КИБЕРБЕЗОПАСНОСТЬ ГРАЖДАНСКИХ ЯДЕРНЫХ ОБЪЕКТОВ: ОЦЕНКА УГРОЗЫ И ПУТИ ЕЕ ПРЕОДОЛЕНИЯ[1]

Доклад подготовлен ПИР-Центром в сотрудничестве с женевским Centre russe d'etudes politiques в 2016 г. Проект реализован в рамках Рабочего процесса по кибербезопасности ядерных установок при Совете по глобальной повестке Всемирного экономического форума.

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 «Кибербезопасность гражданских ядерных объектов: оценка угрозы и пути ее преодоления» 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.

КЛЮЧЕВЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ ГРАЖДАНСКИХ ЯДЕРНЫХ ОБЪЕКТОВ

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 революю-

цией, благодаря которой в различные секторы КИ приходят концепции «приноси свое устройство» (BYOD) 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 SCADA), 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:

1. 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 периме-

тра. 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-инфраструктуры 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.

2. *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/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).

РЕГУЛИРОВАНИЕ В ГРАЖДАНСКОЙ ЯДЕРНОЙ ОТРАСЛИ: НАЦИОНАЛЬНЫЕ ПОДХОДЫ И МЕЖДУНАРОДНЫЕ ФОРМАТЫ

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).

Кибербезопасность ГЯО в национальном праве

Тем не менее с начала 2010-х гг. во многих юрисдикциях наблюдается постепенный прогресс. Один из заслуживающих упоминания индикаторов — заметно ускорившийся во многих государствах за последние пять лет процесс выработки и принятия отраслевого законодательства и обязательных требований по кибербезопасности ГЯО. В числе стран, которые с 2012 г. приняли или начали разрабатывать законодательство или подробные требования к кибербезопасности сектора ГЯО, — Австралия, Бельгия, Канада, Чехия, Франция, Венгрия, Нидерланды, Норвегия и Южная Корея. В 2016–2017 гг. этот список должен пополниться еще рядом государств, и многие из них ориентируются на рекомендации и технические руководства МАГАТЭ.

Кроме того, даже в тех государствах, где отсутствуют единый профильный регулятор для сектора ГЯО и соответствующее национальное законодательство, отмечается повышение активности регуляторов, сконцентрированной на ГЯО. В процесс выработки регулирующих норм все больше вовлекаются операторы таких объектов. Один из примеров — Россия, где в 2014 г. концерн *Росэнергоатом* начал активно адаптировать требования, содержащиеся в приказах о защите информации, принятые ранее Федеральной службой технического и экспортного контроля (ФСТЭК), для обеспечения ИБ при эксплуатации АЭС. Государства с развитой системой регуляторных норм для секторов ядерной энергетики и кибербезопасности активно переходят от регулирования отдельных вопросов ИБ ГЯО (защита информации в корпоративных сетях ядерных объектов, физическая изоляция таких сетей, лицензирование ИТ-поставщиков, обслуживающих ГЯО, и т. д.) к комплексным системам требований, которые бы обеспечивали гибридное регулирование вопросов на пересечении ФЯБ и кибербезопасности. Отдельного упоминания заслуживают США, где в 2010 г. были опубликованы всеобъемлющие и обязательные для всех операторов ГЯО требования Комиссии по ядерному регулированию NRC RG 5.71 *Программы кибербезопасности для ядерных установок*.

Наконец, прослеживается растущий интерес госорганов к участию в международных дискуссиях и разработке инициатив в сфере обеспечения кибербезопасности ГЯО. В июне 2015 г. 92 правительственные делегации приняли участие в первой

Международной конференции по компьютерной безопасности в ядерном мире, проведенной в штаб-квартире МАГАТЭ в Вене. Стоит отметить, что число участников конференции превысило число государств, имеющих гражданскую ядерную отрасль промышленности. Ряд инициатив и предложений, выдвинутых отдельными государствами, получили международную поддержку. Наконец, национальные научные и экспертные сообщества также демонстрируют растущий уровень активности в сфере кибербезопасности ГЯО.

