Ольга Михайлова

КИБЕРУГРОЗЫ И ФИЗИЧЕСКАЯ ЯДЕРНАЯ БЕЗОПАСНОСТЬ

Растущая автоматизация производственных процессов и применение цифровых технологий при эксплуатации ядерных установок и обращении с радиоактивными материалами увеличивают риск нападения на автоматизированные системы (АС) с использованием программно-технических средств и телекоммуникационных сетей. Иначе говоря, создают риск кибератак.

Обеспечение кибербезопасности — проблема, актуальная для всех объектов критической инфраструктуры, в которых используются АС. Несмотря на то, что общие принципы и подходы к защите различных отраслей несомненно существуют, необходимо учитывать специфику и потенциальные последствия кибератак для каждой из них.

Применительно к ядерной отрасли это могут быть: сложившаяся практика регулирования деятельности ядерных объектов; технические особенности их функционирования, включая необходимость непрерывного осуществления технологических процессов в течение долгого времени; исторически сложившаяся обособленность и закрытость ядерной отрасли; недостаточная осведомленность работников ядерных объектов о киберугрозах и их потенциальных последствиях для безопасности радиоактивных материалов и ядерных установок, а также ложное чувство защищенности ядерных объектов от киберугроз.

Чтобы оценить масштаб проблемы надо иметь в виду, что АС используются для управления реакторами и установками по обогащению урана, сбора и анализа данных о параметрах ядерного объекта, управления транспортно-техническими операциями с ядерными материалами и изделиями из них (например, перегрузкой топлива в активной зоне реактора) и т. п. Кроме того, на ядерных объектах[1] автоматизированными являются системы физической защиты ядерных объектов, учета и контроля ядерных материалов, различные системы документооборота и бухгалтерского учета.

Чтобы разобраться в этом подробнее, зададимся вопросом: что, если в результате кибератаки автоматизированные системы ядерного объекта прекратят выполнять свои функции или будут выполнять их с измененными параметрами, *забыв* сообщить об этом операторам?

Теоретически неожиданное *своенравие* систем, обеспечивающих управление ядерной установкой, процессами обращения с ядерными материалами, а также элемен-

тами безопасности, призванными не допустить аварии, может привести к инциденту, последствия которого могут быть сравнимы с чернобыльской катастрофой.

Не менее пугающими выглядят сценарии отказа или ненадлежащего функционирования системы физической защиты ядерного объекта либо автоматизированной системы учета и контроля ядерных материалов вследствие кибератаки, равно как и хищение данных, с помощью которых злоумышленники могли бы найти способ обойти меры безопасности и похитить ядерные материалы с целью последующего создания ядерного взрывного устройства или *грязной* бомбы. Физическое воздействие на элементы ядерной установки, доступ к которым был получен при помощи кибератаки, может привести к радиационному загрязнению окружающей среды и облучению населения.

Помимо вышеупомянутых рисков, применение АС на ядерных объектах может создавать и другие, менее катастрофические риски, как-то: убытки в результате нарушения бизнес-процессов ядерного объекта, репутационные потери в результате хищения информации о функционировании объекта или разрушения имиджа объекта как надежно защищенного от злоумышленных воздействий.

В зависимости от того, какую цель преследуют злоумышленники (спровоцировать аварию, завладеть радиоактивными материалами или получить доступ к информации), кибератаки могут быть направлены на доступ, уничтожение, модифицирование, блокирование или копирование информации в соответствующих автоматизированных системах ядерного объекта.

В рамках данной статьи мы ограничимся рассмотрением кибератак с целью спровоцировать аварию с неприемлемыми радиационными последствиями или похитить ядерные материалы. Иначе говоря, будем обсуждать угрозы физической ядерной безопасности (ФЯБ).

КИБЕРУГРОЗЫ В КОНТЕКСТЕ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

Обеспечение ФЯБ на ядерных объектах заключается в предотвращении, обнаружении и пресечении хищений ядерных материалов; диверсий (саботажа) в отношении ядерных материалов или ядерных установок, создающих угрозу здоровью или жизни людей в результате воздействия радиации или приводящих к радиоактивному загрязнению окружающей среды; незаконной передачи или других злоумышленных действий в отношении ядерных материалов и установок[2].

Для этого на ядерных объектах проектируются и создаются системы ФЯБ, включающие оборудование, персонал и регламенты. Исходными данными для проектирования таких систем являются результаты анализа уязвимости ядерных объектов: составление перечня предметов, которые необходимо защитить, а также описания возможных сценариев осуществления угроз.

К предметам защиты относят элементы ядерных установок, несанкционированные действия в отношении которых могут привести к аварийной ситуации, облучению людей или радиоактивному загрязнению окружающей среды, например, системы управления реакторной установкой, включая управление цепной реакцией деления.

Список элементов установки, подлежащих защите, составляется для каждого ядерного объекта с учетом результатов вероятностного анализа безопасности,

потенциального масштаба облучения и радиоактивного загрязнения, характеристик ядерного объекта, особенностей ядерной установки и технологического процесса, а также других факторов.

