УДК 621.039

К ВОПРОСУ ОБ ИНТЕРФЕЙСЕ ФИЗИЧЕСКОЙ И КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Крупчатников Б. Н. (krupchatnikov@secnrs.ru), Сазонов А. Д., к.т.н. (sazonov@secnrs.ru),
Гареев М. Д., к.т.н. (gareev@secnrs.ru) (ФБУ «НТЦ ЯРБ»)

Рассматриваются основные направления, по которым формируется регулирование компьютерной безопасности, отраженные в документах МАГАТЭ, Комиссии по ядерному регулированию США и Ростехнадзора. Предлагаются некоторые рекомендации по совершенствованию российской нормативной базы в этой области путем разработки новых федеральных норм и правил или внесения дополнений в действующие, а также рекомендации относительно документов, регламентирующих экспертизу безопасности, осуществление надзора, и руководств по безопасности; рекомендации по организации межведомственного взаимодействия.

Подчеркивается необходимость следовать общей идеологии построения физической ядерной безопасности, предусматривающей формирование проектной угрозы с оценкой возможных нежелательных последствий радиационного воздействия, а также проведение оценки эффективности системы физической ядерной безопасности в целом и ее подсистем.

► ***Ключевые слова:*** *компьютерная безопасность, физическая ядерная безопасность, регулирование безопасности, атомная энергия, угроза, кибератака.*

ON THE ISSUE OF NUCLEAR SECURITY AND COMPUTER SECURITY INTERFACE

Krupchatnikov B., Sazonov A., Ph. D., Gareev M., Ph. D.
(SEC NRS)

The main directions of computer security regulation, reflected in the documents of the IAEA, the U.S. Nuclear Regulatory Commission and Rostekhnadzor, are considered. Some recommendations are proposed to improve the Russian regulatory framework in this area by developing new Federal rules and norms or making additions to existing ones, as well as recommendations on documents regulating safety expertise, supervision and nuclear security guidelines and recommendations on the organization of interdepartmental cooperation.

The need to follow the general ideology of building nuclear security, providing for the construction of a design basis threat with an assessment of the possible adverse effects of radiation exposure, as well as the assessment of the effectiveness of the nuclear security system as a whole and its subsystems.

► ***Key words:*** *computer security, nuclear security, safety regulation, nuclear energy, threat, cyber attack.*

Зарубежный опыт и, в первую очередь, рекомендации, содержащиеся в документах МАГАТЭ, ясно демонстрируют все возрастающее внимание к вопросам компьютерной безопасности в области использования атомной энергии, при этом компьютерная безопасность рассматривается как составная часть физической ядерной безопасности. В техническом руководстве МАГАТЭ по компьютерной безопасности для промышленных систем управления на ядерных установках [1] отмечается, что применение компьютерных мер безопасности в контексте физической ядерной безопасности направлено на защиту таких промышленных систем управления, которые обеспечивают защиту, безопасность и вспомогательные функции на ядерных установках. При этом под системами управления защитой и безопасностью понимаются системы физической защиты, учета и контроля ядерных материалов. В соответствии с публикацией [2] регулирующие требования в области безопасности при использовании атомной энергии должны учитывать актуальное законодательство в сфере компьютерной безопасности и, желательно, чтобы регулирующие органы сотрудничали таким образом, чтобы в требованиях по компьютерной безопасности отражалась специфика физической ядерной безопасности.

В приложении к сегодняшней нормативной российской практике указанные положения документов МАГАТЭ можно считать ориентиром, указывающим на то, что независимым образом уставленные требования ядерного регулятора по вопросам физической безопасности и требования регулятора по вопросам компьютерной безопасности сбалансировано решают основную задачу – снижение риска радиационного воздействия, возникающего в результате возможного злонамеренного действия. Существующее законодательство непосредственно не устанавливает требований к организации взаимодействия регулятора в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, которым является Федеральная служба таможенного и экспортного контроля, и Ростехнадзора – уполномоченного органа государственного регулирования безопасности при использования атомной энергии. Вопросы, связанные с компьютерной безопасностью в атомной отрасли, подлежат регулированию в той мере, в какой они оказывают влияние на физическую и эксплуатационную безопасность объектов использования атомной энергии.

