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.