К предметам защиты систем ФЯБ также относятся ядерные материалы, имеющиеся на объекте. Для определения приоритетов при проектировании систем ФЯБ ядерные материалы категорируют по степени привлекательности с точки зрения хищения, а элементы ядерных установок — исходя из масштабов последствий, которые может вызвать направленная против них диверсия. Чем привлекательнее ядерный материал или масштабнее последствия, тем более интенсивными должны быть меры ФЯБ.

Разработчикам систем ФЯБ важно правильно оценивать *проектные угрозы*, то есть понимать, кто и каким образом может попытаться совершить противоправные действия в отношении предметов защиты. Возможные злоумышленники разнятся от фанатиков-одиночек, смутно представляющих себе принципы функционирования ядерного объекта, до хорошо вооруженных преступных групп, обладающих знаниями и технологиями, необходимыми для управления ядерной установкой, имеющих возможность удаленного доступа к управлению системами объекта и действующих в сговоре с персоналом ядерного объекта.

Чтобы выявить реальные угрозы и сценарии их осуществления для каждого конкретного объекта необходимо провести тщательный анализ криминогенной и социальной обстановки, угроз безопасности, признанных на уровне государства и отрасли, степени риска для имеющихся радиоактивных материалов, потенциальных последствий аварий и возможных путей воздействия на элементы ядерной установки с целью вызвать ядерный инцидент.

Кибератаки могут осуществляться удаленно, либо с территории ядерного объекта. Во втором случае злоумышленнику необходимо получить физический доступ к элементам ядерной установки или обеспечить подключение носителя с вредоносным программным обеспечением к элементам установки. Проще всего сделать это при содействии персонала ядерного объекта или подрядных организаций.

Сценарии осуществления угроз могут включать кибератаки следующих типов:

- Кибератаки на автоматизированные системы управления технологическими процессами (АСУ ТП) ядерной установки. Они могут быть направлены на изменение или блокирование управляющих команд, блокирование доступа операторов к информации о состоянии ядерного объекта или искажение такой информации, а также на перепрограммирование промышленных контроллеров. Целью кибератаки может быть инициирование аварии или создание условий для возникновения аварийной ситуации. В результате возможно радиационное заражение местности и/или облучение персонала и населения.
- Кибератаки на автоматизированные системы ФЯБ, включая систему физической защиты и систему учета и контроля ядерных материалов. В данном случае целью кибератаки может быть нарушение функционирования систем физической защиты и/или учета и контроля с целью подготовки хищения радиоактивных материалов или совершения диверсий, в том числе удаленное отключение средств контроля и управления доступом в помещениях с предметами защиты

или изменение настроек измерительных систем, применяемых для учета и контроля ядерных материалов.

- Кибератаки на автоматизированные информационные системы ядерного объекта. Доступ, уничтожение или фальсификация данных дает злоумышленникам возможность осуществить хищение или диверсию, преодолеть меры ФЯБ и т. п. В результате атаки могут быть изменены данные об инвентарных количествах ядерных материалов с целью сокрытия факта их хищения в течение как можно большего срока. Другой пример — несанкционированный доступ к системе документооборота ядерного объекта, где могут находиться сведения о графике проведения технического обслуживания элементов системы физической защиты, транспортирования ядерных материалов или порядке действий персонала по обнаружению и пресечению несанкционированных действий.

Кибератаки на системы ядерного объекта, которые не могут привести к хищению ядерных материалов или диверсии, в контексте ФЯБ не рассматриваются.

Для оценки возможных последствий кибератак с точки зрения ФЯБ рассмотрим несколько сценариев, основанных на данных об имевших место киберинцидентах.

В качестве первого примера возьмем кибератаку в отношении обогатительной установки в иранском городе Натанз. Как известно, для нападения использовался вирус Stuxnet[3], перепрограммировавший промышленные контроллеры таким образом, что они отдавали установке *несовместимые с жизнью* управляющие команды, игнорируя данные датчиков, которые в нормальных условиях должны были привести к выдаче команды на перевод установки в безопасный режим. Пострадавший объект считался защищенным от вирусов в связи с отсутствием физического подключения к интернету, однако вредоносная программа была занесена в его систему управления с внешнего носителя.

Теперь представим, что системы безопасности АЭС, призванные локализовать и/или предотвратить аварию, построены на основе программируемых контроллеров[4], а каналы защиты с жесткой логикой не предусмотрены или выведены из строя. Атака вируса, действующего подобно Stuxnet, может перепрограммировать контроллеры систем безопасности таким образом, что при достижении определенных параметров (например, давления, температуры или реактивности), они не сработают, но сообщат оператору о срабатывании. Другими словами, произойдет отказ систем безопасности, который не будет вовремя обнаружен персоналом. При бездействующих системах безопасности авария, спровоцированная действиями злоумышленников или случайным стечением обстоятельств, может принять катастрофические масштабы[5].