Показателен пример организации процесса регулирования кибербезопасности Комиссией по ядерному регулированию США (Nuclear Regulatory Commission – NRC). После событий, произошедших 11 сентября 2001 г., NRC издала ряд рекомендаций и распоряжений, требующих от атомных электростанций принятия мер, включая усиление защиты компьютерных систем. В октябре 2006 г. специалисты NRC приступили к разработке правил безопасности для энергетических реакторов. Правила кибербезопасности первоначально были изданы как подраздел нормативного документа 10 CFR [1] 73.55 «Требования к физической защите против радиологического саботажа для ядерных энергетических реакторов». Однако в дальнейшем было принято решение выпустить правила кибербезопасности в качестве отдельного раздела 10 CFR 73.54 для того, чтобы обеспечить возможность применения требований кибербезопасности к другим типам лицензируемых установок и видам деятельности в последующих нормативных актах.

В марте 2009 г. NRC выпустила раздел в составе 10 CFR 73.54 с требованием к лицензиатам и заявителям «обеспечить высокую степень уверенности в том, что цифровые компьютерные и коммуникационные системы и сети, связанные с безопасностью, охраной и обеспечением готовности к чрезвычайным ситуациям, защищены от кибератак». Результатом разработки соответствующего руководства по выполнению требования 10 CFR 73.54 стала публикация руководства [3]. Этот документ был разработан для атомных электростанций и основан на стандартах и документах, отражающих практику обеспечения кибербезопасности, опубликованных Национальным институтом стандартов и технологий, Министерством национальной безопасности США, Институтом инженеров по электротехнике и электронике и Международным обществом автоматизации. Он также содержит общий шаблон, который лицензиаты могут использовать в качестве руководства при разработке своих планов кибербезопасности, и построен таким образом, чтобы будущие изменения могли быть адаптированы для использования другими категориями лицензиатов и объектов. Институт ядерной энергии (Nuclear Energy Institute – NEI) независимо разработал документ «План кибербезопасности ядерных энергетических реакторов» (NEI 08-09) [4]. NRC сочла возможным использование [4] в промышленности в соответствии с требованиями,

[1] 10 CFR XX.XX – Коды Федерального регулирования Комиссии по ядерному регулированию США.

изложенными в 10 CFR 73.54. Этот документ предоставляет еще один шаблон, который атомные электростанции могут использовать при представлении планов обеспечения кибербезопасности (Cyber Security Plans – CSP) в NRC для последующего рассмотрения и утверждения CSP [4]. Следующим шагом NRC было принятие «дорожной карты» кибербезопасности в целях регулирования по четырем категориям лицензируемых NRC объектов и видов деятельности: топливный цикл, исследовательские реакторы, пункты хранения отработавшего топлива и изотопной продукции, транспортирование.

В работе [5] указываются основные этапы программы работ по обеспечению кибербезопасности в период с 2002 по 2017 гг.:

- 2002 – 2003 гг.: NRC включала впервые требования по кибербезопасности в документы по физической безопасности и в проектную угрозу;
- 2005 г.: NRC выпустила в поддержку промышленности программу внедрения кибербезопасности на добровольном основании (Cyber security program for operating reactors – NEI 04-04);
- 2009 г.: введены правила кибербезопасности в 10 CFR 73.54;
- 2012 г.: реализация/контроль за исполнением промежуточных этапов по обеспечению кибербезопасности;
- 2013 – 2015 гг.: проверка выполнения мероприятий, предусмотренных этапов дорожной карты;
- 2015 г.: требования по уведомлению о событиях кибербезопасности введены в 10 CFR 73.77;
- 2017 г.: полномасштабная реализация программ кибербезопасности.

Как отмечается в [4], большое внимание в рамках программы уделялось организации межведомственного взаимодействия, в том числе проведению под эгидой NRC совещаний с участием таких организаций, как Комиссия по регулированию в энергетике, Федеральная торговая комиссия, Министерство национальной безопасности, Береговая Охрана США, Министерство транспорта, Федеральная авиационная администрация, Министерство финансов, Национальная ассоциация страховых комиссаров, Министерство торговли, Национальный институт стандартов и технологий, а также подписанию соглашений с Федеральной комиссией по регулированию в энергетике (FERC) и Североамериканской корпорацией по надежному электроснабжению (NERC).

