БЮЛЛЕТЕНЬ МАГАТЭ
МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
Флагманская публикация МАГАТЭ | Июнь 2023 года | www.iaea.org/ru/bulletin

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ В ЯДЕРНОЙ СФЕРЕ

БЮЛЛЕТЕНЬ МАГАТЭ
издается
Бюро общественной информации
и коммуникации (OPIC)
Международное агентство по атомной энергии
Венский международный центр
А/я 100, 1400 Вена, Австрия
Тел.: (43-1) 2600-0
iaeabulletin@iaea.org

Ответственный редактор: Эмма Миджли
Дизайн и верстка: Риту Кенн

БЮЛЛЕТЕНЬ МАГАТЭ имеется в интернете по адресу:
www.iaea.org/ru/bulletin

Обложка: (Adobestock.com)

Читайте наши новости на сайтах:

IAEA

Миссия Международного агентства по атомной энергии состоит в том, чтобы предотвращать распространение ядерного оружия и помогать всем странам — особенно развивающимся — в налаживании мирного, безопасного и надежного использования ядерной науки и технологий.

Созданное в 1957 году как автономная организация под эгидой Организации Объединенных Наций, МАГАТЭ — единственная организация системы ООН, обладающая экспертным потенциалом в сфере ядерных технологий. Уникальные специализированные лаборатории МАГАТЭ способствуют передаче государствам — членам МАГАТЭ знаний и экспертного опыта в таких областях, как здоровье человека, продовольствие, водные ресурсы, экономика и окружающая среда.

МАГАТЭ также служит глобальной платформой для укрепления физической ядерной безопасности. МАГАТЭ выпускает Серию изданий по физической ядерной безопасности, в которой выходят одобренные на международном уровне руководящие материалы по физической ядерной безопасности. МАГАТЭ также ставит своей задачей содействие минимизации риска того, что ядерные и другие радиоактивные материалы попадут в руки террористов и преступников и что ядерные установки окажутся объектом злоумышленных действий.

Нормы безопасности МАГАТЭ устанавливают основополагающие принципы, требования и рекомендации, касающиеся обеспечения ядерной безопасности, и отражают международный консенсус в отношении того, что можно считать высоким уровнем безопасности для защиты людей и окружающей среды от вредного воздействия ионизирующего излучения. Нормы безопасности МАГАТЭ разрабатывались для всех типов ядерных установок и деятельности, преследующих мирные цели, а также для защитных мер, необходимых для снижения существующих рисков облучения.

Кроме того, при помощи своей системы инспекций МАГАТЭ проверяет соблюдение государствами-членами их обязательств, касающихся использования ядерного материала и установок исключительно в мирных целях, в соответствии с Договором о нераспространении ядерного оружия и другими соглашениями о нераспространении.

Работа МАГАТЭ многогранна, и в ней участвует широкий круг партнеров на национальном, региональном и международном уровнях. Программы и бюджет МАГАТЭ формируются на основе решений его директивных органов — Совета управляющих, насчитывающего 35 членов, и Генеральной конференции всех государств-членов.

Центральные учреждения МАГАТЭ находятся в Венском международном центре. Полевые бюро и бюро по связи расположены в Женеве, Нью-Йорке, Токио и Торонто. В Вене, Зайберсдорфе и Монако работают научные лаборатории МАГАТЭ. Кроме того, МАГАТЭ оказывает содействие и предоставляет финансирование Международному центру теоретической физики им. Абдуса Салама в Триесте, Италия.

Важнейшая роль компьютерной безопасности в обеспечении ядерной и физической безопасности

Рафаэль Мариано Гросси, Генеральный директор МАГАТЭ

Темпы цифровых инноваций поражают воображение: такие технологии, как искусственный интеллект (ИИ), только за последние несколько месяцев продемонстрировали небывалый прогресс. Эти достижения помогут нам совершенствовать технологии цифрового управления и автоматизации на ядерных установках, что дает потенциальные преимущества в виде повышения эффективности эксплуатации, снижения затрат на рабочую силу и укрепления безопасности.

Усовершенствованные проекты ядерных реакторов, например модульные реакторы малой мощности (ММР) и микрореакторы, изначально предусматривают планы по использованию ИИ и машинного обучения (МО) для реализации таких инновационных функций, как автоматизация, дистанционный диспетчерский контроль и техническое обслуживание, а также использование единого пункта управления для нескольких установок. Но цифровые инновации, в том числе ИИ и МО, также несут в себе и риски. Они требуют от персонала постоянной бдительности для обеспечения целостности чувствительных активов и защиты информации на ядерных и радиологических установках.

В то время как для обеспечения защиты ядерных установок от саботажа или проникновения злоумышленников было достаточно металлических дверей и службы охраны, сегодня мы попадаем все в большую зависимость от цифровых систем. Для реализации ключевых функций ядерной и физической безопасности на ядерных установках предусмотрены системы контроля и управления. Это повышает эффективность, но также и подразумевает, что мы должны особенно внимательно относиться к вопросам защиты этих компьютерных систем. Страны во всем мире придают этому первостепенную важность.

МАГАТЭ играет уникальную роль в развитии сотрудничества между странами и формировании среды для обмена технологическими ноу-хау и передовыми наработками для внедрения быстро развивающихся технологий. В то же время мы консультируем страны на тему того, как минимизировать и смягчить неизбежно возникающие при этом потенциальные уязвимости, влияющие на компьютерную безопасность. Только за последние два года масштабы нашей глобальной деятельности по оказанию помощи в обеспечении компьютерной безопасности возросли более чем на четверть. Особый акцент при этом делается на предоставляемую на национальном уровне поддержку по вопросам нормотворчества и инспекционной деятельности в области компьютерной безопасности и организации учений по компьютерной безопасности.

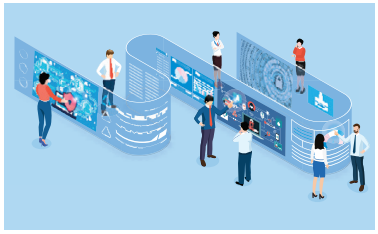
Для реагирования на потребности своих государств-членов в области физической ядерной безопасности МАГАТЭ предлагает широкий спектр различных услуг и мероприятий, в том числе руководящие документы и учебные модули, которые помогают в разработке полноценных национальных программ по информационной и компьютерной безопасности. Эти руководства используются также в качестве эталона для оценки программы страны по обеспечению информационной и компьютерной безопасности в рамках международных консультационных услуг по физической защите (ИППАС).

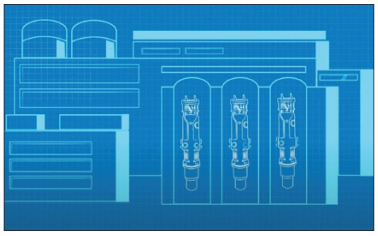
Кроме того, мы открываем школу для подготовки специалистов, которые будут разрабатывать нормативные положения в области компьютерной безопасности. Вскоре, после того как будет запущена онлайн-платформа виртуального обучения, доступ к учебным курсам МАГАТЭ по компьютерной безопасности смогут получить гораздо больше стран.

Одновременно с этим, в целях повышения осведомленности об угрозе кибератак и их возможных последствиях для физической ядерной безопасности, МАГАТЭ содействует проведению национальных и региональных учений по компьютерной безопасности. Мы создаем условия для сотрудничества между международными экспертами и представителями директивных органов и организуем сопутствующие исследования по данной теме.

Деятельность МАГАТЭ в области компьютерной безопасности будет расширяться на фоне того, как многие страны, включая страны с низким и средним уровнем дохода, будут все чаще обращаться к ядерной технологии для решения своих приоритетных задач, в том числе в области экологически чистой энергетики, онкологической помощи, питания и прикладных исследований.

Мы соберемся вместе на международной конференции МАГАТЭ «Компьютерная безопасность в ядерном мире: в интересах обеспечения ядерной безопасности» для обсуждения ключевых проблем и решений и определения дальнейших направлений работы, чтобы извлекать максимальную пользу из цифровых инноваций в ядерном секторе и быть на шаг впереди тех, кто намеревается использовать их для причинения вреда.





ИНТЕРВЬЮ

МИРОВОЙ ОБЗОР

СЕГОДНЯ В МАГАТЭ

Реагирование на угрозы компьютерной безопасности

Эволюция программы помощи МАГАТЭ

Василики Тафили

Существенное влияние на ядерную и физическую безопасность оказывает переход к новым типам общественного взаимодействия на основе цифровых сетей, когда повседневные задачи связываются между собой при помощи компьютерных систем, искусственного интеллекта (ИИ) и цифровых технологий. Трудно переоценить важную роль цифровых технологий в поддержании функций ядерной и физической безопасности на установках, где используется ядерный материал или другой радиоактивный материал.

«Компьютерные системы имеют важнейшее значение для установок, в которых используется ядерный и другой радиоактивный материал, и связанной с ними деятельности», — говорит директор Отдела физической ядерной безопасности МАГАТЭ Елена Буглова. Она особо отмечает необходимость реализации всеми странами программ компьютерной безопасности и совершенствования глубокоэшелонированной защиты для целей физической ядерной безопасности. «Для обеспечения конфиденциальности, целостности и доступности чувствительной информации и активов в условиях быстрого развития технологий необходима неусыпная бдительность для предотвращения и снижения рисков, а также надежная программа информационной и компьютерной безопасности», — добавляет г-жа Буглова.

Впервые о необходимости реагирования на угрозы компьютерной безопасности, вредоносных кибератак и любых потенциальных уязвимостей, с которыми могут быть сопряжены цифровые технологии, а также о важности обеспечения компьютерной безопасности в интересах физической ядерной безопасности было заявлено в резолюции по физической ядерной безопасности, принятой Генеральной конференцией МАГАТЭ в 2011 году во время ее 55-й очередной сессии. В резолюции были отмечены усилия Агентства «по повышению осведомленности о растущей угрозе кибератак и их возможных последствиях для физической ядерной безопасности». В ней содержался также призыв к МАГАТЭ в интересах оказания государствам-членам помощи в защите от кибератак разработать соответствующие руководящие документы и организовать учебные курсы и дальнейшие совещания экспертов, посвященные кибербезопасности на ядерных установках.

«Во исполнение принятой в 2011 году резолюции Генеральной конференции деятельность МАГАТЭ направлена на совершенствование средств компьютерной безопасности как на уровне государств, так и на уровне отдельных установок», — говорит г-жа Буглова. Она отмечает, что эта деятельность впоследствии получила отражение в разработанных МАГАТЭ планах по физической ядерной безопасности, включая более подробную информацию о текущей деятельности МАГАТЭ в области компьютерной безопасности, которая содержится в Плане по физической ядерной безопасности на 2022–2025 годы.

Как МАГАТЭ помогает странам развивать или совершенствовать их программы компьютерной безопасности?

Одним из основных элементов защиты стран от кибератак на критически важную инфраструктуру любого типа является создание надежной и современной программы компьютерной безопасности. МАГАТЭ оперативно оказывает странам помощь на всех этапах разработки национальных программ информационной и компьютерной безопасности, включая предоставление руководящих документов и подготовку кадров.

Рекомендации по вопросам информационной и компьютерной безопасности представлены в четырех публикациях категории руководящих материалов из Серии изданий МАГАТЭ по физической ядерной безопасности и в трех дополнительных технических публикациях. Эти руководящие материалы могут быть использованы в качестве основы для разработки национальных концепций компьютерной безопасности, включая национальные стратегии, а также норм компьютерной безопасности и соответствующих учебных курсов.

Одним из ключевых принципов руководящих материалов МАГАТЭ является сохранение критических важных функций ядерных установок посредством защиты информационных и компьютерных систем для поддержания безопасной и защищенной среды как для работы установок, так и для обращения с материалами. Это достигается за счет разработки программы компьютерной безопасности (см. стр. 6); закрепления обязанностей по обеспечению физической ядерной безопасности; использования принципов риск-менеджмента для определения потенциальных последствий нарушения безопасности; определения необходимого уровня компьютерной безопасности для защищаемых цифровых активов; а также реализации дифференцированного подхода и принципов глубокоэшелонированной защиты в отношении компьютерной безопасности. Эти элементы необходимо разрабатывать и реализовывать так, чтобы не допустить нарушения безопасности и способствовать расширению возможностей оператора по обнаружению и реагированию на вмешательства, а также смягчению возможных последствий кибератак.

МАГАТЭ по запросу стран предоставляет разнообразные возможности обучения для различных категорий слушателей. Среди них представители компетентных органов, операторов, поставщиков и других организаций, на которых могут быть возложены обязанности по обеспечению компьютерной безопасности. Им могут быть полезны также экспертные знания МАГАТЭ в области организации учений по компьютерной безопасности как элемента программы по физической ядерной безопасности.

Кроме того, на учебной киберплатформе МАГАТЭ для сетевого образования и подготовки кадров в свободном доступе размещены четыре курса электронного обучения по компьютерной безопасности на английском, арабском, испанском, китайском, русском и французском языках. Доступ к ним можно получить после регистрации или используя учетную запись на портале NUCLEUS. Вскоре будет представлена также новая инновационная виртуальная учебная платформа (см. стр. 12).

Одновременно МАГАТЭ в рамках своих усилий по повышению осведомленности об угрозе кибератак и их возможных последствиях для физической ядерной безопасности содействует проведению национальных или региональных учений по компьютерной безопасности. Такие учения предусматривают различные сценарии, согласно которым чувствительная информация и компьютерные системы подвергаются прямой или косвенной угрозе в ходе атаки на системы физической защиты и электронные системы.

Деятельность МАГАТЭ в области компьютерной безопасности дополняется профильными исследованиями, которые проводятся главным образом на основе хорошо отлаженного механизма проектов координированных исследований. В последние годы начаты проекты координированных исследований с целью активизировать усилия мирового исследовательского сообщества в области информационной и компьютерной безопасности и повысить готовность к реагированию на возникающие проблемы и риски (см. стр. 18).

