УДК 621.3

Ключевые проблемы кибербезопасности гражданских ядерных объектов

Плешко Д.Ю., Федосевич Э.А.
Научные руководители – к.т.н., доцент БЛАДЫКО Ю. В.,
ст. препод. САПОЖНИКОВА А.Г.

Вызовы в сфере кибербезопасности стали одной из ключевых проблем для операторов критической инфраструктуры (КИ) во всех отраслях. Кибератаки способны нарушать критически важные бизнес-процессы и операции на физическом уровне, выводить из строя оборудование и угрожать потерей доступа к услугам и инфраструктурным сервисам первой необходимости. Общемировые тенденции использования информационно-коммуникационных технологий (ИКТ) делают КИ всех секторов более уязвимой для кибератак, однако возможности киберзащиты гражданских ядерных объектов (ГЯО) стоит рассматривать отдельно в силу уникальных особенностей этой области.

В докладе «Ключевые проблемы кибербезопасности гражданских ядерных объектов» рассматриваются особенности сектора ГЯО с точки зрения обеспечения кибербезопасности его КИ, национальные и международные подходы к регулированию КИ ГЯО, попытки выработать классификацию киберугроз для ядерной отрасли, а также приоритетные направления деятельности для обеспечения кибербезопасности ГЯО на данном этапе.

Общемировые тенденции в использовании ИКТ делают критическую инфраструктуру всех секторов (электроэнергия, транспорт, нефтегазовый сектор, авиация и т. д.) более уязвимой для кибератак. К таким тенденциям относится масштабный и все еще продолжающийся переход на автоматизированные системы управления технологическими процессами (АСУ ТП) на критически важных объектах (КВО), а также практика подключения офисных и даже промышленных корпоративных сетей объектов КИ к интернету.

Эта практика получает более широкое распространение по мере внедрения технологий Интернета вещей и Всеобъемлющего Интернета. Доступ объектов КИ к Сети идет параллельно с мобильной революцией, благодаря которой в различные секторы КИ приходят концепции «приноси свое устройство» и «карманная АСУ ТП». Наконец, для большинства секторов КИ общей проблемой стала исключительная сложность трансконтинентальных цепочек поставок систем управления ТП, программного обеспечения (ПО) для контроля таких систем (включая автоматизированные системы управления и сбора данных), а также устройств нижнего уровня.

Эти тенденции проявляются по всех областях, и ядерная энергетика здесь не исключение, но в силу присущих ему особенностей, сектор ГЯО является наиболее консервативным в части некоторых из них: использование больших данных, применения Интернета вещей в промышленных процессах, удаленного мобильного управления системами управления и сбора данных, а также проведения политики «приноси свое устройство» среди сотрудников.

Сектор ГЯО обладает уникальными характеристиками и требует особого подхода к обеспечению кибербезопасности объектов. С одной стороны, гражданские ядерные установки практически повсюду защищаются глубоко проработанными и всеобъемлющими системами норм и правил физической ядерной безопасности (ФЯБ), которые позволяют принципиально устранить некоторые вопросы, связанные с кибербезопасностью.

С другой стороны, уникальность сектора ГЯО создает проблемные точки и барьеры для эффективного противодействия киберугрозам.

К таким особенностям относятся, в частности, уникальная инфраструктурная сложность сектора ГЯО.

Объекты сектора ГЯО разнообразны и включают, например, малые исследовательские реакторы на базе университетов. Но в большинстве случаев, в частности когда в анализ

включаются АЭС, речь идет об исключительно сложных, масштабных и опасных объектах. Соответственно, для поддержки функционирования

АЭС требуется исключительно сложная ИТ-система. К примеру, на АЭС последнего поколения современная ИТ-инфраструктура включает как минимум четыре контура, причем корпоративная офисная сеть представляет собой лишь один контур – верхний. Каждый силовой блок на АЭС оснащен несколькими десятками подсистем АСУ ТП, которые необходимо интегрировать между собой, а также обеспечить их безопасность и совместимость с корпоративным ПО, отвечающим за управление и сбор данных.

