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).