Состоянию дел с кибербезопасностью в нашей стране в контексте физической ядерной безопасности посвящена работа [6], где рассматриваются вопросы интерфейса физической ядерной безопасности и кибербезопасности и показано, что в отличие от того, как МАГАТЭ использует понятие интерфейса в отношении пары «эксплуатационная безопасность – физическая ядерная безопасность», полагая, что компьютерная безопасность является неотъемлемой частью «института» физической ядерной безопасности, в российской нормативной практике – это вопрос об интерфейсе компьютерной безопасности и «физической составляющей» физической ядерной безопасности (физической защиты и учета и контроля) [2].

За время, прошедшее с момента выхода публикации [6], нормативная база в сфере безопасности критической информационной инфраструктуры была дополнена рядом нормативных документов, относящихся к области действия закона «О безопасности критической информационной инфраструктуры Российской Федерации» [7], содержащих как технические, так и организационные требования, и положений [8 – 14] и обрела определенную завершенность.

При этом в ситуации, когда требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры и требования к созданию систем физической ядерной безопасности устанавливаются различными органами, независимо друг от друга, а также проверка их выполнения предусмотрена независимым образом, важным является вопрос, не возникает ли пробелов в регулирующих воздействиях и, соответственно, пробелов на стыках каждой из указанных систем безопасности. Те функции безопасности, которые в терминологии МАГАТЭ присущи системе физической ядерной безопасности, у нас распределены по ряду условно независимых систем [15]:

- учета и контроля ядерных материалов, радиоактивных веществ и радиоактивных отходов;
- физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов;
- защиты чувствительной информации о ядерных и радиационных объектах, ядерных материалах, радиоактивных веществах и радиоактивных отходах, связанной с системами учета и контроля и физической защиты;

[2] Следует отметить, что понятие «физическая ядерная безопасность» не имеет юридической силы в наших нормативных документах и используется по мере необходимости в документах, касающихся аспектов международного сотрудничества.

- противодействия ядерному терроризму;
- компьютерной безопасности и защиты информации, связанных с системами эксплуатационной безопасности.

В соответствии с существующими правилами организации указанных систем, которые, как правило, действуют на федеральном, ведомственном или региональном уровне, на объектах создаются соответствующие объектовые системы безопасности.

Физическая ядерная безопасность и физическая защита близки по сути, но имеется различие, которое состоит в том, что физическая защита не предназначена непосредственно для противодействия киберугрозе, более того, она сама может являться потенциальной целью кибератаки.

В соответствии с установившейся и закрепленной в нормативных документах практикой построения системы физической защиты, администрацией объекта должны быть приняты меры, предусматривающие:

- предупреждение (сдерживание);
- своевременное обнаружение;
- затруднение и замедление продвижения к цели;
- нейтрализацию угрозы и устранение последствий.

Указанные меры должны быть действенными в отношении таких сценариев, когда возможны совместные согласованные действия внешнего «физического» нарушителя, кибератакующего из внешнего киберпространства, внутреннего «физического» нарушителя и внутреннего кибернарушителя (рис. 1).

Все комбинации из вариантов возможных совместных действий показывают, что «физические» (находящиеся в сфере физической защиты) и компьютерные (находящиеся в сфере компьютерной безопасности) нарушители составляют комбинации по три составляющих в каждой (1, 2, 12) и (34, 3, 4) соответственно. Остальные 12 возможных вариантов – «гибридная» угроза. Это простое сопоставление указывает на необходимость комплексного подхода к формированию регулирующих механизмов в отношении проектной угрозы.

Универсальным методом совокупной оценки действенности системы физической защиты является оценка риска с учетом смягчающих факторов, которая выражается уравнением [16, 17]:

$$R=F(1-E)\cdot C,$$

где:

R – величина, характеризующая риск события, связанного с действиями нарушителя; может быть выражена величиной финансового ущерба или неким иным, в том числе условным, показателем;

F – ожидаемая частота события;

E – эффективность системы физической защиты;

C – величина, характеризующая последствия события.