Что ждет нас в будущем?

Программа МАГАТЭ по обеспечению компьютерной безопасности в интересах физической ядерной безопасности постоянно развивается. Широкое применение передовых технологий и цифровых систем контроля в малых модульных реакторах и усовершенствованных реакторах, ожидаемый рост влияния ИИ и формирование виртуальной среды обучения представляют собой как проблемные области для государств, так и области оказания им расширенной помощи.

«На наших глазах страны, регулирующие органы, операторы и другие заинтересованные стороны начинают все глубже осознавать потенциальные или фактические последствия для ядерной и физической безопасности, — говорит г-жа Буглова. — Ожидаемое значительное расширение мирного применения ядерных технологий, в частности ядерной энергетики, диктует необходимость рассматривать информационную и компьютерную безопасность в качестве неотъемлемой составляющей физической ядерной безопасности».

Кибератака

Термин «кибератака» используется для описания злоумышленного действия с целью похитить, изменить или уничтожить определенные объекты или препятствовать доступу к ним посредством несанкционированного проникновения в уязвимую компьютерную систему (либо действий внутри нее). Кибератаки ставят под угрозу конфиденциальность, целостность или доступность (либо сочетание этих свойств) важной информации в рамках защищаемого цифрового актива, или же собственно защищаемого цифрового актива, и могут быть использованы для совершения или содействия в совершении злоумышленного действия в отношении установки или деятельности, равно как и иного преступного или преднамеренного несанкционированного действия с использованием ядерного или другого радиоактивного материала.

Кибератака может осуществляться — за счет прямого физического доступа к информации или информационным активам или электронного доступа, а также их сочетания — непосредственно злоумышленником или инсайдером (либо с его помощью), который сознательно или неосознанно находится под влиянием злоумышленника.

Кибератаки после обнаружения должны рассматриваться как инциденты, связанные с компьютерной безопасностью.

Данное определение заимствовано из публикации «Computer Security for Nuclear Security» («Обеспечение компьютерной безопасности в интересах физической ядерной безопасности») (IAEA Nuclear Security Series No. 42-G).

Что нужно для разработки программы компьютерной безопасности

Василики Тафили и Трент Нельсон

Объекты, на которых используется ядерный или иной радиоактивный материал и ведется соответствующая деятельность, входят в состав критически важной инфраструктуры, на которой необходимо обеспечивать высокий уровень ядерной и физической безопасности. Применяя комплексный и инициативный подход к компьютерной безопасности, организации могут защитить активы чувствительной информации и компьютерные системы на этих объектах. МАГАТЭ рекомендует практиковать подход к компьютерной безопасности, заключающийся в том, что государства устанавливают требования к национальной стратегии или политике и способствуют обеспечению конфиденциальности и защиты чувствительной информации и компьютерных систем, связанных с физической защитой, ядерной безопасностью, учетом и контролем ядерного материала. Эти требования могут также быть оформлены в виде национальных регулирующих положений, которые предусматривают разработку и внедрение программы обеспечения компьютерной безопасности (ПКБ)*.

ПКБ — это всеобъемлющая структура, включающая ключевые элементы эффективного плана осуществления политики и процедур компьютерной безопасности, которые будут использоваться на протяжении всего срока эксплуатации ядерной установки или установки с радиоактивными источниками. Ее целью является защита активов чувствительной информации и компьютерных систем, критически важных для поддержания функций ядерной и физической безопасности, от киберугроз для смягчения последствий кибератак.

Национальная стратегия

Комплексная и эффективная стратегия компьютерной безопасности требует системного подхода, который объединяет различные элементы, включая нормативные акты, программы, меры защиты и безопасности и потенциал реагирования для поддержания национальных режимов физической ядерной безопасности.

Регулирующие положения

Эффективные регулирующие положения обеспечивают правовую основу для защиты чувствительных компьютерных систем и наличие у организаций ПКБ с надлежащими механизмами контроля.

Ключевые элементы ПКБ

Функции и обязанности

Организационные функции и обязанности, а также структура подотчетности принципиально важны для эффективного управления, особенно в случае критической инфраструктуры. Четкое понимание организационной иерархии, распределения полномочий и структуры отчетности необходимы для эффективного и результативного сотрудничества и синергетического взаимодействия в рамках ПКБ.

Управление рисками, контроль факторов уязвимости и обеспечение соответствия нормативным требованиям

Управление рисками в области компьютерной безопасности включает оценку факторов уязвимости и потенциальных последствий, связанных с чувствительными цифровыми активами и компьютерными системами, для внедрения средств компьютерной безопасности на основе дифференцированного подхода с целью защиты от кибератак. Уровень применяемых мер безопасности должен быть соизмерим с уровнем угроз для защищаемой информации и/или компьютерных систем. Организации могут корректировать уровень мер безопасности, необходимых для снижения риска, с учетом возможных последствий реализации рисков или угроз.

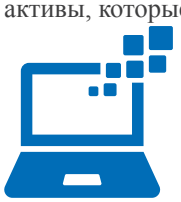
Разработка мер безопасности и управление ими

Структура системы компьютерной безопасности — важнейший аспект защиты от киберугроз. Основные принципы построения такой системы — дифференцированный подход и глубокоэшелонированная защита, когда противодействие атакам ведется на

нескольких рубежах безопасности. Требования к физической безопасности также должны выполняться на всех этапах процесса разработки системы, в том числе сторонними организациями, которые должны соблюдать четко сформулированные принципы и договоренности для обеспечения последовательности и эффективности мер физической безопасности.

Управление цифровыми активами

Эффективное обеспечение компьютерной безопасности сложно представить без системного подхода к составлению полного перечня всех функций, активов и систем объекта, включая чувствительные цифровые активы, которые необходимы для защиты ядерной



деятельности и для обеспечения безопасного и надежного использования ядерного и другого радиоактивного материала. Такой перечень также дает представление о потоках данных и взаимосвязях, которое необходимо организации для организации контроля доступа, резервного копирования и других мер безопасности, направленных на защину активов от саботажа или хищения.

Процедуры обеспечения физической безопасности

Оперативная политика и процедуры обеспечения физической ядерной безопасности распределяют ответственность за предотвращение хищения, саботажа или несанкционированного использования ядерного материала и установок. Эти процедуры предусматривают жесткий контроль доступа к конфиденциальной информации и активам, а также отбор и соответствующее обучение лиц, имеющих доступ.

Управление кадрами

Особое значение при управлении кадрами в ядерной промышленности придается благонадежности

сотрудников, их квалификации и обучению. Оценка благонадежности проводится для того, чтобы убедиться: на сотрудника можно положиться, он компетентен и не вовлечен в какие бы то ни было конфликты интересов, которые могут поставить под угрозу ядерную безопасность или физическую ядерную безопасность. Укомплектование квалифицированными и благонадежными кадрами имеет решающее значение для обеспечения ядерной и физической безопасности.

**Более подробные сведения включены в публикацию «Computer Security Techniques for Nuclear Facilities» («Методы обеспечения компьютерной безопасности для ядерных установок») (IAEA Nuclear Security Series No. 17-T (Rev. 1)).*

Не только физическая защита

Как международные консультационные услуги по физической защите способствуют повышению уровня компьютерной безопасности

Василики Тафили

На протяжении уже почти тридцати лет МАГАТЭ предоставляет странам международные консультационные услуги по физической защите (ИППАС), в рамках которых выносятся рекомендации по обеспечению физической защиты всех типов объектов, на которых используются ядерные и другие радиоактивные материалы, включая атомные электростанции и радиотерапевтические установки в больницах. Однако технический прогресс не стоит на месте, и сегодня цифровые системы играют в работе этих объектов важнейшую роль. Это вызвало множество новых проблем в области физической ядерной безопасности.

В ответ на реальную угрозу кибератак на объекты, включая ядерные установки, в 2012 году в сферу компетенции ИППАС была включена информационная и компьютерная безопасность для физической защиты. С тех пор страны все чаще запрашивают этот модуль в рамках ИППАС, стремясь поддержать свою работу по противодействию угрозам в области кибербезопасности.

ИППАС — ключевой компонент программы МАГАТЭ по физической ядерной безопасности, который помогает странам в проведении анализа существующей практики с точки зрения соответствующих международных документов и руководящих материалов МАГАТЭ по физической ядерной безопасности. Эксперты, участвующие в миссиях ИППАС, помогают странам, обратившимся с такой просьбой, в совершенствовании национальных режимов, систем и мер физической ядерной безопасности, предоставляя консультации по осуществлению положений международно-правовых документов.

«После первой миссии ИППАС прошло 27 лет, и за это время услуги эволюционировали с учетом актуальных задач и потребностей, — говорит Хизер Луни, руководитель Секции физической ядерной безопасности материалов и установок Отдела физической ядерной безопасности МАГАТЭ. — Физическая защита от кражи, саботажа и несанкционированного использования ядерных и других радиоактивных материалов не может быть обеспечена без мер кибербезопасности. Пригласив миссию ИППАС, страны могут получить рекомендации о том, что и как можно усовершенствовать».

Миссии ИППАС включают пять модулей, в рамках которых проводится анализ следующих аспектов: национального режима физической ядерной безопасности ядерного материала и ядерных установок; систем и мер физической безопасности, принимаемых на ядерных объектах; физической безопасности перевозки материалов; физической безопасности радиоактивного материала, связанных с ним объектов и деятельности; информационной и компьютерной безопасности. В общей сложности после первой миссии ИППАС, проведенной в 1996 году, на сегодняшний день было организовано 97 миссий, и 22 страны обратились с просьбой включить модуль информационной и компьютерной безопасности в услуги ИППАС.

Чего следует ожидать стране в ходе оценки информационной и компьютерной безопасности?

На первом этапе группа международных экспертов по физической ядерной безопасности в составе миссии ИППАС изучает, как разрабатывались и осуществлялись национальные стратегии, связанные с программами информационной и компьютерной безопасности. Затем группа рассмотрит законодательную и нормативную базу, сопоставив действующие в стране процедуры и сложившуюся практику с обязательствами, предусмотренными Конвенцией о физической защите ядерного материала и поправкой к ней 2005 года, а также с руководящими указаниями, содержащимися в соответствующих публикациях Серии изданий МАГАТЭ по физической ядерной безопасности. Таким образом они установят, имеются ли в стране необходимые стратегии и процедуры для обеспечения должного уровня кибербезопасности на критически важных ядерных и радиологических установках.

На уровне установки в ходе проверки компьютерной безопасности будут проанализированы такие аспекты, как управление компьютерной безопасностью, программа компьютерной безопасности (см. стр. 6), механизмы контроля доступа, защитная архитектура компьютерной безопасности, а также обнаружение событий, связанных с компьютерной безопасностью, и реагирование на них. Группа может также провести оценку в смежных областях, таких как управление рисками, дифференцированные подходы, культура физической ядерной безопасности и управление людскими ресурсами.

Япония приняла миссию ИППАС в 2015 году, а повторную миссию ИППАС — в 2018 году. «Для Японии опыт проведения анализа текущего положения дел в области компьютерной безопасности и содействия совершенствованию в этой сфере на основе предложений рецензентов оказался весьма ценным, — считает

С 1996 года в рамках международных консультационных услуг по физической защите (ИППАС) странам оказывается помощь в определении способов укрепления защиты ядерных материалов и установок. (Фото: МАГАТЭ)

Хироюки Сугавара, директор по международным проблемам физической ядерной безопасности Отдела физической ядерной безопасности Управления ядерного регулирования (УЯР) Японии. — Реагируя на выводы ИППАС, мы решили усилить меры компьютерной безопасности и увеличить число инспекторов с опытом работы в этой области. Кроме того, УЯР включила угрозы компьютерной безопасности в свою национальную оценку угроз и потребовала от лицензиатов принимать надежные меры компьютерной безопасности, а также доработать свои планы компьютерной безопасности, включив в них меры противодействия кибератакам».

Во Франции по итогам организованной в 2018 году миссии ИППАС в национальной системе физической ядерной безопасности была повышена значимость компьютерной безопасности. «Миссия ИППАС потребовала от различных заинтересованных сторон значительных усилий и открыла возможности для укрепления во Франции режима физической ядерной безопасности, а также стимулировала принятие конкретных мер в этой области, — отмечает Фредерик Боен, руководитель проектов по компьютерной безопасности в Отделе физической ядерной безопасности Департамента обороны и безопасности Министерства экологии Франции. — Был увеличен штат сотрудников, занимающихся вопросами компьютерной безопасности, также были разработаны нормативные документы, соответствующие международным нормам и руководящим материалам МАГАТЭ по физической ядерной безопасности».

МАГАТЭ делится результатами таких миссий с международным сообществом специалистов по физической ядерной безопасности и в этих целях с 2016 года ведет базу данных по передовой практике ИППАС — это позволяет усилить отдачу от помощи, которую Агентство оказывает странам по всему миру. «Ведение этой базы данных и обмен информацией о примерах оптимальной практики позволяет извлекать пользу из миссий ИППАС не только принимающей стране, но и всему международному сообществу по ядерной безопасности и усиливает положительный эффект помощи, которую МАГАТЭ оказывает своим государствам-членам», — убеждена г-жа Луни.

Большинство примеров передовой практики на уровне государства относятся к управлению физической ядерной безопасностью, которое обеспечивает основу для кибербезопасности и координации. Кроме того, существует 40 примеров передовой практики, относящихся к компьютерной безопасности как на уровне государства, так и на уровне установки, информацию о которых государства — члены МАГАТЭ могут получить в назначенных пунктах связи.

МАГАТЭ продолжает оказывать странам содействие в укреплении национального режима физической ядерной безопасности; интерес стран к проведению в 2023 и 2024 годах миссий ИППАС остается высоким.