Другим примером может стать получение удаленного доступа к автоматизированной системе с помощью программного обеспечения для создания VPN, применяемого поставщиком оборудования системы физической защиты, IP-адресов оборудования системы физической защиты, имени пользователя и пароля, используемых по умолчанию. Эта информация может быть получена различными способами, включая кибератаки на поставщиков оборудования, подкуп, обман или шантаж персонала. Путем удаленного управления элементами системы физической защиты злоумышленники могут обеспечить себе беспрепятственный проход в охраняемые зоны объекта и выход из них, одновременно заблокировав проход для персонала. Изображение с камер видеонаблюдения может быть *зациклено* таким образом,

чтобы демонстрировать оператору отснятую ранее картинку пустого помещения в то время, как в нем находятся злоумышленники. В результате преступники смогут совершить задуманное, например, похитить ядерные материалы или осуществить диверсию и беспрепятственно покинуть объект[6].

Весьма эффективный способ скомпрометировать корпоративную сеть — рассылка во внутренней сети предприятия фишинговых сообщений, через которые может быть загружен вирус, способный выкрасть чертежи и схемы ядерной установки[7]. Полученная информация может затем быть использована преступниками для выявления наиболее эффективных способов диверсии или хищения радиоактивных материалов.

При этом важно понимать, что вышеописанные сценарии могут иметь комбинированный характер. Злоумышленники могут совершать кибератаки не только с непосредственно диверсионными целями, но и для подготовки диверсий или усиления их негативных последствий.

ЗАЩИТА ОТ КИБЕРУГРОЗ, ЗНАЧИМЫХ С ТОЧКИ ЗРЕНИЯ ФЯБ: ПОДХОДЫ И ПЕРСПЕКТИВЫ

Необходимость осмысления проблемы кибербезопасности в контексте ядерной отрасли в целом и физической ядерной безопасности в частности в настоящее время признана на международном уровне. Происходит активное обсуждение и выработка подходов к ее решению при непосредственном участии и поддержке МАГАТЭ. Ярким примером такой деятельности является проведенная МАГАТЭ в июне 2015 г. международная конференция, посвященная компьютерной безопасности в ядерной отрасли, *Компьютерная безопасность в ядерном мире: дискуссия экспертов и обмен мнениями.*

В рамках конференции широко обсуждались вопросы безопасности информации в автоматизированных информационных системах, системах управления технологическими процессами, а также физической защиты, применяемых в ядерной отрасли. Помимо прочего, были охвачены все вышеописанные киберугрозы, значимые для ФЯБ, а также отмечена необходимость разработки указаний и рекомендаций по вопросам кибербезопасности с учетом особенностей ядерной отрасли. В материалах конференции МАГАТЭ[8,9] отмечены три направления обеспечения кибербезопасности, которым необходимо уделить внимание как важной составляющей обеспечения безопасности ядерных объектов и других организаций ядерной отрасли:

- кибербезопасность автоматизированных систем управления технологическими процессами ядерных объектов;
- кибербезопасность автоматизированных информационных систем;
- кибербезопасность систем физической защиты ядерных объектов.

В настоящее время существует ряд исследований и публикаций по каждому из трех направлений, содержащих описание соответствующих киберугроз, подходов к их выявлению и подходов к выявлению уязвимостей автоматизированных систем, которые могут быть использованы для реализации угроз. Также публикации описывают уже предпринятые усилия для создания методической, нормативной и технической базы в области защиты от киберугроз, значимых с точки зрения

ФЯБ, а также приводят рекомендации по дальнейшим усилиям, которые необходимо предпринять.

Говоря о кибербезопасности автоматизированных систем ядерных объектов хотелось бы отметить исследования, посвященные состоянию и перспективным направлениям работ по этому вопросу, проведенные Chatham House (Британским Королевским институтом международных отношений), а также работы фонда *Инициатива по снижению ядерной угрозы* и Университета прикладных наук Бранденбурга[10,11,12].

Первое исследование в основном посвящено кибербезопасности автоматизированных систем управления ядерными установками, другие касаются мер по обеспечению кибербезопасности в контексте ФЯБ. Публикации по результатам данных исследований содержат общее описание киберугроз, которые необходимо учитывать, а также описывают инструменты и подходы, используемые для обеспечения защиты от них в различных станах (в том числе — Соединенных Штатах Америки и Российской Федерации). В работах также представлены рекомендации по созданию, совершенствованию и развитию указанных подходов и инструментов.

В числе прочего, в упомянутых публикациях обозначена проблема недостаточной осведомленности о киберугрозах и возможных мерах защиты от них как на уровне ядерной отрасли в целом, так и на уровне специалистов, эксплуатирующих и проектирующих автоматизированные системы. В связи с этим рекомендовано наращивать обмен информацией о киберугрозах АСУ ТП и практиках защиты от них как внутри ядерной отрасли, так и со специалистами других отраслей, в которых эксплуатируются потенциально опасные объекты, например, химической промышленности или гидроэнергетики, имеющими опыт разработки и применения мер по защите от киберугроз.

Примеры использования ядерной отраслью опыта других отраслей в обеспечении кибербезопасности АСУ ТП описаны в материалах ежегодных конференций Института управления ядерными материалами[13,14].