Состояние международного сотрудничества в обеспечении кибербезопасности ГЯО

На международном уровне повестка дня в сфере обеспечения кибербезопасности ГЯО и противодействия актуальным киберугрозам развивается в условиях нормативного вакуума и отсутствия механизмов совместного управления инцидентами и их расследования. С одной стороны, такая ситуация типична для традиционных задач ФЯБ, когда угрозы локализованы, а необходимость обеспечивать безопасность и конфиденциальность превалирует над потребностью в тесном взаимодействии. Однако такой подход недостаточно эффективен, когда речь идет об обеспечении кибербезопасности ГЯО, поскольку зачастую киберугрозы имеют трансграничный характер. Даже если исходить из того, что какое-то конкретное государство способно обеспечить полную защиту своих мирных ядерных объектов от сетевых компьютерных атак, оно тем не менее останется зависимым от международных поставщиков и цепочек поставок ИТ-продуктов и сервисов, используемых на таких объектах. К примеру, в топ-3 поставщиков автоматизированных систем управления и сбора данных (SCADA) входят две компании из США и одна из Германии: Schneider Electric, Siemens и Rockwell Automation. Для большинства из сотен систем программного и аппаратного обеспечения, используемых на любом ГЯО, наиболее популярные решения поставляются крупными транснациональными компаниями. Полная локализация разработки и поставки ИТ-систем ГЯО невозможна. Поэтому операторам приходится мириться с тем, что в используемом им программном и аппаратном обеспечении могут присутствовать недоработки, дефекты и уязвимости, способные открыть дверь для кибератак. Тем не менее, несмотря на убедительные доводы в пользу необходимости международного сотрудничества в области кибербезопасности, в настоящее время уровень взаимодействия по ГЯО отстает от уровня взаимодействия по *традиционным* вопросам ядерной безопасности и противодействию *аналоговым* угрозам.

В частности, кибератаки против ГЯО не подпадают под действие существующих международных механизмов противодействия киберпреступлениям и их расследования. Наиболее известным механизмом такого рода является Будапештская конвенция о борьбе с компьютерными преступлениями, принятая Советом Европы в 2001 г. и открытая для подписания всеми странами. Схожая ситуация имеет место в отношении региональных соглашений в сфере кибербезопасности, например, межправительственного соглашения государств Шанхайской организации сотрудничества (ШОС) о сотрудничестве в области обеспечения международной информационной безопасности от 2009 г., а также двусторонних соглашений (российско-американская серия соглашений 2013 г., российско-китайское двустороннее соглашение 2015 г. и пр.).

Киберинциденты на ГЯО также не подпадают под действие необязывающих юридически трансграничных механизмов сотрудничества, таких как альянс Международного союза электросвязи (МСЭ) и международного государственно-частного партнерства ИМПАКТ или FIRST (международный Форум по взаимодействию между центрами реагирования на инциденты кибербезопасности). Более того, не выработана международная система стандартизации в отношении специфических ИТ-продуктов и сервисов, которые поставляются операторам ГЯО. Такая система могла бы включать набор требований по защите цепочек поставок особо важных ИТ-компонентов (программные и аппаратные комплектующие АСУ ТП АЭС), а также стандарты, описывающие надежную изоляцию промышленных сегментов сетей ГЯО от интернета, и т. д. Наконец, отсутствуют общие критерии и стандарты аудита кибербезопасности на ГЯО.

Кроме того, международные нормы и договоры по вопросам кибербезопасности ГЯО до сих пор отсутствуют. Существующие международные соглашения по ядерной безопасности и ядерному нераспространению были приняты раньше, чем на повестку дня вышли вопросы защиты объектов мирного атома от киберугроз. Обновление ранее принятых соглашений с учетом этой новой проблемы потребует долгосрочных усилий без гарантированного результата. Кроме того, отсутствие режима международного регулирования киберпространства в целом сказывается и на возможностях обеспечения кибербезопасности в секторе ГЯО.

Вместе с тем за последние годы был разработан ряд проектов соглашений и норм ответственного поведения в киберпространстве. В том числе такие проекты норм и правил поведения продвигала на международных площадках Россия — самостоятельно и вместе со своими партнерами по ШОС в 2011 и 2015 гг. Однако соблюдение предлагаемых норм может быть затруднено, поскольку позитивные и негативные механизмы для этого отсутствуют. Такое препятствие будет неизбежно возникать, пока не будут выработаны эффективные решения проблем атрибуции в киберпространстве и верификации предлагаемых мер. То же относится и к идеям о создании специального договора, который бы запрещал атаки на ГЯО и установки, содержащие опасные силы (включая АЭС), в соответствии с определениями статьи 56 Дополнительного протокола I к Женевским конвенциям 1949 г.

Тем не менее можно констатировать определенный прогресс и наличие открытого окна возможностей для выработки норм в связи с деятельностью Группы правительственных экспертов ООН (ГПЭ ООН) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. В июне 2015 г. четвертый созыв Группы завершил подготовку доклада Генерального секретаря ООН, в котором государствам — членам ООН был предложен список необязывающих добровольных норм, закладывающих основу для ответственного поведения в киберпространстве. Из числа этих норм как минимум две: запрет кибератак на КВО и обеспечение целостности цепочек поставок критически важной ИТ-продукции, — можно и нужно применить для обеспечения кибербезопасности сектора ГЯО.

