый уровень компьютерной безопасности. Зоны отражают логическое и физическое группирование компьютерных систем, в то время как уровни определяют степень требуемой защиты.

МАГАТЭ ведется разработка нового стандарта по компьютерной безопасности — **NST036** [4], который дополняет и уточняет некоторые положения NSS 17 [3].

В [4] отмечается, что уровни компьютерной безопасности и классы ядерной и радиационной безопасности являются разными, но связанными понятиями. Классификация по безопасности основана на влиянии функций (и их отказов) системы и ее компонентов на безопасность ядерной установки. Уровни компьютерной безопасности определяются на основании последствий отказов или неправильной работы системы и ее компонентов (включая несоответствие проектным требованиям к функционированию) вследствие кибернетических атак.

Согласно [4], меры ядерной и радиационной безопасности, с одной стороны, и меры компьютерной безопасности, с другой стороны, должны быть предусмотрены и реализованы таким образом, чтобы обеспечить взаимосвязь между этими двумя сферами и исключить возможность их взаимного негативного влияния друг на друга.

В NST036 указана необходимость учета возможности того, что множество компонентов могут подвергаться риску вследствие одной кибернетической атаки (например, различные каналы одной системы) или атака может быть направлена на разные цели и совмещать различные виды угроз. Это требует проведения специального анализа с целью оценки потенциальных последствий кибернетических атак для безопасности ядерной установки.

Согласно [4], должны быть идентифицированы компоненты систем, неправильная работа которых может влиять на безопасность или выполнение функций аварийного мониторинга. Уровни компьютерной безопасности устанавливаются в зависимости от значимости таких компонентов для безопасности ядерной установки.

Подчеркивается, что внедрение зон компьютерной безопасности для систем может привести к тому, что отдельным компонентам нужно будет присвоить более высокий уровень компьютерной безопасности, чем это предполагалось изначально. Например, коммуникатор не является компонентом, важным для безопасности, однако если коммуникатор обеспечивает связь между двумя комплектами аварийной защиты, он оказывается в той же зоне компьютерной безопасности, что и система аварийной защиты. Соответственно, коммуникатор должен быть отнесен к тому же уровню компьютерной безопасности, что и система аварийной защиты, поскольку существует потенциальная опасность его использования для нарушения работы одной из систем безопасности. В данном случае включение коммуникатора и системы аварийной защиты в одну зону компьютерной безопасности исключает необходимость реализации дополнительных мер безопасности в системе для защиты от потенциальных опасностей со стороны коммуникатора.

Категоризация систем по компьютерной безопасности, принятая в МЭК. В стандарте **IEC 62645** [5] введена категоризация по степеням компьютерной безопасности (security degree). Термин «степень компьютерной безопасности» аналогичен принятому МАГАТЭ термину «уровень компьютерной безопасности», но в настоящее время считается более корректным.

Степень компьютерной безопасности для ИУС АЭС определяется на основе анализа возможных максимальных последствий успешной кибернетической атаки на систему в части влияния на безопасность и/или производительность АЭС. Чем более опасны такие последствия, тем более высокая степень компьютерной безопасности устанавливается для системы.

Схема категоризации в [5] базируется на следующих принципах.

1. Последствия кибернетических атак, влияющие на безопасность АЭС, должны рассматриваться как более серьезные по сравнению с теми, которые влияют на производительность.

2. Системы АЭС должны рассматриваться с функциональной точки зрения. Нужно оценивать влияние на безопасность и/или производительность АЭС возможной кибернетической атаки по отношению к максимально чувствительной и значимой функции системы, вредоносное воздействие на которую может привести к наиболее серьезным последствиям.

3. Анализ конкретной системы должен учитывать возможность того, что другие ИУС АЭС (в том числе те, с которыми прямо или косвенно взаимодействует рассматриваемая система) могут быть объектом той же кибернетической атаки, что может существенно усложнять общую ситуацию.