В качестве одной из проблем, которую необходимо решить для создания эффективных мер обеспечения кибербезопасности, обозначено отсутствие продолжительной практики внедрения таких мер в проектируемые АСУ ТП, неспособность профессионалов в области киберпространства и специалистов, проектирующих и эксплуатирующих ядерные установки, найти общий язык и эффективно сотрудничать, а также отсутствие практики такого сотрудничества на постоянной основе.

В качестве пути решения проблемы предлагается разработка обучающих программ, которые дали бы специалистам по кибербезопасности представление об особенностях проектирования и функционирования автоматизированных систем управления ядерного объекта, а также систем ФЯБ, а проектировщикам и эксплуатирующему персоналу атомной установки — представление о мерах обеспечения кибербезопасности и порядке их разработки. Это должно привести к отсутствию конфликтов мер ФЯБ и кибербезопасности, включая меры по реагированию на несанкционированные действия, меры по обслуживанию систем и т. п.

Кроме того, рекомендована разработка методик и инструментов, направленных на объединение процессов анализа уязвимости в обеих сферах обеспечения безопасности ядерных объектов. Результатом объединения процессов должно стать выявление программно-технических средств и сетей обмена данными; информации, к которой необходимо применять меры кибербезопасности во избе-

жание реализации угроз ФЯБ, а также оборудования и сетей, физический доступ к которым необходим для совершения кибератаки, с последующим включением их в перечень предметов защиты систем ФЯБ.

Подробнее об этих процессах можно узнать из материалов ежегодных конференций Института управления ядерными материалами[15,16,17,18,19]. В публикациях, ссылки на которые даны в этой части статьи, представлены конкретные технические и организационные меры, которые следует предпринять ядерным объектам для снижения рисков, связанных с применением автоматизированных систем.

СОСТОЯНИЕ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ

В настоящее время вопросам кибербезопасности в обеспечении ФЯБ уделяется внимание как в рекомендациях МАГАТЭ, так и в документах профильных национальных ведомств. Подходы к регулированию этого вопроса могут быть различны. Их сравнительный анализ можно найти в отчетах фонда *Инициатива по снижению ядерной угрозы* и Университета прикладных наук Бранденбурга[20], упомянутых выше. Существующие подходы можно условно разделить на два типа.

В первом случае кибербезопасность на ядерных объектах обеспечивается в соответствии с требованиями законов и подзаконных актов в области защиты критической инфраструктуры, а также государственной тайны и другой конфиденциальной информации. При этом ядерное законодательство и документы ядерного регулятора (органа, осуществляющего регулирование безопасности при использовании атомной энергии: лицензирование, установление требований к обеспечению безопасности, надзор за их соблюдением) содержат отдельные общие требования необходимости обеспечения кибербезопасности. Ядерные регуляторы в этом случае не занимаются данной проблемой, а документы в этой области, которыми руководствуются ядерные объекты, в большинстве своем не учитывают специфику отрасли, за исключением методических документов, издаваемых органами управления использованием атомной энергии (например, Росатом, Минпромторг, и.т.д.) для подведомственных объектов. Именно этот подход принят в Российской Федерации.

Во втором случае вопросы кибербезопасности регламентируются документами, издаваемыми уполномоченным органом в области регулирования безопасности ядерных установок. Такие документы учитывают специфику ядерной отрасли, а ядерный регулятор занимается в том числе и проблемами кибербезопасности атомных установок (в той мере, в которой это связано с обеспечением ФЯБ). Такой подход принят, например, в Соединенных Штатах Америки. Подробнее о деятельности Комиссии по ядерному регулированию США в этой сфере можно ознакомиться в материалах ежегодных конференций Института управления ядерными материалами[21,22]. Далее мы несколько подробнее рассмотрим рекомендации МАГАТЭ и требования, имеющиеся в российских документах.

РЕКОМЕНДАЦИИ МАГАТЭ

Документы, входящие в серию изданий МАГАТЭ по вопросам ФЯБ, содержат рекомендации по обеспечению кибербезопасности, начиная с базовых и заканчивая конкретными указаниями по разработке и внедрению соответствующих мер на ядерных объектах. Базовые рекомендации даны в основополагающем докумен-

те серии № 20 *Цель и основные элементы государственного режима ФЯБ*. Согласно его тексту, чувствительная информация (информация, несанкционированные действия в отношении которой могут поставить под угрозу физическую ядерную безопасность), а также средства, используемые для взаимодействия с ней, являются потенциальными целями злоумышленников (нарушителей) и должны быть защищены в рамках деятельности по обеспечению ФЯБ. Кибербезопасность в этом случае только подразумевается. Также в документе прямо указано на необходимость проведения регулярного анализа факторов, негативно влияющих на способность обеспечивать физическую ядерную безопасность, включая киберугрозы.