Хотя эти нормы и не являются обязательными, если они будут приняты и поддержаны широким кругом государств, они могут стать основой для последующих, более конкретных и юридически обязательных международно-правовых документов. Кроме того, такие наработки ГПЭ ООН могут послужить механизмом укрепле-

ния международного взаимодействия с участием частного сектора, нацеленного на обеспечение целостности цепочек поставок ИТ-систем ГЯО, а также на решение других актуальных проблем.

Роль МАГАТЭ

Основополагающую роль в проработке вопросов кибербезопасности ГЯО до сих пор сохраняет за собой МАГАТЭ. Агентство начало поднимать эту тему на своих Генеральных конференциях с 2012 г., но поворот к систематической работе по обеспечению кибербезопасности ядерных установок произошел в 2013 г. Именно тогда была запущена Программа компьютерной и информационной безопасности при Управлении ядерной безопасности агентства. Цель программы — обеспечить государства — члены МАГАТЭ необходимыми рекомендациями, для того чтобы поддержать их деятельность по реагированию на трансграничные кибератаки, которые так или иначе затрагивают ядерные и другие радиоактивные материалы, а также связанные с ними объекты и виды деятельности. Программа включает шесть направлений деятельности МАГАТЭ в этой области, в том числе разработку технических руководств, организацию и поддержку форумов по обмену технической информацией, региональные тренинговые мероприятия, региональную и международную экспертную поддержку, предметную экспертизу по реагированию на инциденты, а также деятельность по повышению информационного охвата.

В настоящее время МАГАТЭ в своих рекомендациях по ядерной безопасности рассматривает кибербезопасность как фактор, способный повлиять на обеспечение должного уровня ФЯБ и, таким образом, подлежащий проработке и учету в контексте ФЯБ. Кроме того, в рекомендациях агентства, отмечается необходимость защиты от взлома компьютеризованных систем обеспечения ядерной безопасности (в том числе систем физической защиты и систем учета и контроля ядерных материалов).

Значимой инициативой, запущенной агентством в 2015 г., стала Международная конференция по компьютерной безопасности в ядерном мире, привлекшая широкий международный круг участников. В пятидневной конференции приняли участие представители 92 государств и 14 международных организаций. В общей сложности было представлено 172 доклада, в том числе доклады, содержащие проработанные сценарии возможных инцидентов на объектах ГЯО. Среди таких сценариев рассматривался и ход многоэтапных кибератак на АЭС. Конференция может стать важным каналом для повышения осведомленности о вызовах кибербезопасности ГЯО среди развивающихся стран, а также площадкой для обмена лучшими практиками. Несмотря на то что технические руководства и рекомендации МАГАТЭ по обеспечению компьютерной безопасности ядерных установок не являются обязательными для выполнения, они оказываются все более актуальными для тех стран, которые находятся на начальных этапах разработки собственной регуляторной базы в этой области. Также в отсутствие норм и трансграничных механизмов сотрудничества по предотвращению, расследованию и подготовке отчетности по киберинцидентам на ГЯО усилия МАГАТЭ по повышению осведомленности и наращиванию потенциала реагирования имеют особую ценность. Однако для более эффективной борьбы с киберугрозой агентству, возможно, имело бы смысл подтолкнуть государства-члены и международное сообщество

к диалогу по поводу формирования более практико-ориентированных механизмов и форматов трансграничного сотрудничества в данной сфере.

КИБЕРУГРОЗЫ ГЯО: БАЗОВАЯ МОДЕЛЬ КЛАССИФИКАЦИИ И ПРИМЕРЫ ИНЦИДЕНТОВ

На сегодняшний день не выработана универсальная классификация кибернетических воздействий на ядерные установки, равно как и на другие КВО.

Предлагаемая МАГАТЭ трехкомпонентная классификация позволяет выделить основные виды компьютерных инцидентов в зависимости от их последствий. Однако классификация агентства не позволяет установить источник и характер угрозы, а также определить базовые технические параметры для описания инцидентов. К таким параметрам относятся, в частности, затронутые атакой системы, возможные векторы угрозы, сценарии кибератаки и т. д. Существуют и более подробные классификации, описывающие виды инцидентов кибербезопасности на объектах КИ по признаку элементов информационных систем, которые могут выступать целью атаки. Одна из подобных широких классификаций для неядерных объектов КИ энергетической отрасли была разработана ОБСЕ в 2014 г.