Обычно полагается, что событие обязательно произойдёт, то есть F=1. В работе [16] эффективность представлена как $E=P_{об}\cdot P_{бс}$, где $P_{об}$ и $P_{бс}$ – вероятность обнаружения нарушителя и вероятность благоприятного исхода боестолкновения соответственно. В работе [18] предлагается ввести коэффициент, учитывающий фактор сдерживания $F_{сд}$, тогда выражение принимает вид $R=F_{сд}(1-P_{об}\cdot P_{бс})\cdot C$.

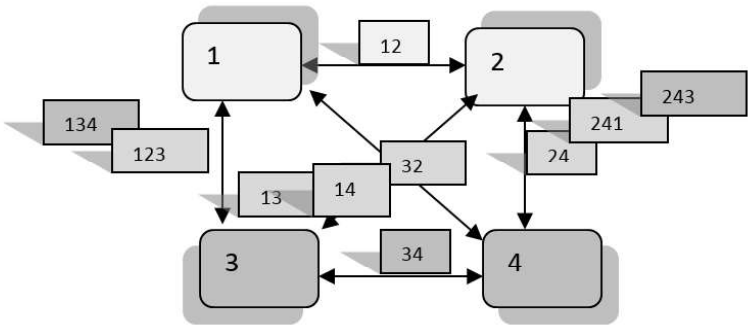

Рис. 1. Условное изображение взаимодействующих «типов» нарушителя:
1, 2 – внешний и внутренний «физический» нарушитель;
3, 4 – внешний и внутренний кибернарушитель

Исходя из того, что можно допустить наличие как независимых от кибератак актов диверсии или хищения, так и комбинированной «гибридной» угрозы таких событий и кибератак в «чистом» виде, приводящих к радиационным последствиям, можно записать выражение для риска следующим образом:

$$R=R_{фн}+R_{гн}+R_{ка}=(F_{сд}(1-P_{об}\cdot P_{бс}))_{фн}\cdot C+(F_{сд}(1-P_{об}\cdot P_{бс}))_{гн}\cdot C+(1-P_{об}\cdot P_{нейтр})_{кибер}\cdot C_{кибер},$$

где:

C – характеристика последствий от событий, связанных с «физическим» и «гибридным» нарушителем (полагаем их одинаковыми);

$C_{кибер}$ – характеристика последствий от событий, связанных с кибернарушителем;

$P_{нейтр}$ – вероятность нейтрализации кибератаки.

Данное выражение не следует рассматривать как рекомендуемое непосредственно для проведения расчетных оценок. Цель авторов – продемонстрировать тесную взаимосвязь аспектов безопасности и необходимость реализации на практике одного из принципов физической ядерной безопасности – адаптивность систем физической безопасности, а также показать необходимость совершенствования механизмов регулирования в этой области в направлении повышения достоверности и надежности решений, принимаемых органом регулирования безопасности. Это относится ко всем этапам регулирующего процесса, начиная с установления требований к осуществлению стратегии физической безопасности в нормах и правилах и заканчивая процессом надзора, о чем сказано далее. В Заявлении о политике в области качества [19] отмечается, что для обеспечения всесторонней оценки ядерной и радиационной безопасности блоков АС, а также для повышения эффективности ее регулирования следует использовать риск- информативные методы, основанные на совместном использовании детерминистических и вероятностных методов оценки безопасности. В области физической безопасности предстоит сделать многое для развития инструментов риск-ориентированного подхода в практической плоскости.

Развитие технологий позволяет предположить, что диверсия в отношении ядерно- и радиационно опасных объектов, в результате которой возможно неблагоприятное радиационное воздействие на людей и окружающую среду, а также хищения ядерных материалов и радиоактивных веществ с намерением изготовить ядерное взрывное устройство или «грязную» бомбу могут быть реализованы не только совместными действиями «физических» нарушителей и кибернарушителей, но в определенных условиях могут быть последствиями кибератак в чистом виде. Это делает необходимым учет кибератаки при оценке угрозы для ядерно- и радиационно опасных объектов на государственном уровне и, соответственно, учет ее в проектной угрозе каждого конкретного ядерно- и радиационно опасного объекта еще и потому, что система физической защиты не является инструментом противодействия компьютерной атаке до тех пор, пока та не включена в проектную угрозу.