Рекомендации МАГАТЭ № 13 *Рекомендации по ФЯБ, касающиеся физической защиты ядерных материалов и ядерных установок (INFCIRC/225/Rev. 5)*[23], описывающие конкретные меры физической защиты, которые должны быть предприняты для выполнения основополагающего документа, конкретизируют рекомендации к мерам по обеспечению кибербезопасности автоматизированных систем, также необходимым для обеспечения ФЯБ. Согласно документу, «компьютеризированные системы, используемые для обеспечения физической защиты, ядерной безопасности, а также учета и контроля ядерных материалов, следует защищать от компрометации (например, кибератак, манипуляции или фальсификации) в соответствии с оценкой угроз или проектной угрозой» (см. пп. 4.10 и 5.19). Рекомендации INFCIRC/225 рассматриваются ядерными регуляторами и ядерными объектами как описание минимально необходимых на объекте мер физической защиты. В некоторых случаях данным рекомендациям придается обязательный характер путем включения требований об обеспечении физической защиты на уровне не ниже рекомендуемого INFCIRC/225, в международные договоры, связанные с транспортированием радиоактивных материалов или с развитием ядерной энергетики. Таким образов включение пп. 4.10 и 5.19 в этот документ способствует тому, что киберугрозы, значимые с точки зрения обеспечения ФЯБ, будут учтены при проектировании систем ФЯБ большинства ядерных объектов.

INFCIRC/225 рекомендует обеспечивать кибербезопасность исходя из вызовов, предусмотренных проектной угрозой. Практическое руководство № 10 *Разработка, применение и актуализация проектной угрозы* предусматривает необходимость учета возможностей потенциальных нарушителей по использованию уязвимостей автоматизированных систем ядерного объекта для непосредственной поддержки физической атаки на нем, сбора данных при подготовке к физической атаке и других целей.

Еще одно практическое руководство в этой серии — № 23-G *Безопасность информации в области ядерной энергетики* — содержит рекомендации МАГАТЭ по выявлению информации, чувствительной с точки зрения ФЯБ, и обеспечению защиты такой информации — в первую очередь с точки зрения обеспечения конфиденциальности. Документ касается общих мер по защите информации без привязки к киберугрозам.

Наиболее детальные рекомендации по обеспечению кибербезопасности в контексте обеспечения ФЯБ даны в справочном руководстве № 17 *Компьютерная безопасность на ядерных установках*. В документе приведены рекомендации, предназначенные для органов, осуществляющих регулирование в ядерной сфере и области кибербезопасности. Они включают в себя замечания о необходимости учета специфики ядерных объектов при определении требований к кибербезопасности, для чего регуляторы должны взаимодействовать друг с другом при анализе и согла-

совании имеющихся требований законодательства и нормативных документов как в области ФЯБ, так и в области кибербезопасности. В документе содержатся подробные рекомендации по учету возможностей потенциальных злоумышленников при формировании проектной угрозы, а также при разработке сценариев диверсий или хищений в ходе подготовки к проектированию систем ФЯБ. Даны рекомендации по выявлению на ядерных объектах конкретных программных и технических средств и телекоммуникационных сетей, которые необходимо защитить от киберугроз, а также рекомендации по дифференциации мер защиты от кибератак в зависимости от их возможного влияния на обеспечение ФЯБ. Помимо этого, приведены рекомендации по созданию программы обеспечения кибербезопасности на ядерном объекте, которую необходимо согласовать с мерами по обеспечению ФЯБ.

В настоящее время ожидается пополнение серии изданий МАГАТЭ публикациями в области кибербезопасности (практические руководства, технические руководящие материалы и документы серии TECDOC), которые должны оказать государствам и ядерным объектам практическую помощь в разработке мер по обеспечению ФЯБ[24].

РОССИЙСКАЯ НОРМАТИВНО-ПРАВОВАЯ БАЗА

Практика регулирования кибербезопасности в контексте обеспечения ФЯБ, сложившаяся в РФ, отличается от рекомендаций МАГАТЭ. Обеспечение физической ядерной безопасности регламентируется в основном документами, касающимися физической защиты, а также учета и контроля ядерных материалов, издаваемых правительством и ядерным регулятором — Ростехнадзором. Эти документы требуют обеспечивать защиту информации в системах учета и контроля и физической защиты, но не определяют конкретные меры защиты информации, а содержат общие ссылки на нормативные правовые акты в области защиты информации. Например, указывается, что защита информации должна быть обеспечена в соответствии с законодательством Российской Федерации.

Документов правительства и Ростехнадзора, применимых ко всем ядерным объектам и дающих детальные указания по обеспечению кибербезопасности в контексте ФЯБ, не существует. Обеспечение безопасности автоматизированных систем управления ядерными установками и процессами обращения с ядерными материалами, а также автоматизированных информационных систем не относится к задачам обеспечения физической защиты или учета и контроля и, соответственно, не регулируется российскими нормативными правовыми документами в области ФЯБ. Соответствующие требования установлены законодательством в области защиты государственной тайны, защиты информации, не составляющей государственную тайну, безопасности критической информационной инфраструктуры Российской Федерации, а также методическими и нормативными документами ведомств, имеющих регуляторные полномочия в этих областях — Федеральной службы безопасности и Федеральной службы по техническому и экспортному контролю.