За некоторыми оговорками, такой подход также применим к сектору ГЯО, поскольку информационные системы ядерных и неядерных объектов КИ по основным параметрам схожи. Подобную классификацию может использовать ИТ-департамент ГЯО в качестве полезного теоретического примера. Однако для принятия решений оператору ГЯО и структурному подразделению, отвечающему за обеспечение кибербезопасности на таком объекте, скорее необходима многомерная *ось координат*, позволяющая классифицировать инцидент по различным критериям. В частности оператору потребуется установить, чем вызван инцидент: действием человеческого фактора или технологическим сбоем; является нарушитель внутренним или внешним по отношению к системе; какова цель атакующего; какие системы могут быть затронуты инцидентом и т. д. Отсутствие такой *оси координат* — пробел, который следует закрыть совместными усилиями ИТ-отрасли, операторов и регуляторов. В качестве первого шага в этом направлении может быть предложена базовая модель классификации, позволяющая выстроить типологию инцидентов на ГЯО.

Надежная статистика инцидентов для сектора ГЯО не ведется, поскольку практика открытой отчетности об инцидентах отсутствует в силу соображений национальной безопасности и репутационных рисков для бизнеса. На основе открытых данных можно найти информацию как минимум о 14 серьезных инцидентах кибербезопасности на ГЯО за последние 25 лет. Тринадцать из них — инциденты на АЭС, а еще один инцидент связан с кампанией *Олимпийские игры*, которая велась против мирной ядерной инфраструктуры Ирана с использованием вирусов Stuxnet, DuQu, Flame и другого профессионального вредоносного ПО. Для того чтобы заложить базу дальнейшего исследования и сформулировать выводы на основе конкретных прецедентов, были изучены четыре инцидента. В частности были проанализированы инцидент на АЭС Дэвис-Бессе (США), кибероперация *Олимпийские игры*, кибератака на корпоративную сеть штаб-квартиры оператора южнокорейских АЭС KHNP и заражение сети АЭС Гундреммингen (Германия) в апреле 2016 г. Акцент был сделан на инцидентах, вызванных злоумышленными действиями, включая применение вредоносного ПО или других средств целенаправленного кибернетического воз-

действия. Хотя большинство из этих инцидентов хорошо известны, дополнительную ценность может иметь их анализ с точки зрения базовой модели классификации и описанной выше концепции комплексной среды кибербезопасности. Вместе с тем инциденты в корпоративной сети KHNP и в сети АЭС Гундремминген произошли относительно недавно, а их исследование может способствовать лучшему пониманию логики целенаправленных кибератак на ГЯО, что стало востребованной темой после кампании *Олимпийские игры*. При обобщении результатов проведенного анализа конкретных инцидентов в первую очередь нужно отметить, что было сформировано новое понимание ландшафта киберугроз в рассматриваемой области. Дальнейший углубленный анализ позволит развить и конкретизировать существующий ландшафт. Однако уже на этой стадии исследовательской работы несколько базовых тенденций выглядят неоспоримыми. Они требуют согласованной реакции от всех заинтересованных сторон, включая операторов ГЯО, ИТ-поставщиков, национальных регуляторов и международные площадки.

Во-первых, в отличие от 1990-х и 2000-х гг., сегодня в отношении ГЯО преимущественно используются киберугрозы повышенной опасности. Предположительно, они могут исходить от государственных игроков. Эти угрозы сочетают в себе средства кибершпионажа и киберсаботажа. При этом такие кибератаки тщательно спланированы: они нацелены на поражение критических систем и затрагивают сотрудников ядерных объектов. Наиболее серьезный вызов кибербезопасности ГЯО исходит от инцидентов, вызванных целенаправленным внешним человеческим вмешательством. Сегодня отсутствуют средства, которые позволяли бы комплексно и эффективно бороться с постоянными угрозами повышенной опасности, особенно в международном масштабе. Основными причинами этого являются неразрешенная проблема атрибуции и отсутствие международных норм и форматов для решения подобных вопросов.

Во-вторых, выявления и расследования инцидента может быть недостаточно для окончательного устранения угрозы. В случае с киберугрозами повышенной опасности, нацеленными конкретно на ГЯО, вредоносное ПО не является *одноразовым оружием*, как его зачастую описывают. Для атак используются комплексные пакеты ПО (тулкиты) и компьютерные черви с множеством модулей, которые легко подвергаются модификации и в каждой своей обновленной версии представляют новую угрозу кибербезопасности КВО.