IEC 62645 определяет три степени компьютерной безопасности: S1, S2 и S3. Отметим, что категоризация по компьютерной безопасности, согласно [5], касается только ИУС АЭС, непосредственно участвующих в управлении технологическими процессами, и не распространяется на другие компьютерные системы АЭС. В [5] установлена связь между степенями компьютерной безопасности и категориями функций, согласно IEC 61226 [6], выполняемых ИУС АЭС.

Степени компьютерной безопасности в [5] определяются для ИУС в соответствии со следующими критериями:

ИУС	Степень компьютерной безопасности
Выполняющие функции ядерной и радиационной безопасности категории А	S1
Необходимые для работы в режиме реального времени (без указания категории ядерной и радиационной безопасности); выполняющие функции ядерной и радиационной безопасности категории В	Не ниже S2
Выполняющие функции ядерной и радиационной безопасности категории С	S3 или выше, в зависимости от максимально опасных последствий
Отвечающие за эксплуатацию и техническое обслуживание АЭС	S3

Однозначное соответствие между степенью компьютерной безопасности и категорией функций, выполняемых ИУС АЭС, не требуется. Системе может быть назначена более высокая степень компьютерной безопасности, если максимальные последствия вредного воздействия на любую из выполняемых ею функций требуют принятия более жестких мер по обеспечению компьютерной безопасности.

Кроме того, в [5] указано, что при необходимости количество степеней компьютерной безопасности может быть увеличено для установления требований по компьютерной безопасности по отношению к другим компьютерным системам, не участвующим в управлении технологическими процессами.

По аналогии с подходом, принятым МАГАТЭ, в IEC 62645 также вводится понятие зон компьютерной безопасности с целью практической реализации дифференцированного подхода путем логического объединения систем с одинаковыми степенями компьютерной безопасности в группы для администрирования и реализации идентичных защитных мер. Критериями для определения зон компьютерной безопасности могут быть архитектура и физическое размещение систем, организация межсистемных интерфейсов, топология локальных сетей и т. д.

Согласно [5], применение зональной модели должно соответствовать следующим принципам:

1. Каждая зона включает системы, которые имеют одинаковую степень компьютерной безопасности. Если по архитектурным или другим причинам определенная ИУС АЭС имеет более низкую степень компьютерной безопасности, чем другие системы в конкретной зоне, ее степень повышается и приводится в соответствие с требованиями, предъявляемыми к степени компьютерной безопасности других систем этой зоны.

2. Дополнительные защитные барьеры между системами, принадлежащими к одной и той же зоне компьютерной безопасности, не требуются. Однако для межзональных интерфейсов барьеры могут быть эффективным средством защиты.

3. Сетевое оборудование (коммуникаторы, кабели и т. д.) размещается в той же зоне компьютерной безопасности, что и связанные с ним ИУС АЭС. Если сетевое оборудование используется для соединения систем, относящихся к разным зонам, реализуется соответствующее разделение этого сетевого оборудования на зоны и к нему предъявляются требования того же уровня компьютерной безопасности, что и к системам, входящим в соответствующую зону.

4. Обмен данными инициируется со стороны зоны, содержащей системы более высокой степени компьютерной безопасности, путем запроса к зоне, содержащей системы более низкой степени компьютерной безопасности.

5. Границы зон оборудуются техническими средствами для разделения потоков данных в соответствии с требованиями, предъявляемыми к степеням безопасности ИУС АЭС.

Взаимосвязь между зонами и степенями компьютерной безопасности не является однозначной. Например, в случае необходимости несколько зон могут иметь одинаковую степень компьютерной безопасности.

По аналогии с NSS 17 [3] в стандарте IEC 62645 [5] также описаны возможные меры защиты (общие для всех систем и дифференцированные по разным уровням компьютерной безопасности).

Категоризация систем по компьютерной безопасности, принятая КЯР США. Регулирующее руководство КЯР США **RG 5.71** [7] определяет требования к защитной архитектуре компьютерной безопасности.