В настоящее время кибербезопасность АСУ ТП ядерных установок и обращения с ядерными материалами обеспечивается в соответствии с применимыми во всех отраслях документами, устанавливающими требования и конкретные меры по обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации. Эти документы еще не образуют четкую структуру, а являются скорее набором разрозненных актов, объединенных общей тематикой. К ним относятся:

- *Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации,* утвержденные президентом Российской Федерации 3 февраля 2012 г.; указ президента Российской Федерации от 15.01.2013 № 31 С *О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации*, *Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации* утвержденная президентом 12 декабря 2014 г. Эти документы определяют базовые термины и требования в отношении защиты критической информационной инфраструктуры, а также основные факторы, влияющие на состояние защищенности объектов.
- Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. *Об утверждении требований 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*. Документ является обязательным для критически важных объектов, включая ядерные.
- Методические документы Федеральной службы по техническому и экспортному контролю, касающиеся защиты информации в ключевых системах информационной инфраструктуры:
  - Информационное сообщение Федеральной службы по техническому и экспортному контролю России от 25 июля 2014 г. по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа Федеральной службы по техническому и экспортному контролю России от 14 марта 2014 г.
  - *Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры*, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю России 18 мая 2007 г.
  - *Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры*.
  - *Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры*.
  - *Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры* от 19 ноября 2007 г.

Конкретные рекомендации по защите информации в автоматизированных системах, а также по аттестации таких систем, применимые в том числе к системам учета и контроля, а также физической защиты, определены в методических документах Федеральной службы по техническому и экспортному контролю, таких как *Специальные требования и рекомендации по технической защите конфиденциальной информации* и *Автоматизированные системы. Защита от несанкционированного*

доступа к информации. Классификация автоматизированных систем и требования о защите информации.

В соответствии с Законом о государственной тайне и Указом Президента РФ № 1203 от 30 ноября 1995 г. (ред. от 28 февраля 2016 г.) *Об утверждении Перечня сведений, отнесенных к государственной тайне,* к ней относится информация, значимая для обеспечения ФЯБ: сведения о проектировании, сооружении, эксплуатации, обеспечении безопасности объектов ядерного комплекса, о физической защите ядерных материалов, изделий на их основе, ядерных установок, пунктов хранения ядерных материалов, об охране радиационно-опасных объектов. Требования к обеспечению безопасности такой информации, в том числе кибербезопасности, включают требование о лицензировании ядерного объекта на право ведения работ с использованием указанных сведений и о применении только сертифицированных средств защиты информации в соответствующих автоматизированных информационных системах. Сертификация осуществляется в соответствии с требованиями государственных стандартов, создаваемых Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности.

Основные документы в области ФЯБ в Российской Федерации[25,26,27] устанавливают следующие требования в части обеспечения кибербезопасности:

- Система государственного учета и контроля ядерных материалов должна обеспечивать ограничительный порядок доступа к информации в целях защиты сведений, отнесенных к государственной тайне или служебной информации ограниченного распространения.
- Системы физической защиты должны включать подсистемы защиты информации, обеспечивающие в том числе секретность (конфиденциальность) информации об организации, составе и функционировании системы физической защиты, ее целостность и санкционированную доступность, нарушение которых может приводить к снижению эффективности системы физической защиты в целом или ее отдельных элементов (оборудование, соответствующее программное обеспечение, организационные и технические меры)[28].
- Технические и программные средства защиты информации, составляющей государственную и служебную тайны, подлежат обязательной сертификации на соответствие требованиям безопасности.
- На этапе ввода в действие автоматизированной системы физической защиты (до завоза ядерных материалов на объект) должна выполняться ее аттестация на предмет соответствия требованиям информационной безопасности.

Ядерные объекты также руководствуются документами федеральных органов управления использованием атомной энергии (например, Росатома и Минпромторга) и эксплуатирующих организаций (например, требования концерна *Росэнергоатом*, предназначенные для АЭС), выпущенными с целью оказания помощи подведомственным объектам в выполнении требований к обеспечению ФЯБ. Набор документов, доступных конкретному ядерному объекту, зависит от того, какому органу власти и какой эксплуатирующей организации он подчиняется. Некоторые из них накопили значительный практический опыт обеспечения кибербезопасности и согласования его с мерами ФЯБ.

В целом разработка мер кибербезопасности описанных в вышеуказанных документах, включает выявление информации, программных и технических средств, а также телекоммуникационных сетей, защиту которых необходимо обеспечить, определение перечня угроз безопасности информации и моделей нарушителей. Затем определяются требования к организационным и техническим мерам. Интенсивность мер и применимые требования определяются исходя из вида защищаемой информации и ее значимости.

ЗАКЛЮЧЕНИЕ

Рекомендации МАГАТЭ по обеспечению кибербезопасности, в контексте ФЯБ, а также рекомендации в этой области, опубликованные по результатам различных исследований, предусматривают учет киберугроз и последствий их реализации при проектировании систем ФЯБ. Также необходимо учитывать значимость с точки зрения ФЯБ информации в автоматизированных системах объекта, а также соответствующего программного обеспечения и оборудования. Кроме того, опубликованные рекомендации предполагают необходимость согласования мер ФЯБ и кибербезопасности, а также принятия ряда организационных мер на уровне государства и ядерных объектов.