МАГАТЭ помогает странам Африки в разработке норм в области компьютерной безопасности

Андреа Рахандини

Ожидается, что в ближайшем будущем спрос на радиоизотопы в Африке будет расти по мере того, как страны континента будут расширять мирное использование ядерных технологий. Рост заболеваемости раком привел к увеличению спроса на лучевую терапию, радиологию и ядерную медицину. Расширяется применение ядерных технологий в промышленности, сельском хозяйстве и науке. В результате повышается спрос на производство радиоизотопов в исследовательских реакторах. В эксплуатации этих крайне необходимых реакторов применяются компьютерные системы, которые могут быть уязвимы для кибератак. Как и атомные электростанции, исследовательские реакторы являются ядерными установками, которым необходимы планы по защите для предотвращения злоумышленных действия, смягчения их последствий и реагирования на них. Защита всех типов ядерных установок от возможных атак — важное условие безопасного и надежного применения ядерных технологий в Африке.

Стремясь нейтрализовать эти угрозы, многие страны Африки изучают опыт Египта, Ганы и Нигерии — каждая из этих стран эксплуатирует собственный исследовательский реактор. При поддержке МАГАТЭ эти три страны разрабатывают и совершенствуют нормы компьютерной безопасности и реализуют программы по надлежащей защите своих установок от совершаемых с помощью компьютерных систем злоумышленных действий, которые могут оказать негативное воздействие на физическую ядерную безопасность и защищенность установок.

«Важность компьютерной безопасности продолжает расти по мере того, как цифровые и компьютерные технологии все глубже интегрируются в системы обеспечения ядерной и физической безопасности и эксплуатации установок и объектов, связанных с ядерными и другими радиоактивными материалами, — говорит Трент Нельсон, старший специалист по информационной и компьютерной безопасности в Отделе физической ядерной безопасности МАГАТЭ. — МАГАТЭ помогает странам Африки разрабатывать, пересматривать и совершенствовать нормы в области компьютерной безопасности».

В Египте МАГАТЭ сотрудничает с Управлением по ядерному и радиологическому регулированию (УЯРРЕ) в проведении анализа действующих норм компьютерной безопасности и устранении слабых мест в системах регулирования. В 2022 году были организованы национальные учебные курсы для укрепления национального потенциала по проведению инспекций компьютерной безопасности на ядерных установках. Слушатели курсов, которые вобрали в себя руководящие материалы МАГАТЭ по физической ядерной безопасности и методы, доступные инспекторам, вооружились знаниями и практическим опытом, которые позволят им лучше оценивать уровень компьютерной безопасности на ядерных и радиологических установках.

Надя М. Наввар, компьютерный инженер на установке по производству радиоизотопов Управления по атомной энергии Египта (УЯЭЕ), была в числе 22 слушателей этих курсов. «Я узнала, каким образом регулирующий орган проводит проверки компьютерной безопасности и какие необходимые меры компьютерной безопасности должны быть приняты оператором, — говорит она. — Благодаря участию в курсах мы можем более эффективно анализировать и валидировать элементы норм компьютерной безопасности. Курсы помогли нам разработать и внедрить программу компьютерной безопасности, чтобы защитить конфиденциальную информацию установки и цифровые активы, уязвимые для кибератак».

В апреле 2023 года МАГАТЭ направило в Гану миссию экспертов для оценки действующих национальных норм компьютерной безопасности и программы инспекций, реализуемой Управлением по ядерному регулированию Ганы (УЯРГ).

«В ходе разработки системы компьютерной безопасности в Гане мы столкнулись с рядом проблем, в том числе связанных с нехваткой в стране технических экспертов в этой области, взаимосвязью между юридическими вопросами и техническим ноу-хау, а также изысканием необходимых ресурсов, — рассказывает Нельсон Кодзоце Агбемава, руководитель группы в Отделе ядерной кибербезопасности УЯРГ. — В ходе разработки нормативных документов мы обратились к МАГАТЭ и другим странам за экспертной поддержкой с целью обеспечения комплексного и системного подхода к компьютерной безопасности».

В октябре 2022 года МАГАТЭ также направило аналогичную миссию экспертов в Нигерию. «Необходимость в эффективной законодательной и

В августе 2023 года начнет работу Школа МАГАТЭ по подготовке элементов нормативных актов в области компьютерной безопасности, которая призвана помочь странам в разработке собственных национальных норм компьютерной безопасности.

нормативной основе для обеспечения компьютерной безопасности была выявлена в 2019 году в ходе обзора Комплексного плана поддержки физической ядерной безопасности (КППФЯБ), проведенного под руководством МАГАТЭ, — говорит Этель Офоэгбу, главный специалист по вопросам регулирования Нигерийского управления по ядерному регулированию (НУЯР). — Впоследствии МАГАТЭ провело оценку национальных норм компьютерной безопасности, выявило слабые места и предоставило необходимые консультации. Одним из результатов стала разработка проекта норм компьютерной безопасности Нигерии для ядерных и радиологических установок и связанной с ними деятельности». В настоящее время Нигерия рассматривает проект нормативных документов и планирует организовать учебные курсы по проверкам компьютерной безопасности.

Принимая во внимание рост числа запросов на оказание помощи, поступающих от стран, МАГАТЭ разрабатывает технический документ, который поможет странам сформировать ключевые элементы норм компьютерной безопасности. МАГАТЭ также будет готово помочь многим другим странам в разработке нормативных актов в области компьютерной безопасности, когда в августе 2023 года начнет работу Школа МАГАТЭ по подготовке элементов нормативных актов в области компьютерной безопасности. Школа призвана помочь в разработке конкретных национальных норм компьютерной безопасности нескольким странам сразу, вместо того, чтобы оказывать помощь силами МАГАТЭ отдельным странам по очереди. После первого семинара-практикума, который состоится в августе, сессии Школы будут проводиться во всех регионах раз в полгода. Слушателям будет оказана помощь в разработке национальных стратегий в области компьютерной безопасности — нормативной основы надежной программы компьютерной безопасности.

Инновации в области подготовки персонала ядерных и радиологических установок по вопросам компьютерной безопасности в виртуальном формате

Аньярика Штроаль

Наша жизнь быстро и существенно меняется в результате повсеместного и все более активного применения современных цифровых технологий. Существующая критически важная инфраструктура, к которой относится ядерная энергетика и другие виды мирного использования ядерных технологий, в значительной степени зависит от цифровых технологий для обеспечения бесперебойной и надежной работы. Перспективы, которые открываются вместе с быстрым развитием новых технологий, таких как искусственный интеллект, в области решения проблем и улучшения цифрового управления операциями, вероятно, будут способствовать совершенствованию ядерных применений. Эти технологии уже сегодня используются или учитываются в конструкциях усовершенствованных реакторов.

К сожалению, хотя эти цифровые технологии приносят много преимуществ, они могут также порождать много потенциальных и неизвестных факторов уязвимости. Это связано с постоянно существующей угрозой проникновения хакеров или злонамеренных кибератак на ядерные установки с помощью тех же самых технологий.

Количество и разнообразие все более изощренных кибератак вызывает у ядерной отрасли острую потребность в подготовке персонала ядерных и радиологических установок в области компьютерной безопасности. Чтобы помочь удовлетворить этот возникший спрос, МАГАТЭ разработало серию учебных курсов, посвященных широкому спектру тем — от основ компьютерной безопасности до более совершенных видов компьютерной безопасности, используемых в системах контроля и управления.

В ходе проведения этих специализированных, технических, сложно организованных учебных курсов, которые включают в себя также практические занятия, МАГАТЭ выявило необходимость наличия простой онлайн-платформы, которая могла бы стандартизировать учебную программу и обеспечить ее более широкое и универсальное использование учебными заведениями без необходимости личного присутствия сотрудников МАГАТЭ для оказания помощи. Эта потребность стала особенно актуальной в свете ограничений на поездки в связи с пандемией COVID-19 и распространившегося использования виртуальных технологий, в результате чего разработка платформы была ускорена.

Виртуальный инструмент обучения, который называется «Learners», призван сделать учебные курсы по компьютерной безопасности гибкими и увлекательными для представителей ядерного сообщества за счет предлагаемых учебных материалов и опыта практических занятий, которые организуются в виртуальной среде. Участникам нужен только компьютер и надежное подключение к интернету, чтобы получить доступ ко всем необходимым материалам курса. «Ожидается, что новая платформа будет играть ключевую

Подготовка по вопросам компьютерной безопасности
и другие мероприятия

194 мероприятия

120 государств-членов получили поддержку

2676 участников

3 проекта координированных исследований

14 совещаний экспертов

24 учебных курса

12 технических совещаний или семинаров-практикумов

10 вебинаров

66 консультативных совещаний (разработка учебной программы, руководство, подготовительные совещания)

роль в повышении осведомленности о компьютерной безопасности и улучшении подготовки в интересах обеспечения физической ядерной безопасности, создании более сплоченного сообщества экспертов и содействии повышению ядерной и физической безопасности на ядерных установках и объектах, связанных с радиоактивными материалами», — отмечает директор Отдела физической ядерной безопасности МАГАТЭ Елена Буглова.

С июня 2023 года МАГАТЭ сделает платформу «Learners» доступной во всем мире, чтобы повысить компьютерную безопасность на ядерных установках и связанных с радиоактивными источниками объектах, а также при осуществлении соответствующих видов деятельности.

Австрийский технологический институт (АТИ) — центр сотрудничества МАГАТЭ по вопросам информационной и компьютерной безопасности в целях обеспечения физической ядерной безопасности — создал платформу «Learners» в партнерстве с МАГАТЭ.

«Виртуальная учебная среда открывает огромные возможности для укрепления оперативного и стратегического потенциала за счет оказания поддержки различным видам подготовки и обучения, — говорит Гельмут Леопольд, руководитель Центра цифровой безопасности и физической безопасности АТИ. — Моделируя реальные условия, платформа позволяет учащимся приобрести практические навыки и опыт, которые необходимы для эффективного управления физической ядерной безопасностью».

Обучение в целях повышения уровня компьютерной безопасности

Платформа МАГАТЭ «Learners» предоставляется по запросу для дополнения программы подготовки в области физической ядерной безопасности. Платформа разработана с учетом международной аудитории и предлагает многоязычную поддержку, чтобы обеспечить удобство для всех пользователей. Она содержит различные функциональные элементы, такие как упражнения с пошаговыми инструкциями, мгновенная обратная связь, интеграция презентаций и поддержка многоэкранного режима. Это делает платформу гибкой и доступной для использования учебными учреждениями и непосредственными пользователями.

«Learners» задумана как платформа для разработки, формирования и использования интерактивных имитационных условий, созданных при помощи технологий с открытым исходным кодом. Дополнительные модули включают стандартизированные подходы к вычислительным платформам, подготовке инфраструктуры и конфигурации программного обеспечения, что позволяет легко обмениваться знаниями с существующими учебными учреждениями — партнерами МАГАТЭ и другими организациями, желающими использовать платформу.

Было подготовлено двенадцать практических упражнений, организованных в шесть тематических областей на основе руководящих материалов по обеспечению компьютерной безопасности в интересах физической ядерной безопасности. «Благодаря использованию виртуализованной среды, имитирующей реальные объекты, платформа "Learners" подкрепляет развитие практических навыков и обеспечивает более справедливый доступ к знаниям и профессиональным навыкам», — добавляет г-жа Буглова.

Платформа «Learners» является одним из направлений работы МАГАТЭ по повышению осведомленности, укреплению сотрудничества и оказанию государствам поддержки в борьбе с растущими угрозами кибербезопасности в ядерном секторе. В течение последних 5 лет деятельность по созданию потенциала осуществлялась в более чем 120 странах. Кроме того, адресная помощь посредством организации миссий экспертов, национальных, региональных и международных учебных курсов, технических совещаний и вебинаров способствовала налаживанию активного сотрудничества, обмена знаниями и развитию навыков. Помимо этого, МАГАТЭ оказывает поддержку странам в организации крупномасштабных учений по кибербезопасности.

Учебно-демонстрационный центр на практике

В будущем крайне важно вкладывать средства в подобные инициативы по созданию потенциала, чтобы обеспечить высочайшие стандарты физической ядерной безопасности во всем мире. Современный Учебно-демонстрационный центр по физической ядерной безопасности (УДЦФЯБ) откроется во второй половине 2023 года, чтобы помочь укрепить возможности стран в борьбе с ядерным терроризмом за счет приобретения практического опыта в ходе обучения. Предлагаемые в УДЦФЯБ инновационные учебные курсы будут охватывать темы, связанные с компьютерной безопасностью, и включать в себя сценарии кибератак, которые потенциально могут быть направлены на ядерные установки или объекты и виды деятельности, связанные с радиоактивными источниками.

Мероприятия в разбивке по регионам

Как искусственный интеллект изменит представление об информационной и компьютерной безопасности в ядерной сфере

Митчелл Хьюз

Искусственный интеллект (ИИ) и технологии машинного обучения потенциально способны произвести революцию в мире выступая в качестве двигателя беспрецедентного прогресса и инноваций и меняя наш подход к созданию, потреблению и использованию информации. Технологии ИИ будут становиться все более совершенными, что будет приводить к трансформации целых отраслей, позволит оптимизировать различные процессы и даже может повлиять на наш образ жизни. Ядерный сектор не является здесь исключением, и можно ожидать, что преимущества ИИ найдут применение во многих процессах и операциях на ядерных и радиологических установках.

В то же время, стремительное развитие ИИ порождает массу различных рисков. Злоумышленники могут задействовать ИИ для организации более изощренных и целенаправленных атак или использовать его уязвимости для нарушения целостности компьютерных сетей или систем и доступа к закрытой информации на ядерных и радиологических установках.

Выгоды с точки зрения информационной и компьютерной безопасности

МАГАТЭ готовится к грядущим переменам, обусловленным распространением ИИ, укрепляя международное сотрудничество в этой области, чтобы все страны могли воспользоваться открывающимися возможностями и в то же время принять меры к смягчению рисков. Опираясь на такие механизмы сотрудничества, как технические совещания и проекты координированных исследований (ПКИ), МАГАТЭ поддерживает разработку и применение методов ИИ с учетом их особенностей, а также поиск контрмер и способов защиты от злоумышленников.