Уполномоченный орган регулирования безопасности при использовании атомной энергии должен обеспечить выдачу на основаниях, убедительно подтверждающих, что лицензиат или заявитель приняли все необходимые меры для обеспечения безопасности объекта или вида деятельности. На практике для того, чтобы получить такие убедительные основания, регулятор, прежде всего, должен сформулировать требования к построению проектной угрозы в соответствии с существующими реалиями, обязав лицензиата продемонстрировать, что им учтены все значимые типы угроз и модели нарушителей. Эти требования должны быть сформулированы таким образом, чтобы положения документа федерального уровня, устанавливающего перечень основных угроз и моделей нарушителей, были основой, но не ограничителем в отношении проектной угрозы для объекта и не только давали возможность, но и обязывали адаптировать проектную угрозу к быстроизменяющейся в связи с развитием технологий среде угроз. При этом необходимо актуализировать перечень основных угроз и моделей нарушителей, зафиксированных в документе федерального уровня, и придать этому перечню большую универсальность. Наличие самостоятельной системы регулирования компьютерной безопасности, независимой от системы регулирования физической безопасности, в принципе, может обеспечить комплексность и завершенность системы регулирования безопасности, но убедиться в этом нельзя до тех пор, пока ядерный регулятор не проанализирует достаточность всего комплекса мер в целом.

В таблице отражен процесс создания системы безопасности объекта в отношении существующих угроз противоправных действий.

Основные этапы создания системы безопасности

Наименование этапа	Физическая безопасность	Компьютерная безопасность	Физическая безопасность и компьютерная безопасность
Описание объекта	Ядерные материалы. Радиоактивные вещества. Оборудование и системы, важные для эксплуатационной безопасности	Автоматизированные системы управления. Информационные системы	Базы данных, связанные с учетом и контролем. Информация, связанная с системой физической защиты
Построение проектной угрозы, типы нарушителей, возможные сценарии их действий	Внешний нарушитель. Внутренний нарушитель	Киберугроза из внешнего пространства (хакеры). Киберугроза из внутреннего пространства	Комбинации действий нарушителей различных типов
Анализ возможных последствий реализации угроз и оценка их масштабов	Хищение ядерных материалов с намерением изготовить самодельное ядерное взрывное устройство. Хищение с намерением изготовить «грязную бомбу» или иное устройство для радиоактивного загрязнения местности. Диверсия в отношении объекта с радиационными последствиями	Компьютерная атака в отношении автоматизированных систем управления и информационных систем, приводящая к нарушениям в работе объекта без радиационных последствий	Нарушения в работе автоматизированных систем управления и информационных систем, приводящие к радиационным последствиям
Определение имущества и цифровых активов, подлежащих защите на объекте	Предметы физической защиты и их категории опасности с целью размещения в соответствующих защищенных зонах		
Состав систем безопасности на объекте	Системы физической защиты с функциями: • сдерживания • обнаружения • затруднения продвижения • нейтрализации • ликвидации последствий. Системы учета и контроля с функциями: • создания, поддержания в актуальном состоянии данных о фактическом наличии и перемещении ядерных материалов и радиоактивных веществ • обеспечения непрерывного контроля со стороны уполномоченного персонала, исключающего бесконтрольное изъятие, перемещение и обращение с ядерными материалами и радиоактивными веществами	Системы защиты	Защита чувствительной информации, связанной с физической безопасностью. Меры контроля физического доступа к оборудованию, влияющему на компьютерную безопасность

Наименование этапа	Физическая безопасность	Компьютерная безопасность	Физическая безопасность и компьютерная безопасность
	• предоставления информации о наличии и перемещениях ядерных материалов и радиоактивных веществ уполномоченным организациям • расследования аномалий и иных событий, связанных с возможным несанкционированным использованием ядерных материалов и радиоактивных веществ и утерей регулирующего контроля		
Оценка эффективности систем безопасности	Системы ФЗ	Системы защиты	

Не учтенные риски, связанные с возможностью компьютерной атаки, снижают достоверность оценок уровня защищенности, в том числе антитеррористической защищенности объектов использования атомной энергии, в связи с чем необходима актуализация всех механизмов регулирования.