В настоящее время в российских документах нет целостного универсального набора требований и рекомендаций, которыми могли бы воспользоваться специалисты для того, чтобы обеспечить всесторонний учет значимых с точки зрения ФЯБ киберугроз. Для обеспечения эффективности программ кибербезопасности и ФЯБ на всех ядерных объектах, а также распространения имеющихся лучших практик необходимы:

- дальнейшее совершенствование и структурирование национального законодательства, нормативных документов и рекомендаций в области защиты критической информационной инфраструктуры и защиты информации;
- активное участие специалистов ядерной отрасли в обсуждении проектов документов в области кибербезопасности (включая проекты документов, касающихся критической информационной структуры);
- адаптация и применение рекомендаций МАГАТЭ, связанных с обеспечением кибербезопасности в контексте ФЯБ, в том числе терминологии, к российским реалиям, включение их, например, в рекомендации Ростехнадзора и практическое применение на ядерных объектах;
- включение в документы Ростехнадзора, применимые ко всем мирным ядерным объектам, положений, предусматривающих учет сценариев реализации угроз, включающих кибератаки, при проектировании систем ФЯБ;
- анализ совокупности применимых к ядерным объектам требований в области обеспечения кибербезопасности, включая документы федеральных органов власти, которым подведомственны объекты, и оценка их достаточности и согласованности с требованиями в области ФЯБ;
- развитие и поощрение совместной работы специалистов в области кибербезопасности, ФЯБ и проектирования ядерных установок для обеспечения внедрения мер кибербезопасности на ранних стадиях проектирования систем ядерного объекта;

- дальнейшее совершенствование методов анализа уязвимостей, применяемых для целей ФЯБ и для целей кибербезопасности, а также методов оценки эффективности мер ФЯБ и мер кибербезопасности, направленное на учет сценариев, связанных с кибератаками на системы ФЯБ и системы управления ядерными установками, а также с физическим доступом злоумышленников к элементам автоматизированных систем атомных установок;
- обмен опытом между федеральными органами власти, осуществляющими управление использованием атомной энергии и координирующими вопросы безопасности на подведомственных объектах, между ядерными объектами, подведомственными различным органам управления, а также между ядерной отраслью и отраслями, в которых эксплуатируются объекты критической инфраструктуры, для взаимного обмена лучшими практиками обеспечения кибербезопасности и выполнения требований, установленных в нормативных правовых документах.

Примечания

1 Организация, на территории которой осуществляется использование ядерных материалов, размещаются и/или эксплуатируются ядерные установки

2 International Atomic Energy Agency. Division of Nuclear Security. Nuclear Security Series Glossary: Version 1.3 (November 2015). P. 18, http://www-ns.iaea.org/downloads/security/nuclear-security-series-glossary-v1-3.pdf (последнее посещение — 21 марта 2016 г.).

3 Описание кибератаки можно найти, например, в Baylon Caroline, Brunt Roger, Livingstone David. Chatham House Report. Cyber Security at Civil Nuclear Facilities: Understanding the Risks. P. 3–4. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005 CyberSecurityNuclearBaylonBruntLivingstone.pdf (последнее посещение — 21 марта 2016 г.).

4 В примере описан гипотетический случай, не учитывающий требования российских документов к проектированию систем, обеспечивающих безопасность ядерных объектов, и практику, сложившуюся в этой области.

5 Упомянутая кибератака описана, например, в Baylon Caroline, Brunt Roger, Livingstone David. Chatham House Report. Cyber Security at Civil Nuclear Facilities: Understanding the Risks. P. 3–4. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf (последнее посещение — 21 марта 2016 г.)

6 Приведенный пример описан в Anderson Robert S., Bjornard Trond, St. Michel Curtis, Schanfein Mark, Moskowitz Paul. Cyber Threats to Nuclear Infrastructures. Proceedings of 51st Annual Meeting of the Institute of Nuclear Materials Management. 11–15 July 2010

7 Упомянутая кибератака описана, например, в Baylon Caroline, Brunt Roger, Livingstone David. Chatham House Report. Cyber Security at Civil Nuclear Facilities: Understanding the Risks. P. 5. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf (последнее посещение — 21 марта 2016 г.) .

8 IAEA's Amano Calls for Strengthened Computer Security in a Nuclear World (Press Release). International Atomic Energy Agency. 1 June 2015, https://www.iaea.org/newscenter/news/iaea%E2%80%99s-amano-calls-.strengthened-computer-security-nuclear-world (последнее посещение — 21 марта 2016 г.).

9 Secure Computer Systems Essential to Nuclear Security, Conference Finds (Press Release). International Atomic Energy Agency. 8 June 2015, https://www.iaea.org/newscenter/news/secure-computer-systems-essential-nuclear-security-conference-finds (последнее посещение — 21 марта 2016 г.).