Возможно, самым значительным преимуществом ИИ в плане информационной и компьютерной безопасности является снижение зависимости от анализа оператором и необходимости его вмешательства. Системы с поддержкой ИИ могут работать круглосуточно и без выходных, выполняя мониторинг компьютерных сетей и систем на наличие угроз. Благодаря автоматизации этих задач у специалистов по физической ядерной безопасности появляется время для того, чтобы сосредоточиться на задачах более стратегического характера и эффективнее реагировать на инциденты, как только они произошли.

«Возможности ИИ в плане адаптивного обучения могут быть использованы для повышения информационной и компьютерной безопасности за счет быстрого выявления угроз и автоматического предоставления экспертам-людям необходимой информации для координации действий по реагированию, — рассказывает доцент Технологического института Джорджии в Соединенных Штатах Америки Фань Чжан, который участвовал в ПКИ, призванном поддержать исследования в области укрепления компьютерной безопасности. — Это не заменит штатных работников, а скорее позволит формировать ресурсы и аналитические выкладки, благодаря которым действия по раннему обнаружению и реагированию в области компьютерной безопасности станут реально осуществимыми».

Используя передовые алгоритмы машинного обучения, ИИ поможет также повысить эффективность защиты от кибератак на ядерных и радиологических установках за счет выявления аномальных данных в компьютерных системах. Оснащенные элементами ИИ системы безопасности могут непрерывно отслеживать и анализировать огромное количество данных, чтобы определить, является ли какая-либо активность аномальной на фоне нормальной эксплуатации установки. Кибератаки могут предусматривать передачу поддельных данных, чтобы предумышленно ввести в заблуждение операторов ядерных установок. В этом случае системы с элементами ИИ могут использоваться для предупреждения сотрудников, отвечающих за управление атомной электростанцией, о малейших отклонениях от нормальной эксплуатации. Создавая предпосылки для повышенной ситуационной осведомленности, ИИ также обеспечивает возможность раннего обнаружения преступных действий и подсказывает необходимые шаги для реагирования на инциденты.

Проблемы, требующие решения

Преимущества, которые дает применение ИИ на ядерных и радиологических установках, в значительной степени зависят от того, как было выполнено обучение систем ИИ. ИИ сведущ только в тех пределах, в которых представлены обучающие данные для его работы, и если он не располагает правильными исходными данными, им можно манипулировать, чтобы получать ложные показания и результаты. Это остается серьезным препятствием на пути к его применению в сфере физической ядерной безопасности. Даже с учетом последних достижений в технологии ИИ, использовать его в качестве замены человека не представляется целесообразным. Физическая защита, учет и контроль материалов и непосредственные измерения — все эти важнейшие направления работы для

обеспечения физической ядерной безопасности требуют участия человека.

Еще одной проблемой, связанной с применением ИИ в сфере физической ядерной безопасности, является понимание того, как и почему моделью ИИ было принято то или иное решение или выдан определенный прогноз. «Одними из самых значительных проблем с моделями ИИ являются их прозрачность и объяснимость — то есть когда люди могут понять логику предложенных ИИ решений или прогнозов. Часто бывает трудно понять, как эти модели приходят к тому, чтобы представить свои выводы, и это усложняет вопрос о доверии к таким результатам и обеспечении их достоверности, — говорит начальник Секции управления информацией Отдела физической ядерной безопасности МАГАТЭ Скотт Первис. — Это становится особенно проблематичным, когда эти модели заменяют собой датчики, предназначенные для непосредственных измерений, и человеческий опыт, накапливаемый с учетом уникальных характеристик каждой установки. Из-за этого становится практически невозможным дать какие-либо гарантии целостности системы, если нет предварительного глубокого и всестороннего понимания алгоритмов ИИ, чтобы представлять, как и почему принимаются соответствующие решения».

Руководящие материалы МАГАТЭ по обеспечению компьютерной безопасности в интересах физической ядерной безопасности включают в себя примеры положительной практики, касающейся системы сдержек и противовесов с участием человека, и дают операторам установок рекомендации о том, какие процессы могут быть автоматизированы за счет ИИ, а какие должны и далее оставаться под надзором человека, по крайней мере, до тех пор, пока не будут изучены риски, связанные с этой быстро развивающейся технологией. Они также являются важным ресурсом, который может служить подспорьем для стран при реализации первоочередных мер компьютерной безопасности для обнаружения кибератак, их предотвращения и реагирования на них.

Кроме того, МАГАТЭ разработало ПКИ для поддержки исследовательских работ в области укрепления компьютерной безопасности. Соответствующий ПКИ под названием «Совершенствование анализа инцидентов в сфере компьютерной безопасности на ядерных установках» объединил усилия исследователей из 13 стран, работающих над совершенствованием средств компьютерной безопасности на ядерных установках, включая методы на основе ИИ, в целях выявления аномалий, являющихся признаком целенаправленных кибератак.

Гонка технологий, связанных с внедрением ИИ

ИИ продемонстрировал свою способность приносить пользу там, где ядерные технологии используются в мирных целях. По мере того, как он все чаще находит

ИИ может также повысить эффективность защиты от кибератак на ядерных и радиологических установках за счет выявления аномальных данных в компьютерных системах. (Изображение: AdobeStock)

применение для улучшения процессов и операций на ядерных и радиологических установках, должна также расти и осведомленность о рисках, обусловленных его широким внедрением. Реализуя на практике преимущества ИИ, организации должны предусмотреть надежную программу обеспечения компьютерной безопасности в интересах физической ядерной безопасности.

Для этого требуется фундаментальная смена парадигмы, определяющей наши взгляды на аспекты доверенности и секретности. Необходимо учитывать каждую потенциальную точку отказа в системе, включая даже те, которые не связаны с ее системной архитектурой. Злоумышленники могут использовать ИИ для создания более изощренного вредоносного ПО, автоматизации кибератак, вскрытия систематических ошибок и уязвимостей в моделях или обхода мер безопасности путем имитации поведения добропорядочных пользователей. Эта гонка вооружений между защищающимися и нападающими будет требовать постоянных инноваций и адаптации к новым реалиям.

Более широкое внедрение технологий ИИ для укрепления мер компьютерной безопасности на ядерных установках может дать значительные преимущества, включая более эффективное обнаружение угроз, применение упреждающих мер безопасности, снижение зависимости от вмешательства оператора и улучшение реагирования на инциденты. Используя преимущества искусственного интеллекта и одновременно нейтрализуя его риски, организации могут значительно повысить свой уровень компьютерной безопасности перед лицом эволюционирующих киберугроз.

Как учения по компьютерной безопасности помогают повысить готовность к реагированию на кибератаки в сфере физической ядерной безопасности

Эмма Миджли

Исторически сложилось так, что на ядерных объектах основное внимание уделялось защите ядерного материала от злоумышленных действий путем принятия мер физической защиты — вооруженной охраны и контроля доступа. Эти меры и сейчас широко применяются, чтобы превратить ядерный объект в крепость и не допустить хищение ядерного или другого радиоактивного материала, саботаж или несанкционированный доступ к системам контроля. Однако в последние десятилетия в условиях продолжающейся цифровизации угроза кибератак существенно возросла. Любая страна, даже та, которая реализует самые передовые программы в области ядерной энергии и исследований, может быть уязвима для нападения. Возникла необходимость разработки национальных систем компьютерной безопасности и реагирования на киберугрозы применительно к ядерным объектам. С помощью масштабных учений МАГАТЭ помогает странам усилить защиту от кибератак и усовершенствовать стратегии обнаружения кибератак против ядерных объектов и реагирования на них.

МАГАТЭ разработало учения по компьютерной безопасности для атомных электростанций и радиологических установок, которые проводятся на национальном уровне по всему миру. Эти учения позволяют странам попрактиковаться и подготовить ответные меры при худшем сценарии нарушения кибербезопасности на ядерном объекте. Теоретические сценарии позволяют выявить слабые места в политике, процедурах и процессах, а также слабые места, которые необходимо устранить с помощью корректирующих мер, укрепления потенциала и/или организационных изменений. Помимо помощи государствам в проведении крупномасштабных учений по компьютерной безопасности на ядерных объектах, МАГАТЭ подготовило руководящие материалы по обеспечению компьютерной безопасности в интересах физической ядерной безопасности — это также важный ресурс, который может служить подспорьем для стран при принятии важных мер компьютерной безопасности для обнаружения кибератак, их предотвращения и реагирования на них.

«Очень важно разработать политику, сформулировать роли и обязанности, а также подробные процедуры реагирования на инциденты в области компьютерной безопасности до того, как такой инцидент произойдет, — считает Трент Нельсон, старший специалист по информационной и компьютерной безопасности в Отделе физической ядерной безопасности МАГАТЭ. — Именно здесь МАГАТЭ может помочь во многих вопросах: от учений и руководящих материалов до обмена передовым опытом и процедурами для обеспечения эффективной коммуникации и физической безопасности».

К факторам, повышающим уязвимость ядерных объектов к кибератакам, относятся человеческий фактор, многосоставные цепочки поставок и конфиденциальный характер информации, доступ к которой имеют различные пользователи компьютерных систем, обеспечивающих ядерную деятельность.

«Рассмотрим направленную на подрядчика атаку, организаторы которой подделали заказ-наряд, чтобы пользующийся доверием и имеющий необходимый доступ технический специалист совершил ошибочное действие, — предлагает Трент Нельсон. — Это лишь один из способов, с помощью которых злоумышленники могут обойти систему безопасности».

Важным элементом снижения негативных последствий любой кибератаки является информированность заинтересованных пользователей и эффективное взаимодействие между ними, поскольку любой из таких пользователей или групп пользователей может стать мишенью злоумышленников. В организации защиты ядерных объектов участвуют четыре ключевых субъекта: регулирующий орган; оператор установки; организации технической поддержки (группы реагирования на инциденты в области компьютерной безопасности и/или операционные центры компьютерной безопасности); сторонние организации, такие как поставщики и организации поддержки. Проведение учений — хороший способ проверки коммуникации между этими субъектами и процедур отчетности и уведомления, а также проверки и подтверждения безопасности и надежности организационных структур.

В идеальном сценарии хотелось бы полностью исключить возможность доступа злоумышленников к системам компьютерной безопасности на ядерных объектах, но злоумышленники не стоят на месте, а человеческая природа несовершенна, поэтому практически невозможно

Информированность сторон и эффективное взаимодействие между ними важны для минимизации возможных последствий кибератаки. (Изображение: AdobeStock)

предсказать, какой будет следующая крупномасштабная атака. Поэтому крайне важно обеспечить оперативное обнаружение атак. Недавно в Словении были организованы учения, в ходе которых с помощью учебной кибератаки были протестированы возможности по обнаружению подобных злонамеренных действий и реагированию на них.

«Компьютерная безопасность — это не проект или процесс, но "путешествие длиною в жизнь", которое требует постоянных усилий, внимания и практики, — считает Само Томажич, руководитель отдела кибербезопасности Администрации по ядерной безопасности Словении. — Учения, подобные тем, которые были проведены в Словении, позволяют всем соответствующим субъектам ядерного сектора оценить, насколько надежны их планы реагирования на инциденты в случае успешной кибератаки».

В случае серьезного инцидента в области компьютерной безопасности, который потенциально может привести к нарушению ядерной безопасности или физической ядерной безопасности, помимо обычных заинтересованных сторон на ядерном объекте, следует привлекать группы реагирования на инциденты в области компьютерной безопасности. Такой инцидент может повлечь за собой, например, нарушение политики или процедур физической безопасности; воздействие на конфиденциальные цифровые активы или системы; потерю конфиденциальной информации и контроля над критическими функциями ядерной безопасности.

После выявления инцидента или сбоя в области компьютерной безопасности группа реагирования начинает работать с заинтересованными сторонами на объекте с целью расследования инцидента, сбора криминалистических данных, анализа того, что и где произошло, и оказания помощи в ограничении и недопущении несанкционированного доступа, чтобы помочь операторам вернуть ядерный объект в рабочее состояние. Затем проводится сбор данных компьютерной криминалистики, которые необходимы для расследования кибератаки и обеспечения эффективного обмена информацией для дальнейшего усиления мер компьютерной безопасности на ядерном объекте в будущем.

На учениях, проведенных в Словении, обнаружение кибератак было необходимо для того, чтобы иметь возможность отреагировать на гипотетический инцидент в области безопасности и проверить на практике процедуры реагирования на инциденты. Эти учения способствовали тестированию процессов на стыке между безопасностью, физической безопасностью и аварийной готовностью, а также укрепления режимов физической ядерной безопасности путем выявления потенциальных слабых мест и принятия необходимых корректирующих мер для повышения общего уровня готовности к угрозам в области кибербезопасности. Кроме того, эти учения дают возможность протестировать национальные и международные каналы связи для оповещения и отчетности. В целом, регулярное проведение учений по компьютерной безопасности является важным аспектом обеспечения физической безопасности ядерных объектов.

Совершенствование методов обнаружения аномалий в области компьютерной безопасности с помощью проектов координированных исследований

Родни Буским э Силва и Андреа Рахандини

Выявление аномалий в работе компьютерных систем, контролирующих критически важные функции ядерной и физической безопасности, требует высокой квалификации, а необходимые меры, чтобы быть эффективными, должны быть протестированы, проанализированы и скорректированы.

«Обнаружение аномалий играет важную роль в оперативной оценке потенциальных опасностей, угрожающих компьютерным системам на ядерных и радиологических установках, — говорит Скотт Первис, начальник Секции управления информацией Отдела физической ядерной безопасности МАГАТЭ. — Обычно для обнаружения аномалий используется искусственный интеллект, в том числе машинное обучение, методы, основанные на статистике и знаниях, а также другие технологии». Такие технологии используются для выявления отклонений от ожидаемых параметров сетевых коммуникаций или показателей, которые могут быть первым признаком того, что злоумышленникам удалось преодолеть защиту компьютерной системы; они способны обеспечивать обнаружение кибератак в режиме реального времени.