Общее количество поставщиков программного и аппаратного обеспечения для одной АЭС сегодня может превышать три сотни. Более того, каждый силовой блок оснащен более чем 10 тыс. датчиков, сенсоров и детекторов, отсылающих данные оператору на системы мониторинга. В общей сложности ИТ-системы современной АЭС регистрируют до 200 тыс. изменений параметров в секунду. Такая сложность порождает ряд последствий и проблем, которые требуют продуманного решения.

Во-первых, для ГЯО не существует универсальных стандартных решений по интеграции ИТ-подсистем объекта. Так, каждая АЭС с точки зрения своей ИТ-инфраструктуры, ее архитектуры и топологии является уникальным объектом, на котором реализованы оригинальные решения по ИТ-интеграции. Соответственно, в каждом случае сетям и ИТ-системам такого объекта присущ уникальный набор уязвимостей кибербезопасности и брешей в защите сетевого периметра. Это серьезно ограничивает возможности и практический смысл применения операторами ГЯО накопленного опыта и лучших практик.

Во-вторых, проблема доверия к ИТ-поставщикам и необходимость обеспечения целостности цепочек поставок ИТ-продукции, особенно для АСУ ТП. Операторы не располагают возможностями провести доскональную проверку тысяч контроллеров, дистанционных терминалов, маршрутизаторов, программных комплексов по управлению производственными процессами и т. д. на скрытый функционал, вредоносное ПО или ошибки. Это серьезная проблема, поскольку, как уже говорилось выше, каждый оператор АЭС вынужден зависеть от многих десятков и даже сотен поставщиков, а многие из них – транснациональные компании.

В-третьих, сложность внутренней ИТ-инфраструктуры ГЯО и интенсивность потоков данных в этой инфраструктуре требуют комплексного и всеобъемлющего подхода к кибербезопасности, который принципиально выходит за рамки только лишь реагирования на инциденты.

Можно наметить несколько элементов такого перспективного подхода:

– обеспечение кибербезопасности на этапе проектирования – концепция, которая имеет много общего с ядерной безопасностью на этапе проектирования;

– обнаружение сетевых событий, реагирование на них, а также мониторинг сетевого трафика в режиме реального времени для всех контуров ИТ-инфра-структуры ГЯО, включая АСУ ТП;

– введение новых требований к поставщикам критически важных комплектующих АСУ ТП. Например, обязать поставщика раскрывать оператору ГЯО исходный код прошивки программных логических контроллеров после подписания контракта на поставку;

– внедрение решений по криптографической защите информации, а также цифровых подписей и защищенных меток времени на нижних уровнях сетевой инфраструктуры ГЯО (уровень АСУ ТП) для более надежной защиты целостности и конфиденциальности данных.

Ещё одной особенностью является неопределенность места и роли кибербезопасности ГЯО в физической ядерной безопасности. Область кибербезопасности ГЯО формируется на пересечении промышленной безопасности АСУ ТП, физической ядерной безопасности (ФЯБ) и информационной безопасности (ИБ).

Задача ИБ – обеспечение триады «конфиденциальность, целостность, доступность» в отношении информации, которая обрабатывается, хранится и передается в информационных

системах объекта. Эта задача распространяется как на информацию из баз данных офисного сегмента сети ГЯО, так и на данные, которые получает ПО для сбора и управления технологическими процессами от устройств нижнего уровня.

ФЯБ является уникальной составляющей экосистемы безопасности ГЯО, отсутствующей в прочих секторах КИ. Согласно определению МАГАТЭ, обеспечение ФЯБ заключается в предотвращении, обнаружении и реагировании на хищение, саботаж (диверсию), несанкционированный доступ, незаконную передачу или другие злоумышленные действия в отношении ядерных материалов и других радиоактивных веществ, а также связанных с ними установок и пунктов хранения ядерных материалов.