10 Cyber Security at Nuclear Facilities: National Approaches An ISS Research Project in Cooperation with the Nuclear Threat Initiative (NTI), http://www.nti.org/media/pdfs/Cyber_Security_in_Nuclear_FINAL.pdf?_=1445548675 (последнее посещение — 21 марта 2016 г.)

11 Chamales George. A New Approach to Nuclear Computer Security, http://www.nti.org/media/pdfs/A_New_Approach_to_Nuclear_Computer_Security.pdf?_=1445875704&_=1445875704 (последнее посещение — 21 марта 2016 г.)

12 Baylon Caroline, Brunt Roger, Livingstone David. Chatham House Report. Cyber Security at Civil Nuclear Facilities: Understanding the Risks. P. 3–4. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf (последнее посещение — 21 марта 2016 г.)

13 Bjornard Trond, Schanfein Mark, Moskowitz Paul, Anderson Robert. DOE/DHS Industrial Control System Cyber Security Programs: A Model For Use in Nuclear Facility Safeguards and Security. Proceedings of 52nd Annual Meeting of the Institute of Nuclear Materials Management. 17–21 July 2011.

14 Ibid.

15 Anderson Robert, Price Joseph. Cyber Informed Engineering: The Need for a New Risk Informed and Design Methodology. Proceedings of 56th Annual Meeting of the Institute of Nuclear Materials Management. 12–16 July 2015.

16 Anderson Robert S., Bjornard Trond, St. Michel Curtis, Schanfein Mark, Moskowitz Paul. Cyber Threats to Nuclear Infrastructures. Proceedings of 51st Annual Meeting of the Institute of Nuclear Materials Management. 11–15 July 2010.

17 MacDonald Doug, Key Brad, Clements Sam, Hutton William, Craig Philip, Patrick Scott, Crawford Cary. Cyber/Physical Security Vulnerability Assessment Integration. Proceedings of 52nd Annual Meeting of the Institute of Nuclear Materials Management. 17–21 July 2011.

18 Whattam Kevin, Gastelum Zoe N., Cramer Nick O., Conklin K. Examining Impacts, Challenges and Next Steps for Nuclear Nonproliferation and the Cyber Environment. Proceedings of 55th Annual Meeting of the Institute of Nuclear Materials Management. 20–24 July 2014.

19 Masica Kenneth, Porter Jeremiah, Porter Stephen J. Physical Protection Systems and the Cyber Security Component. Proceedings of 56th Annual Meeting of the Institute of Nuclear Materials Management, 12–16 July 2015.

20 Cyber Security at Nuclear Facilities: National Approaches An ISS Research Project in Cooperation with the Nuclear Threat Initiative (NTI), http://www.nti.org/media/pdfs/Cyber_Security_in_Nuclear_FINAL.pdf?_=1445548675 (последнее посещение — 21 марта 2016 г.)

21 Smith Brian W., Rivers Joseph, Harris Larry, Sapountzis Alexander, Richardson Rebecca. Development of an Approach for the Creation of a Cyber Security Program for Fuel Cycle Facilities regulated by the Nuclear Regulatory Commission. Proceedings of 54th Annual Meeting of the Institute of Nuclear Materials Management, 14–18 July 2013.

22 Rivers Joseph, Opara Stella, Lee Eric, Bergemann Brad, Felts Russell, Westreich Barry. Cyber Security Program for Facilities regulated by the U.S. Nuclear Regulatory Commission. Proceedings of 55th Annual Meeting of the Institute of Nuclear Materials Management. 20–24 July 2014.

23 Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок. Международное агентство по атомной энергии. Вена, 2012 г. http://www-pub.iaea.org/books/IAEABooks/8814/Nuclear-Security-Recommendations-on-Physical-Protection-of-Nuclear-Material-and-Nuclear-Facilities-INFCIRC-225-Revision-5 (последнее посещение — 20 мая 2016 г.)

24 Подробнее о вышедших и будущих публикациях МАТАГЭ см: Лукацкий Алексей. Кибербезопасность ядерных объектов. *Индекс Безопасности.* 2015. № 4 (115). С. 123–125, а также Gates, Guards, Guns and Geeks: The Changing Face of Nuclear Security and the IAEA's Leading Role in Promoting Computer Security for Nuclear Facilities, https://www.iaea.org/NuclearPower/Downloadable/Meetings/2015/2015-05-27-05-29-NPES/Day2/21.NSNI_CompSecurity__.pdf (последнее посещение — 21 марта 2016 г.)

25 Постановление правительства Российской Федерации № 456 от 19 июля 2007 г. (ред. от 14 марта 2014 г.) *Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов*

26 Приказ Ростехнадзора № 343 от 8 сентября 2015 г. *Об утверждении федеральных норм и правил в области использования атомной энергии «Требования к системам физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов*.

27 Постановление правительства РФ от Российской Федерации 6 мая 2008 г. № 352 (ред. от 4 февраля 2011 г.) «Об утверждении Положения о системе государственного учета и контроля ядерных материалов»

28 Постановление Ростехнадзора от 4 октября 2004 *Об утверждении и введении в действие федеральных норм и правил в области использования атомной энергии «Требования к управляющим системам, важным для безопасности атомных станций»*