Эти технологии важны потому, что злоумышленники могут внедрить вредоносное ПО, способное подорвать функции безопасности и защиты цифровой системы и сфальсифицировать данные, которые датчики и сенсоры передают оператору. Таким образом оператор не сможет узнать о злоумышленных действиях и первое время будет реагировать исходя из показателей приборов в диспетчерской, то есть предпринимать неверные действия. Оператор может быть правильно проинформирован только благодаря автоматизированному обнаружению мельчайших аномалий, проявляющихся в ходе такой кибератаки.

Для охвата этой важной области работы и решения других проблем компьютерной безопасности МАГАТЭ в 2016 году запустило специальный проект координированных исследований (ПКИ).

Исследования и разработки в рамках ПКИ — неотъемлемая часть деятельности МАГАТЭ в области компьютерной безопасности в целях обеспечения физической ядерной безопасности. В рамках таких проектов проводятся исследования и делаются практические выводы, которые дополняют текущие усилия МАГАТЭ по расширению возможностей стран по предотвращению и выявлению инцидентов в области компьютерной безопасности, реагированию на них и восстановлению после них, которые могут прямо или косвенно повлиять на ядерную и физическую безопасность ядерных и радиологических установок.

«Профессиональный уровень противника растет, и их кибервозможности создают все больше проблем при разработке средств обнаружения аномалий, — отмечает Первис. — Разработка методов выявления аномалий требует доступа к реалистичным и физически сопоставимым данным сети и технологических процессов на объекте для обучения и тестирования моделей обнаружения».

Сценарий кибератаки для наращивания потенциала

Начатый в 2016 году ПКИ на тему «Совершенствование анализа инцидентов в сфере компьютерной безопасности на ядерных установках» принес значительные результаты, в частности, способствовал дальнейшему исследованию целевых инструментов и методов, которые ранее было невозможно исследовать без риска раскрытия конфиденциальной информации, связанной с ядерными и радиологическими установками.

Участвующие в реализации ПКИ исследователи из 13 стран и 17 организаций разработали виртуальную модель объекта (АЭС «Ашера»), а специалисты из Университета Сан-Паулу создали на основе этой модели тренажер (ANS). Вместе они разработали реалистичные сценарии кибератаки на ядерный объект. Эти сценарии позволили изучить и оценить эффективность мер компьютерной безопасности, а также потенциальные последствия несанкционированного доступа к цифровым активам для эксплуатации установки. Кроме того, специалисты работали над сбором и анализом данных, разработкой и тестированием методов обнаружения кибератак.

«Мы создали и с помощью ANS наполнили хранилище данных для обучения моделей машинного обучения и оценки их эффективности. В рамках ПКИ МАГАТЭ объединило усилия международных партнеров для проведения исследований и способствовало получению

В Университете Сан-Паулу был разработан тренажер на базе виртуальной АЭС «Ашера». (Фото: МАГАТЭ)

новых знаний в этой области, — говорит Рикардо Маркес, профессор политехнической школы при Университете Сан-Паулу (Бразилия). — Сотрудничество между участниками ПКИ было принципиально важно для подтверждения результатов проделанной работы».

Кроме того, результаты ПКИ использовались для обучения и подготовки большого числа аспирантов и ученых в различных дисциплинах. Это способствовало дальнейшему развитию исследований и подкрепило усилия, направленные на постоянное укрепление компьютерной безопасности на ядерных и радиологических установках.

«Часть моих исследований в аспирантуре проводилась с использованием ANS и его человеко-машинного интерфейса (ЧМИ) — интерфейса, который позволяет пользователю взаимодействовать с тренажером, разработанным в рамках ПКИ МАГАТЭ», — рассказывает Си Вэнь, аспирант Университета Цинхуа (Китай). «Мои исследования касались методов обнаружения аномалий, и ANS был необходим для получения данных для обучения и оценки алгоритма обнаружения, разработанного для АЭС. Без сотрудничества между всеми участвующими учреждениями и инструментов, разработанных в рамках ПКИ, мое исследование по кибербезопасности цифровых систем АЭС было бы невозможно провести», — добавляет она.

Результаты ПКИ — ANS, инструменты и руководящие материалы — доступны для заинтересованных исследовательских институтов по всему миру. Их можно получить, подав в МАГАТЭ через соответствующий национальный орган форму запроса, которая размещена на портале МАГАТЭ по физической ядерной безопасности (NUSEC).

Совсем недавно, в 2023 году, МАГАТЭ приступило к реализации нового ПКИ по теме «Укрепление компьютерной безопасности применительно к системам обнаружения излучения» для исследования методик и способов повышения компьютерной безопасности оборудования для обнаружения излучения. В рамках нового ПКИ, в котором примут участие 12 организаций (включая национальные лаборатории, университеты и национальные исследовательские институты) из 11 стран, будут проводиться исследования, направленные на использование новых цифровых технологий, таких как облачные вычисления, а также дальнейшее изучение и разработка инновационных методов обнаружения аномалий.

Безопасность цифровых технологий для ядерных реакторов следующего поколения

Джоанн Лю

Все инновации подразумевают потенциальные выгоды, которые могут привести к трансформации целых отраслей, но они также и несут в себе потенциальные риски. Что касается ядерной области, инновационные технологии, включая цифровые технологии, на основе которых создаются новые разработки, находят широкое применение в усовершенствованных ядерных реакторах, в том числе модульных реакторах малой мощности (ММР).

На рынке отмечается растущий интерес к ММР. Эти современные ядерные реакторы имеют ограничение по мощности в среднем до 300 МВт (эл.) на энергоблок, что составляет примерно одну треть от генерирующей мощности энергоблоков с традиционными энергетическими реакторами. При этом в этих новых реакторах используются передовые цифровые технологии, которые порождают новые вызовы в плане ядерной и физической безопасности. В мире насчитывается более 80 проектов и концепций ММР, находящихся на разных стадиях разработки.

«Одна из проблем на пути к внедрению ММР заключается в том, как ускорить развитие необходимых для них технологий и продемонстрировать уровень их готовности, обеспечивая при этом соответствие нормам ядерной безопасности, — говорит сотрудник по вопросам безопасности информационных технологий в МАГАТЭ Родни Буским э Силва. — Это является еще одним аргументом в пользу цифровых систем контроля и управления и средств компьютерной безопасности, которые должны предусматриваться и поддерживаться в актуальном состоянии на протяжении всего жизненного цикла ММР».

Новые решения и трудности, связанные с компьютерными технологиями

В основе инновационных проектов ММР лежат цифровые системы контроля и управления (СКУ), с помощью которых реализуются их инновационные функции. Расширенный набор цифровых технологий, обеспечивающих возможность автоматизации, дистанционного диспетчерского контроля и обслуживания, наряду с другими новыми функциями, подразумевает необходимость в соответствующих компьютерных решениях.

Некоторые проекты ММР ставят своей целью развертывание ядерных генерирующих мощностей в изолированных районах и сокращение потребности в присутствии персонала на площадке, для чего могут быть необходимы постоянно действующие и надежные механизмы дистанционного мониторинга. Учитывая конструктивные особенности цифровых СКУ, необходимым условием для защищенной связи между площадкой ММР и центром поддержки должно быть применение мер компьютерной безопасности. «Необходимость обмена информацией может выражаться в использовании определенных каналов связи, которые могут быть взломаны киберпреступниками и, следовательно, требуют надежных мер кибербезопасности на уровне инфраструктуры связи, — отмечает Майк Сент-Джон Грин, эксперт по компьютерной безопасности из Соединенного Королевства. — Чтобы обеспечить безопасную и надежную эксплуатацию ММР и связанной с ними инфраструктуры, в режиме дистанционного управления должна быть предусмотрена защита информации для сохранения ее конфиденциальности, доступности и целостности».

В мире насчитывается более 80 проектов и концепций ММР, находящихся на разных стадиях разработки.

Для поддержки работы ММР применяются также технологии искусственного интеллекта (ИИ) и машинного обучения (МО). Понятие ИИ охватывает технологии, которые позволяют создавать системы, способные отслеживать сложные проблемы, в то время как МО подразумевает обучение решению конкретных задач на основе анализа исходных данных. Объединяя цифровые модели ядерной установки и систем управления с системами ИИ, специалисты отрасли ищут способы оптимизировать сложные функции, с помощью которых может быть повышена эффективность эксплуатации установки. Однако эти преимущества сопряжены с потенциальной угрозой кибератак. Например, необходимые для ИИ и МО программные алгоритмы опираются на базы данных, которые могут стать объектом манипуляций, ставящих своей целью спровоцировать принятие ИИ ошибочных решений.

«Эти системы могут быть подвержены атакам типа «внедрение кода», например, когда в них в процессе разработки, поставки или установки программного обеспечения намеренно передаются искаженные данные. Задача в общем заключается в том, как обеспечить достаточную прозрачность алгоритмов ИИ/МО. Допустимая область применения ИИ/МО должна быть четко определена с учетом допустимых уровней риска», — рассказывает Си Вэнь, аспирант Университета Цинхуа (Китай).

Изначально предусмотренные средства безопасности

Эксперты сходятся во мнении, что соображения компьютерной безопасности ядерных установок должны приниматься во внимание с самого начала. Такой упреждающий подход, известный как «учет требований безопасности при проектировании», опирается на передовую практику и накопленный опыт и реализует принцип учета тех или иных требований еще на этапе проектирования, который применяется также в отношении требований ядерной и физической безопасности и гарантий.

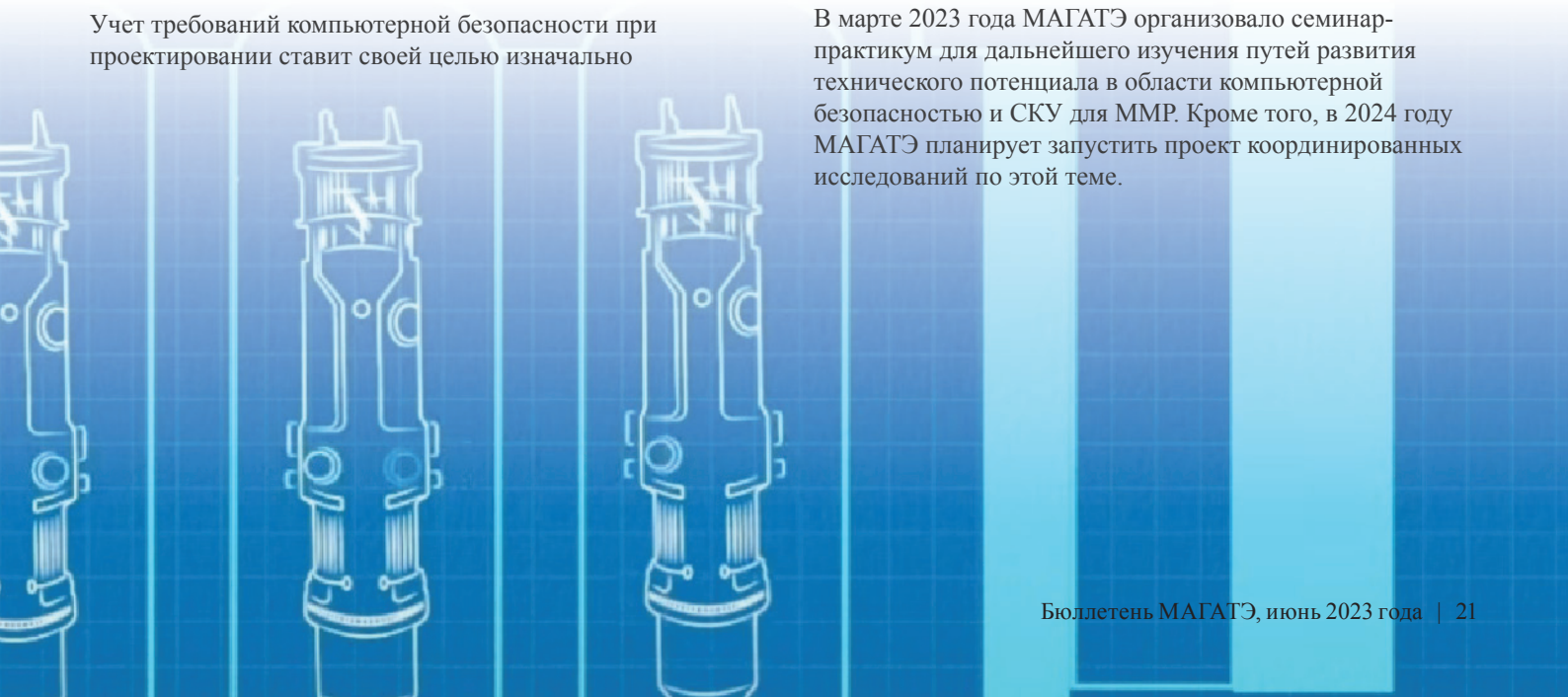
Учет требований компьютерной безопасности при проектировании ставит своей целью изначально снизить риски безопасности на основе подхода, при котором требования безопасности систематически и последовательно принимаются в расчет на всех этапах жизненного цикла установки или процесса.

«Меры компьютерной безопасности должны предусматриваться и поддерживаться в актуальном состоянии на протяжении всего жизненного цикла ММР, от проектирования к эксплуатации и до вывода из эксплуатации», — резюмирует Буским э Силва. — Когда требования безопасности, в том числе компьютерной безопасности, учитываются с самого начала, еще на этапе проектирования разработчики установки могут заложить определенные решения, которые сделают эту установку более защищенной, безопасной, эффективной и экономически выгодной».