Согласно [7], в общей стратегии компьютерной безопасности для ядерной установки должна применяться глубокоэшелонированная защита от кибернетических атак, направленных на критические цифровые ресурсы (системы, компьютеры и технические средства, значимые с точки зрения компьютерной безопасности). Стратегия глубокоэшелонированной защиты описывается в плане компьютерной безопасности. Одним из приемлемых методов реализации данной стратегии является использование защитной архитектуры, которая устанавливает формальные коммуникационные границы (или уровни компьютерной безопасности), в которых вводятся в действие защитные меры для выявления, предотвращения, задержки, смягчения и восстановления в случае кибернетических атак. Пример такой защитной архитектуры включает серию концентрических уровней безопасности, которые

корреспондируются с существующими на ядерной установке зонами физической защиты (например, внутренняя зона, защищенная зона, контролируемая зона, корпоративная зона, публичная зона).

Пример допустимой защитной архитектуры компьютерной безопасности, согласно [7], представлен на рис. 2. Уровни компьютерной безопасности разделяются защитными границами, например с использованием таких средств, как диоды и межсетевые экраны для контроля и защиты коммуникаций между уровнями. Системы, требующие более высокой степени обеспечения компьютерной безопасности, размещаются на более высоком уровне с большим количеством защитных барьеров. Логическая модель, представленная на рис. 2, не всегда должна прямо корреспондироваться с физическим размещением системы в той или иной зоне физической защиты. Например, система, отнесенная к уровню 3, может размещаться в зоне физической безопасности, соответствующей уровню 2, однако для этой системы должны обеспечиваться более строгие защитные меры (в части компьютерной безопасности), соответствующие установленному для нее уровню 3.

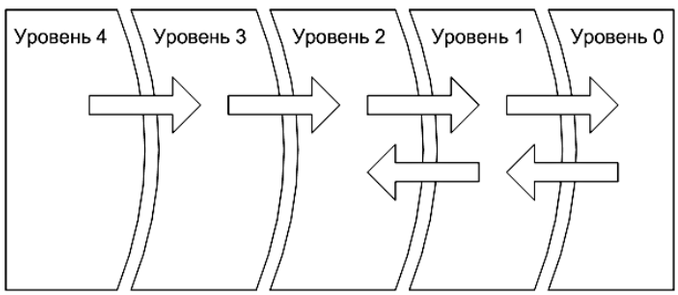

Рис. 2. Упрощенная архитектура компьютерной безопасности

Отметим, что, согласно RG 5.71, системы и технические средства, участвующие в выполнении функций, важных для безопасности или физической защиты ядерной установки, а также вспомогательные системы и оборудование, которые могут негативно повлиять на выполнение указанных функций, должны быть отнесены к наивысшему уровню компьютерной безопасности (т. е. к уровню 4) и надежно защищены от всех более низких уровней.

В RG 5.71 описаны основные принципы взаимодействия между системами, относящимися к различным уровням компьютерной безопасности (например, односторонняя передача информации от уровня 4 на уровень 3 и от уровня 3 на уровень 2), а также даны рекомендации по конфигурированию систем и защитных барьеров для обеспечения соответствующей степени защиты от компьютерных угроз.

Основные отличия существующих категоризаций. МАГАТЭ, МЭК и КЯР США, как видно из представленного анализа, придерживаются единой идеологии в части применения дифференцированного подхода к обеспечению компьютерной безопасности. В основе этого подхода лежит категоризация систем по компьютерной безопасности.

Несмотря на общность идеологии, существует целый ряд принципиальных различий в рассмотренных документах МАГАТЭ, МЭК и КЯР США:

1. *Принятая терминология.* МАГАТЭ и КЯР США используют термин «уровень компьютерной безопасности» (security level). МЭК применяет термин «степень компьютерной безопасности» (security degree), который, хотя и аналогичен термину «уровень компьютерной безопасности», считается более предпочтительным в настоящее время.

2. *Объект рассмотрения.* Объектом рассмотрения в документах МАГАТЭ NSS 17 [3], NST036 [4] и КЯР США RG 5.71 [7] являются любые компьютерные системы ядерных установок. МЭК в стандарте IEC 62645 [5] рассматривает только ИУС, непосредственно участвующие в управлении технологическими процессами на АЭС.