Выводы

В связи с изложенным представляются актуальными следующие меры, направленные на совершенствование механизмов регулирования безопасности объектов использования атомной энергии с учетом аспектов компьютерной безопасности.

1. Провести актуализацию содержания документа федерального уровня, устанавливающего перечень основных угроз и моделей нарушителей в отношении ядерно- и радиационно опасных объектов, с учетом возможной угрозы компьютерной атаки.

2. Ввести дополнения в нормы и правила с целью конкретизации требований по следующим вопросам:

- формирование объектовой проектной угрозы;
- анализ уязвимости и оценка эффективности, установление рамочных требований к соответствующим методикам.

3. Разработать или актуализировать набор методических рекомендаций для развития указанных в п. 2 позиций, включая практические аспекты применения риск-ориентированного подхода и реализацию принципа глубокоэшелонированной защиты с учетом фактора киберугрозы.

4. Конкретизировать требования к содержанию документов, обосновывающих физическую безопасность, и усовершенствовать методы проведения экспертизы, включая независимые оценки заявленных показателей эффективности соответствующих систем физической безопасности.

5. Принять практические меры по организации межведомственного взаимодействия с целью устранения пробелов в сфере регулирования вопросов, связанных с устойчивостью объектов к противоправным действиям, с возможными радиологическими последствиями, имея в виду, в том числе, сопряжение нормативной базы и надзорных процедур по вопросам физической безопасности и компьютерной безопасности.

Список литературы

1. Компьютерная безопасность для промышленных систем управления на ядерных установках. Серия изданий МАГАТЭ по ядерной физической безопасности, № 33-Т. Техническое руководство. Международное агентство по атомной энергии, Вена, 2018.

2. Компьютерная безопасность на ядерных установках. Серия изданий МАГАТЭ по физической ядерной безопасности, № 17. Технические руководящие материалы. Международное агентство по атомной энергии, Вена, 2012.

3. U.S. NUCLEAR REGULATORY COMMISSION. January 2010. REGULATORY GUIDE 5.71. CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES.

4. Status of NRC Licensees' Implementation of Cyber Security Plans NRC/FERC Joint Commission Meeting, February 23, 2017.

5. NRC Cyber Security Regulatory Overview. James Beardsley State Liaison Officers Conference, September 26, 2017 Rockville, Maryland.

6. Киберугрозы и физическая ядерная безопасность. О. Михайлова// Индекс безопасности, 1(116), т. 22, 2016.

7. О безопасности критической информационной инфраструктуры Российской Федерации: Федер. закон от 26.07.2017 № 187-ФЗ.

8. Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Постановление Правительства РФ от 17.02.2018 № 162.

9. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений. Постановление Правительства РФ от 08.02.2018 № 127.

10. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31.

11. Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации. Утвержден приказом ФСТЭК России от 06.12.2017 № 227.

12. Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования. Утверждены приказом ФСТЭК России от 21 декабря 2017 г. № 235.

13. Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Приказ ФСТЭК России от 22 декабря 2017 г. № 236.

14. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации (в редакции приказа ФСТЭК России от 9 августа 2018 г. № 138).

15. Основы государственной политики в области обеспечения ядерной и радиационной безопасности Российской Федерации на период до 2025 года. Утверждены указом президента Российской Федерации 13 октября 2018 г. № 585.

16. SANDIA REPORT SAND2007-5591 Unlimited Release. Printed September 2007. Nuclear Power Plant Security. Assessment Technical Manual D. W. Whitehead C. S. Potter S. L. O`Connor.

17. Крупчатников Б. Н. О некоторых особенностях регулирования физической ядерной безопасности. Ядерная и радиационная безопасность, № 3(61), 2011.