Роль МАГАТЭ

МАГАТЭ привлекает экспертов из ядерных и других организаций для обсуждения и определения круга вопросов и задач, связанных с обеспечением компьютерной безопасности с учетом технологических и эксплуатационных особенностей ММР. Так, в феврале 2022 года МАГАТЭ организовало техническое совещание по безопасности СКУ и компьютерных систем для ММР в целях укрепления сотрудничества и содействия обмену информацией между международными экспертами. Участники согласились с необходимостью гармонизации национальных подходов и правил для создания жизнеспособного международного рынка ММР. «Решения для СКУ в составе стандартизированных ММР представляют собой совершенно новую техническую область. Растущая автоматизация, требуемая для новых режимов работы, и широкое применение цифровых систем подразумевает, что меры компьютерной безопасности и соответствующие инженерные решения должны быть реализованы еще на уровне проектирования, чтобы гарантировать безопасную и надежную работу станции», — считает Хорхе Касанова, который участвовал в совещании как представитель Управления по ядерному регулированию Аргентины.

В марте 2023 года МАГАТЭ организовало семинар-практикум для дальнейшего изучения путей развития технического потенциала в области компьютерной безопасностью и СКУ для ММР. Кроме того, в 2024 году МАГАТЭ планирует запустить проект координированных исследований по этой теме.



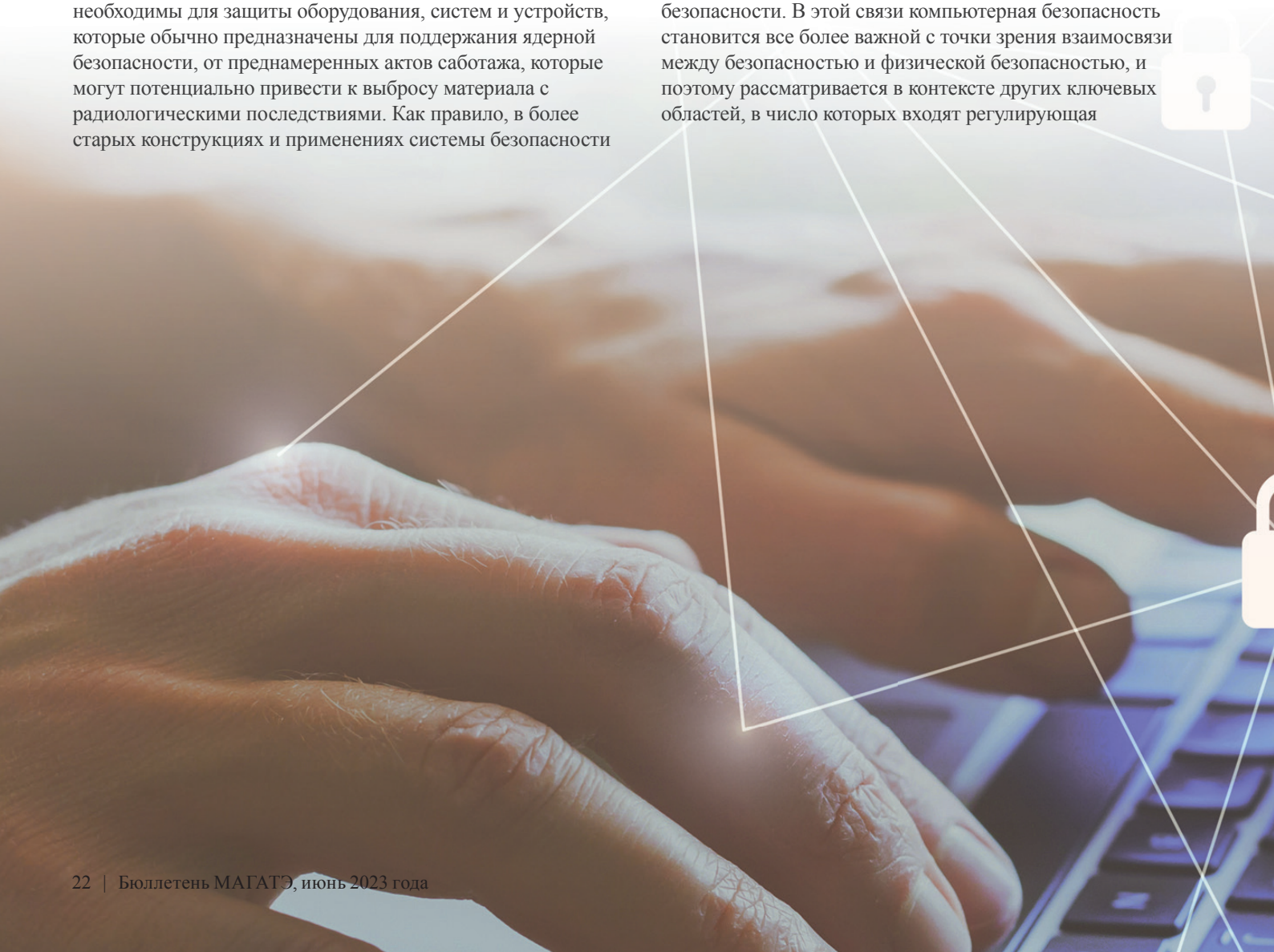
Укрепление компьютерной безопасности в интересах обеспечения ядерной и физической безопасности

Лиди Эврар
заместитель Генерального директора — руководитель Департамента ядерной и физической безопасности

Ядерная безопасность и физическая ядерная безопасность имеют общую цель и единое видение — защищать людей, общество и окружающую среду от возможного вредного воздействия ионизирующего излучения. Хотя виды деятельности, направленной на обеспечение ядерной безопасности и физической ядерной безопасности, различаются, очень важно разработать хорошо скоординированный подход к управлению их взаимосвязью. Важно сделать так, чтобы соответствующие меры осуществлялись таким образом, который не ставит под угрозу ни безопасность, ни физическую безопасность, но при этом использует все потенциально существующие возможности взаимного укрепления этих двух аспектов.

Хорошо известно, что на ядерных и радиологических объектах системы и меры физической безопасности необходимы для защиты оборудования, систем и устройств, которые обычно предназначены для поддержания ядерной безопасности, от преднамеренных актов саботажа, которые могут потенциально привести к выбросу материала с радиологическими последствиями. Как правило, в более старых конструкциях и применениях системы безопасности были защищены только с помощью мер физической защиты. Однако сегодняшние массовые и набирающие силу тенденции в области технологий способствуют значительному повышению роли цифровых систем в обеспечении эффективности операций на ядерных и радиологических установках, особенно касающихся важных функций установки, таких как системы контроля и управления, включая те, которые используются для обеспечения как безопасности, так и физической безопасности.

Физическая безопасность этих систем требует пристального внимания, чтобы выявлять факторы уязвимости и предотвращать несанкционированный доступ к цифровым системам управления, который может привести к подрыву функций обеспечения безопасности или физической безопасности. В этой связи компьютерная безопасность становится все более важной с точки зрения взаимосвязи между безопасностью и физической безопасностью, и поэтому рассматривается в контексте других ключевых областей, в число которых входят регулирующая



инфраструктура, инженерно-технические решения при проектировании и сооружении ядерных установок, меры контроля за доступом к ядерным установкам, категоризация радиоактивных источников, обращение с радиоактивными источниками и радиоактивным материалом, включая отработавшее топливо и радиоактивные отходы, обнаружение и возвращение неконтролируемых источников, а также аварийное реагирование и планы чрезвычайных мер.

При подготовке регулирующих положений в области компьютерной безопасности на национальном уровне директивным органам следует вместе рассматривать ядерную безопасность и физическую ядерную безопасность. В основе взаимодействия безопасности и физической безопасности лежат четкое распределение ответственности, лидерство и управление рисками, которые одинаково важны для осуществления эффективных мер компьютерной безопасности. В то же время обеспечение компьютерной безопасности является по сути глобальной задачей.

В этой связи широко признается важность международного сотрудничества и центральная роль МАГАТЭ. Взаимосвязь между ядерной безопасностью и физической ядерной безопасностью подчеркивается в нормах безопасности МАГАТЭ и руководящих материалах по физической ядерной безопасности. Уже около десяти лет МАГАТЭ разрабатывает и предлагает странам всеобъемлющий набор инструментов помощи в технической области информационной и компьютерной безопасности, оказывая им тем самым поддержку в принятии эффективных мер противодействия кибератакам, которые могут потенциально оказать негативное воздействие на физическую ядерную безопасность. Помимо этого, МАГАТЭ оказывает поддержку в установлении синергетических связей между системами ядерной безопасности и физической ядерной безопасности, а также в принятии мер для того, чтобы действия, предпринимаемые в этих двух областях, дополняли, а не подрывали друг друга.

В результате технического прогресса в будущем еще больше увеличится важность надежной компьютерной безопасности в интересах обеспечения ядерной и физической безопасности на уровне государства и установки. Быстро развивающиеся технологии, такие как искусственный интеллект, являются перспективными с точки зрения решения некоторых проблем и совершенствования цифрового управления операциями. В то же время они вызывают новые вопросы, которыми необходимо заниматься. Аналогичным образом технологии беспроводной связи и автоматизации рассматриваются и используются сегодня в таких конструкциях усовершенствованных ядерных реакторов, как малые модульные реакторы и микрореакторы. Поскольку киберугрозы непрерывно и стремительно развиваются, помощь государствам-членам со стороны МАГАТЭ в удовлетворении их потребностей в области укреплении компьютерной безопасности в интересах обеспечения ядерной и физической безопасности должна отличаться динамикой, чтобы не упускать из виду новые возможности и трудности, связанные с этими новейшими технологиями, и предоставлять наиболее действенные нормы, актуальные примеры наилучшей практики, программы подготовки и руководящие материалы. Именно этого и стремится непременно добиться Департамент ядерной безопасности МАГАТЭ.

Противодействие угрозам в условиях дальнейшей цифровизации мира

Вольфганг Пикот

В мае 2022 года Австрийский технологический институт (АТИ) стал первым центром сотрудничества МАГАТЭ по вопросам информационной и компьютерной безопасности в целях обеспечения физической ядерной безопасности. АТИ содействует проведению международных и региональных учебных курсов и учений по компьютерной безопасности ядерных объектов и деятельности, разрабатывает технические демонстрационные модули для повышения осведомленности о киберугрозах и вносит вклад в разработку учебных материалов для Учебно-демонстрационного центра по физической ядерной безопасности в Зайберсдорфе. Чтобы лучше понять это сотрудничество, мы поговорили с руководителем Центра цифровой безопасности и физической безопасности АТИ Гельмутом Леопольдом.

Каковы новые риски и угрозы в области компьютерной безопасности в целом?

Многие современные цифровые устройства сегодня создаются с учетом более разветвленных сетей. Многим из них для работы необходим доступ к интернету. Каждая разработка программного обеспечения включает в себя потенциальные ошибки, которые могут привести к возникновению уязвимости. Плохо защищенные интерфейсы и безответственные действия пользователей увеличивают количество угроз с точки зрения безопасности работы систем информационных технологий (ИТ). Злоумышленники используют уязвимости цифровых систем для получения доступа.

Методы и инструменты атаки развиваются параллельно с развитием процессов цифровых инноваций. Предназначенное для хакеров программное обеспечение теперь легко найти в интернете, что делает организацию атаки более простой, причем даже для не самых квалифицированных злоумышленников. Нам противостоит многогранная экосистема кибератак, которую подпитывает организованная преступность, экономический и промышленный шпионаж, а также кибертерроризм.

Поэтому сегодня пользователям, компаниям и официальным органам угрожают кибератаки самого широкого спектра, которые могут совершаться в отношении цифровой инфраструктуры целых государств в сочетании с целенаправленными кампаниями по дезинформации, сотрясая основы наших обществ.

Сталкивается ли ядерная отрасль с теми же проблемами?

Промышленные и индивидуальные потребители в основном используют информационные технологии (ИТ), основанные на данных и ориентированные на коммуникацию. Напротив, производственные объекты и критическая инфраструктура используют так называемые операционные технологии (ОТ), которые отслеживают и контролируют поведение и результаты определенных производственных процессов. ОТ традиционно были гораздо менее взаимосвязаны, чем ИТ, однако в ходе технического прогресса эти две области сблизились, и поэтому программное обеспечение и устройства ОТ все чаще подключаются к более широким сетям.

Такое развитие событий представляет проблему, поскольку по сравнению со сферой ИТ осведомленность о кибербезопасности в области ОТ является менее распространенной.

Таким образом, эти новые угрозы в области безопасности ИТ становятся актуальными для ОТ промышленного производства и критической инфраструктуры. Они также становятся все более актуальными и для ядерной отрасли, которая традиционно придерживалась консервативного подхода и имела изолированные системы управления.

Какие мероприятия проводит АТИ для укрепления кибербезопасности в целях обеспечения физической ядерной безопасности?

В рамках исследовательской программы АТИ идет тщательное изучение различных сценариев возможного влияния меняющихся угроз на системы ОТ в целях разработки ноу-хау и новых решений для повышения устойчивости критической инфраструктуры к кибератакам. Эта работа является основой для разработки новых глобальных норм физической безопасности, процедур сертификации элементов критически важных систем и новых видов системной архитектуры для включения в них надежных мер обеспечения кибербезопасности в системы ОТ с начала их проектирования.

АТИ также предлагает комплексную подготовку и обучение для обеспечения готовности к кибератакам. На так называемых «киберполигонах», то есть с использованием сложных имитационных моделей «виртуализованных» систем ИТ, пользователи, разработчики систем, эксплуатационный персонал и представители государственных органов осуществляют реагирование на реалистичные сценарии кибератак. Такие имитационные модели имеют решающее значение для обеспечения устойчивости систем ИТ и ОТ, способных эффективно противостоять киберугрозам.

Каковы преимущества виртуальной учебной среды, разработанной АТИ и МАГАТЭ?