Отметим, что согласно МАГАТЭ и МЭК категории компьютерной безопасности устанавливаются непосредственно для каждой системы. КЯР США, согласно RG 5.71 [7], устанавливает уровни компьютерной безопасности не для систем, а для существующих зон физической защиты ядерной установки. В свою очередь, система, в зависимости от ее значимости, должна размещаться в той зоне, где будут обеспечены надлежащие меры защиты данной системы от кибернетических угроз.

3. *Количество и нумерация категорий.* МАГАТЭ в NSS 17 [3] описывает пять уровней компьютерной безопасности, пронумерованных от 1 до 5 (при этом системы уровня 1 имеют наибольшую значимость, а системы уровня 5 — наименьшую).

В стандарте IEC 62645 [5] рассматриваются три степени компьютерной безопасности: S1, S2, S3, связанные с классами безопасности ИУС АЭС (при этом системы уровня S1 имеют наибольшую значимость, а системы уровня S3 — наименьшую). Также предполагается возможность введения (при необходимости) дополнительных степеней компьютерной безопасности для категоризации компьютерных систем, не участвующих в управлении технологическими процессами на АЭС.

В документе КЯР США RG 5.71 [7] рассматриваются пять защитных уровней компьютерной безопасности, пронумерованных от 0 до 4 (при этом системы уровня 4 имеют наибольшую значимость, а системы уровня 0 — наименьшую, т. е. нумерация уровней по значимости обратна по отношению к принятой в МАГАТЭ).

4. *Описание принципов категоризации и мер защиты.* В NSS 17 [3] имеется обобщенное (но недостаточно строгое) описание принципов категоризации систем по уровням компьютерной безопасности. Подробно рассмотрены возможные меры защиты (общие и дифференцированные по уровням компьютерной безопасности) систем от кибернетических угроз.

В IEC 62645 [5] четко регламентированы критерии установления степени компьютерной безопасности для ИУС АЭС, а также описаны меры защиты (общие и дифференцированные по уровням компьютерной безопасности).

В NSS 17 [3] и IEC 62645 [5] предложено применение зон компьютерной безопасности с целью упрощения административного управления, коммуникации и реализации защитных мер по отношению к системам, имеющим сопоставимую значимость для безопасности.

В документе КЯР США RG 5.71 [7] указано, что основным принципом установления уровней компьютерной безопасности является их привязка к существующим зонам физической защиты. Меры защиты для разных уровней не описаны. Рассмотрены правила взаимодействия между системами разного уровня компьютерной безопасности. Понятие «зона компьютерной безопасности» не применяется, однако сам принцип определения уровней компьютерной безопасности фактически базируется на зональном принципе.

Предложения по категоризации ИУС АЭС по компьютерной безопасности в Украине. ГНТЦ ЯРБ в настоящее время начал подготовку к разработке нормативного документа по компьютерной безопасности ИУС АЭС. Одной из наиболее важных задач является определение в нем принципов категоризации ИУС АЭС по компьютерной безопасности и дифференцирование требований в зависимости от установленной категории.

Проведенный анализ различных принципов категоризации систем по компьютерной безопасности позволил выявить их особенности и различия. По результатам анализа предлагается при разработке нормативного документа взять за основу категоризацию, принятую в МЭК, как наиболее приемлемую для потребностей Украины*:

в МЭК рассматривается тот же объект для обеспечения компьютерной безопасности, что и в разрабатываемом нормативном документе (т. е. ИУС АЭС, а не все компьютерные системы ядерной установки);

степени компьютерной безопасности в документе МЭК привязаны к категориям функций ИУС АЭС, что дает возможность гармонизировать их с действующим НП 306.2.202–2015 [8], в котором установлены классы безопасности ИУС АЭС с использованием аналогичных категорий функций;

в МЭК применен более современный термин «степень компьютерной безопасности».