18. FATHI ELSISI Sanctions as a Legal Deterrence Mean in the National Physical Protection Regime (CN -254-76). International Conference on Physical Protection of Nuclear Material and Nuclear Facilities 13 – 17 November 2017, Session II: Physical Protection Regime.

19. Заявление о политике в области качества государственного регулирования безопасности при использовании атомной энергии. Официальный сайт Федеральной службы по экологическому, технологическому и атомному надзору (gosnadzor.ru).

References

1. Computer Security of Instrumentation and Control Systems at Nuclear Facilities. IAEA Nuclear Security Series, № 33-T. Technical Guidance. International Atomic Energy Agency, Vienna, 2018.

2. Computer Security at Nuclear Facilities. IAEA Nuclear Security Series, № 17. Technical Guidance. International Atomic Energy Agency, Vienna, 2012.

3. U.S. Nuclear Regulatory Commission. January 2010. Regulatory Guide 5.71. Cyber Security Programs for Nuclear Facilities.

4. Status of NRC Licensees' Implementation of Cyber Security Plans NRC/FERC Joint Commission Meeting, February 23, 2017.

5. NRC Cyber Security Regulatory Overview. James Beardsley State Liaison Officers Conference, September 26, 2017 Rockville, Maryland.

6. Cyber Threats and Nuclear Security. O. Mikhailova// Index bezopastnosti, 1(116), т. 22, 2016.

7. On the Security of Critical Information Infrastructure of the Russian Federation. Federal Law № 187-FZ of 26.07.2017.

8. On Endorsement of the Rules for State Control in the Field of Security Assurance at Significant Facilities of Critical Information Infrastructure of the Russian Federation. RF Government Resolution № 162 of 17.02.2018.

9. On Endorsement of the Rules for Categorizing Facilities of Critical Information Infrastructure of the Russian Federation, and of the List of Significance Criterion Indicators for Facilities of Critical Information Infrastructure of the Russian Federation and of Indicator Values. RF Government Resolution 08.02.2018 № 127.

10. Information Protection Requirements for Computerised Systems Controlling Production and Technological Processes at Critical Facilities, Potentially Hazardous Facilities, and Facilities of Greater Risk for the Life and Health of Humans and for the Environment. Endorsed by FSTEC of Russia Order № 31 of March 14, 2014.

11. Register Maintenance Procedure for Significant Facilities of Critical Information Infrastructure of the Russian Federation. Endorsed by FSTEC of Russia Order № 227 of 06.12.2017.

12. Requirements for Arrangement of Security Systems at Significant Facilities of Critical Information Infrastructure of the Russian Federation, and for Provision of their Functioning. Endorsed by FSTEC of Russia Order № 235 of December 21, 2017.

13. On Endorsement of the Template for Reporting Significance Category Assigned to Critical Information Infrastructure Facility, or Reporting Lack of Necessity to Assign any such Category to the Facility. FSTEC of Russia Order № 236 of December 22, 2017.

14. Security Assurance Requirements for Significant Facilities of Critical Information Infrastructure of the Russian Federation (as amended by FSTEC of Russia Order № 138 of August 9, 2018).

15. State Policy Fundamentals of the Russian Federation in the Field of Nuclear and Radiation Safety up to 2025. Endorsed by the RF Presidential Decree № 585 of October 13, 2018.

16. SANDIA REPORT SAND2007-5591 Unlimited Release. Printed September 2007. Nuclear Power Plant Security. Assessment Technical Manual D. W. Whitehead C. S. Potter S. L. O`Connor.

17. Krupchatnikov B.N. On Some Specifics of Nuclear Security Regulation. Nuclear and Radiation Safety, № 3(61), 2011.

18. FATHI ELSISI Sanctions as a Legal Deterrence Mean in the National Physical Protection Regime (CN -254-76). International Conference on Physical Protection of Nuclear Material and Nuclear Facilities 13 – 17 November 2017, Session II: Physical Protection Regime.

19. Policy Statement on Quality of State Nuclear Safety Regulation. Official Website of the Federal Environmental, Industrial and Nuclear Supervision Service (gosnadzor.ru).