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.