Самый эффективный процесс обучения — это получение практического опыта. АТИ и МАГАТЭ разработали «киберполигон», который позволяет создать «цифровых двойников» существующих объектов критической цифровой инфраструктуры, а также предлагает обучение а рамках весьма реалистичных сценариев применения.

Здесь пользователи, представляющие государственные органы и отрасль, могут провести оценку и проверку эффективности механизмов защиты и бизнес-процессов.

Полученный на «киберполигоне» опыт помогает создавать устойчивый оборонительный потенциал как государственных, так и частных организаций.

Помимо виртуального обучения, как работа и опыт АТИ в области компьютерной безопасности способствуют укреплению физической ядерной безопасности?

Мы можем помочь защититься от злоумышленников, например, путем разработки программного обеспечения для мониторинга «периферийных» устройств, которые обычно связывают внутренние сети организаций с интернетом. Злоумышленники часто используют их как точки входа в систему, прежде чем нанести ущерб.

Мы используем наш опыт в обнаружении аномалий для обучения аналитического программного обеспечения, отслеживающего поведение периферийных устройств, которые, как правило, используются на ядерных установках определенного типа.

Такое программное обеспечение может подавать сигнал тревоги или принимать контрмеры, если устройство ведет себя необычным образом. В результате операторы могут быстро обнаруживать и останавливать кибератаки до того, как они смогут нанести значительный ущерб.

Год назад АТИ стал первым центром сотрудничества МАГАТЭ по вопросам компьютерной безопасности в целях обеспечения физической ядерной безопасности и на сегодняшний день остается единственным таким центром. Что это означает для работы АТИ?

Мы невероятно гордимся тем, что получили статус центра сотрудничества, и продолжаем оказывать помощь в проведении региональных учебных курсов по компьютерной безопасности для систем контроля и управления в ядерной отрасли. Курсы проводились дважды в 2022 году с использованием некоторых результатов нашей совместной работы по разработке виртуальной учебной платформы.

Мы также принимали участие в мероприятиях, посвященных вопросам компьютерной безопасности при разработке малых модульных реакторов.

В настоящее время мы помогаем МАГАТЭ в подготовке к международной конференции 2023 года «Компьютерная безопасность в ядерном мире: в интересах обеспечения ядерной безопасности», на которой мы проведем демонстрацию нашей виртуальной учебной платформы, будем председательствовать на панельных заседаниях и представлять доклады, связанные с нашими исследованиями в этой сфере, и так далее.

Каким образом АТИ взаимодействует с Учебно-демонстрационным центром по физической ядерной безопасности (УДЦФЯБ)?

Мы тесно сотрудничаем с нашими коллегами из МАГАТЭ в разработке учебных модулей, демонстраций и учений для УДЦФЯБ. Мы включаем модули компьютерной безопасности в учебные курсы, связанные с физической защитой ядерного и другого радиоактивного материала, а также курсы, связанные с обнаружением и реагированием в случае обнаружения ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля. Организованная таким образом работа призвана укрепить концепцию, согласно которой компьютерная безопасность является неотъемлемым и неотделимым элементом физической ядерной безопасности.

Как международное сотрудничество помогает защитить мир от киберугроз

Тиге Смит является координатором рабочей группы A9 подкомитета 45A. Комитет назначил его руководителем рабочей группы A9, которая занимается вопросами кибербезопасности в Международной электротехнической комиссии (МЭК).

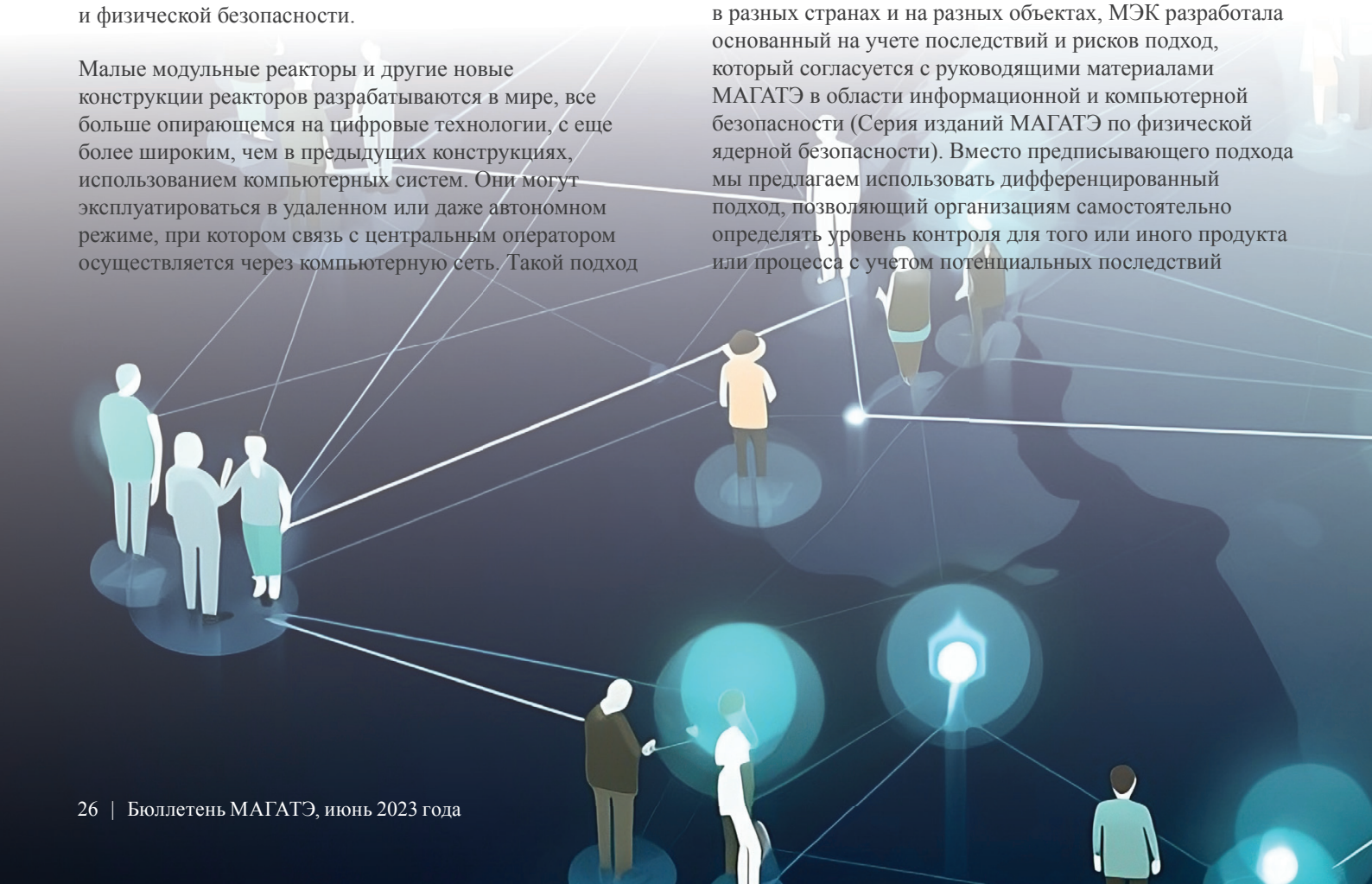
МЭК — это глобальная некоммерческая организация, которая разрабатывает международные стандарты для проектирования, изготовления и эксплуатации электрооборудования, в том числе используемого на атомных электростанциях. МЭК была учреждена в 1906 году, ее членский состав насчитывает более 170 стран, она опубликовала 10 000 международных стандартов.

Ядерная отрасль испытывает серьезные сложности с обеспечением компьютерной безопасности в связи с широким распространением цифровых устройств. Эта тенденция очевидна и в быту, где умные холодильники, осветительные приборы и другие устройства, управляемые дистанционно с помощью облачных технологий, стали обычным явлением. Многие системы на ядерных установках, которые раньше не имели цифровых компонентов, теперь имеют цифровые элементы. Рост вычислительных мощностей и расширение возможностей для перепрограммирования и соединения различных цифровых элементов обеспечивают непревзойденную эффективность при эксплуатации и обеспечении ядерной и физической безопасности.

Малые модульные реакторы и другие новые конструкции реакторов разрабатываются в мире, все больше опирающемся на цифровые технологии, с еще более широким, чем в предыдущих конструкциях, использованием компьютерных систем. Они могут эксплуатироваться в удаленном или даже автономном режиме, при котором связь с центральным оператором осуществляется через компьютерную сеть. Такой подход может давать операторам и автоматизированным системам возможность анализировать большие объемы данных для повышения эффективности работы ядерной установки.

Однако такая цифровизация ядерной отрасли создает дополнительные проблемы, поскольку без должного уровня компьютерной безопасности злоумышленники могут использовать слабые или уязвимые места для атаки на ядерный объект.

Для решения проблем, связанных с быстрым внедрением цифровых технологий на ядерных объектах и необходимостью обеспечивать согласованность подходов в разных странах и на разных объектах, МЭК разработала основанный на учете последствий и рисков подход, который согласуется с руководящими материалами МАГАТЭ в области информационной и компьютерной безопасности (Серия изданий МАГАТЭ по физической ядерной безопасности). Вместо предписывающего подхода мы предлагаем использовать дифференцированный подход, позволяющий организациям самостоятельно определять уровень контроля для того или иного продукта или процесса с учетом потенциальных последствий



кибератаки. Например, в качестве первого шага в разработке программы компьютерной безопасности необходимо проанализировать функции ядерного объекта, оценить их влияние на ядерную и физическую безопасность и определить соответствующий уровень требований к физической безопасности.

Предотвращение, обнаружение и смягчение последствий

Предсказать, как кибератаки будут развиваться в будущем, довольно сложно, поэтому МЭК в тесном сотрудничестве с МАГАТЭ разработала рекомендации о том, что программы компьютерной безопасности на ядерных объектах должны быть направлены не только на предотвращение злонамеренных действий, но и на их обнаружение, реагирование на них и восстановление после них. Даже если элементы кибератаки окажутся успешными, должны существовать механизмы для восстановления и обеспечения корректного выполнения необходимых функций, чтобы гарантировать отсутствие угроз для ядерной или физической безопасности.

Стремительная цифровизация мира, в котором мы живем, в сочетании с развитием искусственного интеллекта (ИИ) и машинного обучения может привести к серьезным проблемам с обеспечением компьютерной безопасности на ядерных объектах. Международное сотрудничество принципиально необходимо для дальнейшей безопасной и надежной эксплуатации таких объектов, несмотря на все проблемы. Вот уже более полувека МАГАТЭ, международное сообщество и ядерная отрасль сообща разрабатывают нормы и стандарты, призванные обеспечить безопасность и надежность мирных ядерных технологий. Острота глобальных проблем, связанных с изменением климата и энергетической безопасностью, продолжает расти, и многие страны уделяют повышенное внимание новым и инновационным ядерным технологиям как к низкоуглеродному источнику энергии — в этих условиях роль стандартизации в поддержании безопасности и надежности ядерных объектов становится все более важной.

Сотрудничество в ядерном мире

МАГАТЭ и МЭК вносят существенный вклад в международные усилия по установлению норм информационной и компьютерной безопасности на ядерных объектах. МАГАТЭ на основе международного консенсуса разрабатывает руководящие материалы в рамках Серии изданий по физической ядерной безопасности (NSS), в которых излагаются концепции и нормы обеспечения информационной и компьютерной безопасности как фундаментальных элементов достижения целей физической ядерной безопасности. Серия изданий по физической ядерной безопасности содержит рекомендации по распределению государственных ресурсов, подготовке отраслевых нормативных документов и концепций для внедрения на ядерных объектах инженерного подхода с учетом аспектов кибербезопасности.

Будучи международной организацией по стандартизации, которая способствует популяризации передового опыта и обмену знаниями, МЭК тесно сотрудничает с МАГАТЭ. В соответствии с меморандумом о взаимопонимании между МЭК и МАГАТЭ ученые и эксперты, сотрудничающие с МЭК, разрабатывают нормы и готовят технические доклады по осуществлению руководящих материалов МАГАТЭ на основе конкретных программных и инженерных требований. Эти требования могут применяться при проектировании и разработке существующих и будущих цифровых систем, которые могут быть сертифицированы по нормативным моделям, согласующимся с руководящими материалами МАГАТЭ. Эксперты ядерной отрасли, обладающие опытом внедрения норм МЭК, могут затем принять участие в разработке дальнейших версий руководящих материалов МАГАТЭ.

Ученые и эксперты участвуют в работе МЭК на добровольной основе и всегда рады коллегам, готовым безвозмездно внести свой вклад. Сообщество экспертов по компьютерной безопасности в ядерной области относительно невелико, даже в мировом масштабе. Вклад в работу МЭК дает возможность разрабатывать нормы, которые могут использоваться во всем мире на благо глобальной ядерной отрасли.

Кодекс поведения МАГАТЭ

20 лет прогресса в области обеспечения ядерной и физической безопасности радиоактивных источников

Выступающие на параллельном мероприятии «Гендерное равенство и инклюзивность в контексте Кодекса поведения по обеспечению безопасности и сохранности радиоактивных источников: 20 лет прогресса». (Фото: В. Вавжута/МАГАТЭ)

В мае 2023 года более 270 правовых и технических экспертов из 128 стран и 4 международных организаций встретились в Вене, Австрия, чтобы дать оценку прогрессу, достигнутому в области обеспечения ядерной и физической безопасности радиоактивных источников, и определить области, нуждающиеся в совершенствовании.

Радиоактивные источники излучения играют незаменимую роль во многих отраслях. В медицине они помогают лечить рак. В сельском хозяйстве — позволяют ученым выводить улучшенные сорта сельскохозяйственных культур для адаптации к изменению климата и укрепления продовольственной безопасности. В сфере искусства и археологии — помогают сохранять бесценное культурное наследие. Обращение с этими источниками предполагает соблюдение надлежащих мер ядерной и физической безопасности.