Исходя из сказанного, в новом нормативном документе Украины по компьютерной безопасности ИУС АЭС предлагается применить следующую категоризацию:

для ИУС класса безопасности 2(А) согласно НП 306.2.202–2015 [8] устанавливается степень компьютерной безопасности К1;

для ИУС класса безопасности 3(В) согласно [8] и ИУС классов безопасности 3(С), 4, необходимых для работы энергоблока АЭС в режиме реального времени, устанавливается степень компьютерной безопасности К2 или выше;

для ИУС класса безопасности 3(С) согласно [8] устанавливается степень компьютерной безопасности К3 или выше;

для ИУС класса безопасности 4 согласно [8], участвующих в выполнении вспомогательных функций при эксплуатации и техническом обслуживании, устанавливается степень компьютерной безопасности К3.

В процессе разработки и согласования нормативного документа указанная классификация может быть уточнена. Также в разрабатываемом ГНТЦ ЯРБ нормативном документе целесообразно предусмотреть применение зонального принципа и регламентировать требования к определению зон компьютерной безопасности, основываясь на положениях NSS 17 [3] и IEC 62645 [5].

Выводы

В статье рассмотрены принципы категоризации ИУС АЭС по компьютерной безопасности в соответствии с документами МАГАТЭ, МЭК и КЯР США. Проанализированы подходы к формированию уровней/степеней и зон компьютерной безопасности.

По результатам анализа можно констатировать, что определение уровней/степеней и зон является основой для применения дифференциального подхода в обеспечении компьютерной безопасности компьютерных систем ядерной установки разной степени их значимости с точки зрения возможных последствий кибернетических атак на безопасность и работоспособность установки в целом.

Анализ отличий в подходах МАГАТЭ, МЭК и КЯР США к определению уровней/степеней и зон компьютерной безопасности свидетельствует о том, что при разработке в Украине нормативного документа по компьютерной безопасности ИУС АЭС целесообразно в качестве базовой принять категоризацию МЭК, которую необходимо гармонизировать с классами безопасности ИУС АЭС, принятыми в Украине.

Даны конкретные предложения по категоризации ИУС АЭС по компьютерной безопасности.

* При этом категории компьютерной безопасности должны быть гармонизированы с классификацией по ядерной и радиационной безопасности, принятой в Украине.

Список использованной литературы

1. *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.

2. *Клевцов А. Л.* Компьютерная безопасность информационных и управляющих систем АЭС: нормативная база / А. Л. Клевцов, М. А. Ястребенецкий, С. А. Трубчанинов // Ядерна та радіаційна безпека. — 2015. — № 4 (68). — С. 51—57.

3. 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.

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

5. *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).

6. *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).

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

8. *НП 306.2.202–2015.* Вимоги з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій. — К. : Державна інспекція ядерного регулювання України, 2015. — 97 с.

References

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

2. *Klevtsov, A.L., Yastrebenetsky, M.A., Trubchaninov, S.A.* (2015), “Computer Security of NPP Instrumentation and Control Systems: Regulatory Framework” [Kompiuternaia bezopasnost informatsionnykh i upravliaiushchikh sistem AES: normativnaia baza], Nuclear and Radiation Safety, No. 4 (68), pp. 51-57.

3. IAEA Nuclear Security Series, No. 17 (2011), Computer Security at Nuclear Facilities: Reference Manual: Technical Guidance, International Atomic Energy Agency, Vienna, 88 p.

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

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

6. *IEC 61226* (2009), Nuclear Power Plants − Instrumentation and Control Important to Safety, Classification of Instrumentation and Control Functions, International Electrotechnical Commission, Geneva, 64 p.

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

8. *NP 306.2.202* (2015), "Requirements for Nuclear and Radiation Safety of Instrumentation and Control Systems, Important for Safety of Nuclear Power Plants" [Vymohy z yadernoi ta radiatsiynoi bezpeky do informatsiynykh ta keruiuchykh system, vazhlyvykh dlia bezpeky atomnykh stantsii], State Nuclear Regulatory Inspectorate of Ukraine, Kyiv, 97 p. (Ukr)

Получено 19.09.2016.