Изначально ФЯБ не имела ничего общего с киберпространством. Однако по мере появления новых векторов угроз операторы ГЯО, технические специалисты и регуляторы были вынуждены работать над включением вопросов кибербезопасности в парадигму ФЯБ. На сегодняшний день интеграция кибербезопасности ГЯО и ФЯБ не завершена, и в некоторых случаях такая незавершенность представляет вызовы для обеспечения кибербезопасности ГЯО в силу следующих обстоятельств:

– нечеткое разведение функций и распределение ресурсов между структурными подразделениями ГЯО, отвечающими за ИБ и кибербезопасность, и подразделениями, ответственными за ФЯБ;

– взаимно противоречащие требования, стандарты и процедуры для обеспечения кибербезопасности с одной стороны и ФЯБ с другой;

– ограничения, которые могут накладываться требованиями и нормативами ФЯБ на значимые технологические нововведения, необходимые для более надежного обеспечения ИБ объекта (например, внедрение средств криптографической защиты информации на сетях передачи данных между АСУ ТП);

– терминологические и концептуальные расхождения между представителями подразделений, ответственных за кибербезопасность и за ФЯБ (что может затруднять совместную работу над нейтрализацией вызовов и реагированием на инциденты).

В большинстве стран кибербезопасность ГЯО только начинает формироваться в качестве отдельной повестки дня для регуляторов национального уровня. Ключевая сложность состоит в нечетком распределении регуляторных задач между государственными органами, которое влечет за собой пробелы в выполнении или, наоборот, дублирование функций регуляторов.

Во многих государствах, особенно в развивающихся (Индия, Украина, Бразилия, ЮАР), связанные с кибербезопасностью ГЯО регуляторные полномочия рассредоточены между несколькими государственными агентствами и министерствами, что зачастую ведет к недостатку коммуникации между ними и отсутствию отлаженного механизма решения вопросов, которые попадают в сферу компетенций сразу нескольких регуляторов.

Следующей проблемой является отсутствие единого регулятора, который отвечал бы за весь комплекс вопросов, связанных с безопасностью ГЯО, а это часто ведет к слабой обратной связи от других участников: операторов ГЯО, их ИТ- и ИБ-поставщиков и подрядчиков. Более широко эта тенденция выражается в недостаточной обратной связи от частного сектора и экспертного сообщества, поскольку в некоторых случаях их представители не могут определить, какому регулятору следует адресовать те или иные вопросы.

Недостаточная гибкость подходов, на которые опираются национальные регуляторы, также может затормаживать развитие политики кибербезопасности ГЯО, в том числе когда в основе таких подходов лежит развитая система норм и технических руководств по ФЯБ или законодательство в сфере защиты информации и кибербезопасности. Преемственность уже сформированного подхода иногда выступает барьером для выработки гибридного регулирования, которое бы охватывало специфические вопросы сектора ГЯО.

Наконец, имеет место недостаточно активная интеграция международных руководств, рекомендаций и лучших практик в национальные нормы и требования, которые во многих

случаях ограничиваются сугубо техническими вопросами. Прежде всего это относится к рекомендациям и техническим руководствам МАГАТЭ, а также к документам и рекомендациям, выработанным в рамках других международных площадок и рабочих процессов (например, Всемирного института ядерной безопасности и Саммита по ядерной безопасности). Такая тенденция отмечается даже в государствах с развитой регуляторной политикой как в секторе ядерной энергетики, так и в сфере кибербезопасности (Россия, США, Франция).

На уровне выработки международных норм и политик быстрого прогресса ждать не приходится. Юридически обязывающие межправительственные соглашения о борьбе с киберугрозами на объектах КИ еще долго могут не приниматься. В то же время дебаты по вопросам адаптации существующих норм международного права к вызовам, исходящим из киберпространства, могут затянуться на десятилетия, но в итоге так и не привести к появлению применимых на практике механизмов сотрудничества.

Действие существующих трансграничных механизмов противодействия киберпреступности практически не распространяется на сектор ГЯО из-за ограничений, связанных с национальной безопасностью. Тем не менее, диалог в рамках всех перечисленных площадок и форматов целесообразен – имеет смысл вести его и далее, даже если он не принесет плоды в ближайшей перспективе.