Для оказания странам помощи в устранении рисков, защите людей и окружающей среды от случайного облучения или преднамеренных несанкционированных действий, связанных с радиоактивными источниками, МАГАТЭ разработало Кодекс поведения по обеспечению безопасности и сохранности радиоактивных источников, который был утвержден Советом управляющих МАГАТЭ в 2003 году и в этом году отмечает свое двадцатилетие.

На открытии совещания открытого состава технических и правовых экспертов, посвященного обмену информацией об осуществлении государствами Кодекса поведения по обеспечению безопасности и сохранности радиоактивных источников, Генеральный директор МАГАТЭ Рафаэль Мариано Гросси заявил: «С момента утверждения Кодекса поведения прошло 20 лет, и мы уверенно добиваемся прогресса в повышении ядерной и физической безопасности радиоактивных источников по всему миру. Однако в целях обеспечения устойчивого обращения с этими источниками, отвечающего требованиям ядерной и физической безопасности, необходимо продолжать работу, направленную на более активное принятие политического обязательства по выполнению Кодекса и обмен наилучшей мировой практикой».

В течение пяти дней своей работы совещание обеспечивало международным экспертам площадку для обмена информацией об осуществлении на национальном уровне Кодекса поведения и двух дополняющих его Руководящих материалов. Такие совещания проводятся каждые три года, что позволяет странам обмениваться опытом и уроками и определять существующие и будущие задачи в связи с осуществлением Кодекса.

На протяжении недели участники подробно рассматривали самые разнообразные темы, включая эволюцию ядерной и физической безопасности, правовые аспекты, международное сотрудничество, будущее развитие и влияние Кодекса поведения. Обсуждались проблемы и приоритетные задачи в области создания надлежащей регулирующей основы для обеспечения ядерной и физической безопасности радиоактивных источников, управления их жизненным циклом, контроля их экспорта и импорта, а также механизмы обращения с источниками после того, как они заявлены в качестве изъятых из употребления. Крайне важно, что совещание позволило участникам обменяться информацией о собственных подходах к эффективному осуществлению положений Кодекса поведения.

Основные руководящие указания для безопасного будущего

На мероприятии по случаю открытия совещания сопредседатель совещания и исполнительный вице-президент и

руководитель службы регулирования Комиссии по ядерной безопасности Канады (КЯБК) Рэмзи Джеммел подчеркнул, что осуществление Кодекса поведения является залогом обеспечения охраны окружающей среды и защиты населения и работников. Он сказал: «Наша конечная цель заключается в обеспечении общей ядерной и физической безопасности радиоактивных источников в течение всего их жизненного цикла в целях предотвращения случайного облучения и злоумышленного использования радиоактивных источников. Это подразумевает совместную постоянную работу».

Тереза Кларк, сопредседатель совещания и заместитель директора отдела в Комиссии по ядерному регулированию США, обратилась к участникам специальной сессии, посвященной истории Кодекса: «Подводя итоги и отмечая двадцатую годовщину, мы стремились достичь общего понимания истории Кодекса как с правовой, так и технической точек зрения, чтобы иметь возможность обмениваться опытом и наилучшей практикой и перенимать друг у друга опыт для повышения эффективности осуществления Кодекса по всему миру».

В Кодексе поведения подробно рассматриваются вопросы обеспечения странами ядерной и физической безопасности радиоактивных источников с момента начального производства и до окончательного захоронения. В нем изложены соображения с учетом международного контекста и даны рекомендации по разработке, согласованию и проведению в жизнь национальной политики, законов и регулирующих положений, а также сотрудничеству между странами. И хотя Кодекс не имеет обязательной юридической силы, с момента его утверждения Советом управляющих в 2003 году политическую поддержку осуществлению его положений выразили 146 государств.

Кодекс поведения дополняют два руководящих документа. Руководящие материалы по импорту и экспорту радиоактивных источников касаются функций и обязанностей при осуществлении импорта и экспорта радиоактивных источников с соблюдением требований ядерной и физической ядерной безопасности. В Руководящих материалах по обращению с изъятыми из употребления радиоактивными источниками приведены рекомендации в отношении обращения с изъятыми из употребления источниками с указанием вариантов обращения по окончании срока их службы, таких как повторное использование или переработка, длительное хранение и захоронение, а также возврат поставщику. Кроме того, в Руководящих материалах содержится призыв к по разработке национальной политики и стратегии обращения с изъятыми из употребления источниками.

«Кодекс поведения и дополняющие его Руководящие материалы приносят ощутимую пользу с точки зрения обеспечения национальной и международной радиационной безопасности и физической ядерной безопасности и позволяют в полной мере использовать преимущества радиоактивных источников в интересах обеспечения устойчивого будущего», — заявила сопредседатель совещания и директор департамента радиационной безопасности Федерального управления по ядерному регулированию ОАЭ (ФУЯР) Аида Ахмед Аш-Шеххи.

МАГАТЭ взаимодействует и тесно сотрудничает со странами для обеспечения согласованного обращения с радиоактивными источниками с соблюдением требований ядерной и физической безопасности. Агентство оказывает поддержку в осуществлении принципов Кодекса и предоставляет всестороннюю помощь по таким вопросам, как разработка стратегий и планов действий по осуществлению Кодекса, совершенствование процессов лицензирования и инспектирования, а также систем исполнения и менеджмента, и укрепление потенциала национальных регулирующих органов в соответствии с нормам безопасности МАГАТЭ, руководящими материалами по физической ядерной безопасности и наилучшей международной практикой.

Укрепление разнообразия и инклюзивности в ядерной сфере

На полях совещания состоялось организованное КЯБК параллельное мероприятие «Гендерное равенство и инклюзивность в контексте Кодекса поведения по обеспечению безопасности и сохранности радиоактивных источников: 20 лет прогресса». Сто двадцать участников мероприятия обсудили вопросы поощрения и расширения участия женщин в ядерной сфере, включая область ядерной и физической безопасности, а также обеспечения равных возможностей для всех независимо от гендерной принадлежности.

Председатель и генеральный директор КЯБК Румина Велши отметила: «Разнообразная представленность участников дискуссии способствует развитию критического отношения, что в свою очередь ведет к формированию высокой культуры безопасности в организации. Обеспечение гендерного равенства — задача не столько для женщин, сколько для всего общества, и она должна быть решена общими усилиями». Г-жа Велши добавила, что растущий спрос на кадровые ресурсы обуславливает необходимость обеспечения более широких возможностей для женщин в ядерной сфере.

Заместитель Генерального директора МАГАТЭ — руководитель Департамента ядерной и физической безопасности Лиди Эврар отметила на мероприятии, что «ядерная и физическая безопасность зиждется на критическом и любознательном отношении, открытости для конструктивных замечаний и способности объединять различные мнения и мобилизовать различные экспертные знания и опыт. Разнообразие, включая гендерное разнообразие, в этом отношении является настоящим преимуществом. Мы становимся сильнее и эффективнее, когда ценим разнообразие и поощряем своих сотрудников высказывать свое мнение».

Заместитель Генерального директора МАГАТЭ — руководитель Департамента управления Маргарет Доан отметила, что «расширение участия женщин и людей с разным опытом в секторах, связанных с ядерной областью, жизненно важно для любой организации». Она рассказала об инициативах МАГАТЭ по повышению гендерного равенства, в том числе Программе стипендий имени Марии Склодовской-Кюри и Программе имени Лизе Майтнер, которые направлены на привлечение большего числа женщин в ядерную отрасль.

Своим видением поделился генеральный директор ФУЯР Кристер Викторссон: «ФУЯР организует целенаправленные мероприятия, направленные на поощрение гендерного равенства. Крайне важны приверженность и поддержка руководства, включая проведение обследований в целях обеспечения соблюдения принципов инклюзивности и справедливого отношения ко всем сотрудникам. Не менее важную роль играет обеспечение инклюзивного характера надлежащей организационной основы и ее эффективного применения».

— Артем Власов

Арабоязычные страны обсуждают планы в области физической ядерной безопасности

Участники состоявшегося недавно в Тунисе регионального совещания обменялись опытом разработки и реализации КППФЯБ. (Фото: З. Хассан/МАГАТЭ и ААЭА)

Недавно страны — участницы Арабской сети ядерных регулирующих органов (АСЯРО) провели в Тунисе совещание с целью обменяться информацией о наилучшей практике, а также проблемах и возможностях, связанных с осуществлением деятельности в области физической ядерной безопасности в рамках их соответствующих комплексных планов поддержки физической ядерной безопасности (КППФЯБ). На совещании была особо отмечена важность развития региональных подходов — неотъемлемого элемента программы МАГАТЭ по физической ядерной безопасности — для укрепления потенциала в области регулирования и эксплуатации.

«Подход к обеспечению физической ядерной безопасности с учетом регионального контекста укрепляет международное сотрудничество и способствует реализации программы МАГАТЭ по физической ядерной безопасности, — говорит директор Отдела физической ядерной безопасности МАГАТЭ Елена Буглова. — Сотрудничество с региональными сетями, такими как АСЯРО, еще больше усиливает действенность механизма поддержки КППФЯБ, создавая возможности для выявления и обсуждения общих потребностей и проблем среди географически близких стран или стран с общим языком».

На совещании 28 участников из 14 стран представили информацию об осуществлении их национальных КППФЯБ. Особое внимание уделялось деятельности, связанной с законодательной и регулирующей основами физической ядерной безопасности, национальными оценками угроз и рисков, режимами физической защиты, обнаружением преступных или несанкционированных действий с использованием ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля (МВРК), реагированием на связанные с МВРК события в области физической ядерной безопасности, а также поддержанием национальных режимов физической ядерной безопасности.

В настоящее время одной из стран, в которых КППФЯБ используется в качестве механизма укрепления национальной инфраструктуры физической ядерной безопасности, является Ливан. «Благодаря семинару-практикуму нам удалось поделиться национальным опытом осуществления КППФЯБ и обсудить проблемы в области физической ядерной безопасности в наших странах, а также возможные пути их решения, — говорит Хасан Басат, руководитель секции в Ливанской комиссии по атомной энергии, ответственный за выдачу официальных разрешений, инспектирование и регулирование. — Самым важным итогом стало выявление общих для участников АСЯРО приоритетных областей КППФЯБ, которые нуждаются в дальнейшем совершенствовании».

В настоящее время утвержденные КППФЯБ имеются у 19 из 22 членов АСЯРО. В целом КППФЯБ утвердили 92 страны.

Руководитель группы физического анализа Управления по радиационной защите Высшего совета Бахрейна по окружающей среде Шаима Халид Аль-Джанахи отмечает: «На региональном уровне у нас общие границы, а также весьма конкретные проблемы. На семинаре-практикуме мы смогли обменяться опытом и знаниями, за которыми, надеюсь, последуют решительные действия в интересах совершенствования и укрепления физической ядерной безопасности в регионе».

Совещание было организовано Арабским агентством по атомной энергии (ААЭА) при финансовой поддержке Европейского союза.

Механизм поддержки КППФЯБ

МАГАТЭ по запросу оказывает странам помощь в разработке КППФЯБ, который служит основой систематического и всеобъемлющего подхода к выявлению национальных потребностей в области физической ядерной безопасности и определению их приоритетности, а также созданию плана по внедрению усовершенствований в области физической ядерной безопасности на национальном уровне. Процесс КППФЯБ дополняет инструмент добровольной самооценки, который доступен для заинтересованных стран на информационном портале по физической ядерной безопасности (NUSEC).

КППФЯБ и связанный с ним план осуществления позволяет странам удовлетворять самые насущные потребности и определять как те задачи, которые возможно решить на национальном уровне, так и те, для решения которых необходимо обратиться за помощью к международному сообществу.

После выявления потребностей каждой страны МАГАТЭ приступает к созданию основ адресной помощи, которая оказывается посредством организации миссий в рамках международных консультационных услуг по физической защите (ИППАС) и международных консультационных услуг по физической ядерной безопасности (ИНССерв).

Сотрудничество МАГАТЭ — АСЯРО

АСЯРО — это региональная сеть, которая была создана в 2010 году в рамках Глобальной сети ядерной и физической ядерной безопасности (GNSSN) МАГАТЭ. АСЯРО формирует, совершенствует и укрепляет основы регулирующей инфраструктуры в сфере радиационной защиты и ядерной и физической безопасности, а также обеспечивает их согласованность в странах-участницах и служит площадкой для обмена информацией об опыте и практике регулирования.

— Василики Тафили

Публикации МАГАТЭ бесплатно онлайн

скачать по ссылке

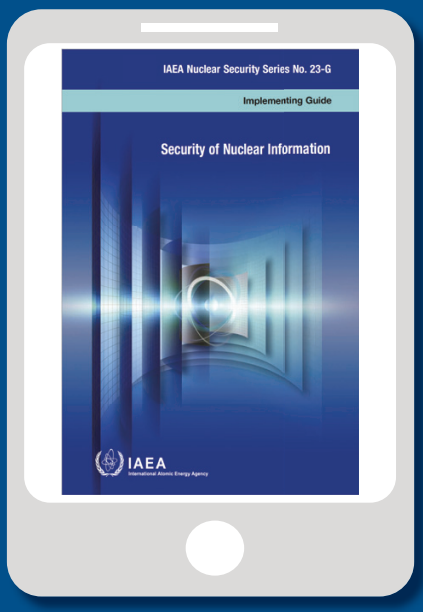
www.iaea.org/ru/publikacii

Для заказа книги просьба обращаться по адресу:
sales.publications@iaea.org

ЗАГРУЗИТЬ

Безопасность ядерной информации
и другие публикации МАГАТЭ по
компьютерной безопасности в ядерной сфере

www.iaea.org/bulletin/64-2



Читайте этот и другие выпуски Бюллетеня МАГАТЭ в интернете по адресу www.iaea.org/ru/bulletin

С более подробной информацией о МАГАТЭ и его работе можно ознакомиться на сайте www.iaea.org/ru

или на наших страницах

ISSN 0250-9938 23-01968R