Более того, как показывают примеры кампании *Олимпийские игры* и атаки на KHNP, однажды внедренное на объект вредоносное ПО начинает жить собственной жизнью независимо от планов своих создателей. Так, оно может превратиться во вредоносный проект с открытым исходным кодом, который доступен для модификации всем игрокам, обладающим необходимыми ресурсами и навыками. Ярким примером этого служит инцидент со Stuxnet. Спустя несколько лет после него производные версии ПО, использованного во время кампании *Олимпийские игры*, нарушили функционирование внутренней сети промышленного комплекса нефтедобывающей компании Saudi Aramco и заразили ряд КИ по всему миру, включая АЭС в России (хотя ущерба заражение не повлекло).

В-третьих, векторы угроз в рассмотренных примерах инцидентов на ГЯО смещаются в сторону от того спектра, который уже стал привычным в рамках концепции ядерной безопасности. Обеспечение безопасности внутреннего периметра

сетей ГЯО теперь идет рука об руку с интернет-безопасностью. Например, так было в случае кибератаки, когда целью номер один для ее авторов стали бывшие сотрудники южнокорейской АЭС. Борьба с кибершпионажем в отношении ГЯО также осложняется необходимостью разработки стратегии противодействия злоумышленникам в медиапространстве. Наконец, следует отметить, что угрозы не приходят поодиночке: кибершпионаж идет в связке с традиционным шпионажем и киберсаботажем. Сектор гражданской ядерной инфраструктуры теперь развивается в условиях постоянного наличия комплексных угроз, хотя они и пришли в сектор ГЯО позже, чем в другие сектора КИ. Кибератаки из краткосрочных спонтанных акций превратились в тщательно продуманные кампании — отныне их жизненный цикл может длиться годами. Соответственно, для эффективной борьбы с такими атаками требуется поддержание среды кибербезопасности с аналогичным по длительности жизненным циклом. Это вновь подчеркивает необходимость создания проактивной комплексной стратегии обеспечения кибербезопасности в режиме реального времени, которая должна прийти на смену подходу, основанному лишь на реагировании на уже случившиеся инциденты.

ПРЕОДОЛЕНИЕ УГРОЗЫ — ПЕРВЫЕ ШАГИ

Технический уровень

На техническом уровне необходимо внедрить новые подходы к обеспечению кибербезопасности ГЯО, прежде всего обеспечить взаимодействие операторов таких объектов с ИТ-вендорами. Необходимо свести к минимуму потенциальные риски скрытого функционала в критически важных ИТ-компонентах (АСУ ТП) за счет более интенсивного и обеспеченного ресурсами тестирования на проникновение (пентеста), анализа предельных значений (фаззинга) и глубокого сканирования прошивок программно-конфигурируемых устройств нижнего уровня.

Существенным шагом вперед мог бы стать консенсус о введении обязательства со стороны поставщиков раскрывать исходный код критически важных компонентов АСУ ТП при заключении контракта с оператором ГЯО. Сама отрасль АСУ ТП к такому требованию отнесется без энтузиазма — скорее, речь может идти о достижении компромисса по итогам длительного торга между отраслью и операторами ГЯО. Продуманное вмешательство со стороны регулятора могло бы дать поставщикам АСУ ТП стимул делиться с операторами исходными кодами своей продукции, не вынуждая их уходить с рынков отдельных государств, где могут быть введены такие требования.

Значимой составляющей нового подхода может стать и концепция обеспечения кибербезопасности на этапе проектирования объектов, особенно применительно к АЭС и другим крупным объектам гражданской ядерной инфраструктуры. Хотя принципы этой концепции известны и имеют общую основу с физической ядерной безопасностью на этапе проектирования, ее внедрение и подробное техническое видение пока по большей части находится в стадии разработки. Более тесный обмен опытом и лучшими практиками между ведущими ИТ-поставщиками и операторами ГЯО может помочь продвинуться вперед в решении этой задачи.

Наконец, необходимость защиты от внешних вторжений в АСУ ТП возвращает дискуссию к необходимости обеспечения не только доступности, но и конфиденци-

альности информации в критически важных ИТ-системах ГЯО. Для отрасли может оказаться целесообразным внедрение современных средств шифрования данных для обеспечения безопасности потоков межмашинных (M2M) данных между АСУ ТП. Как и в случае с раскрытием исходного кода прошивок ключевых продуктов, такой шаг будет непростым, поскольку внедрение криптографии создаст дополнительные издержки для операторов ГЯО. Однако, как показывают примеры недавних инцидентов, такие издержки могут оказаться меньшим из двух зол.

Уровень национальных регуляторов

На национальном уровне приоритетной целью является полная интеграция кибербезопасности ГЯО в концепцию ФЯБ, что позволит устранить функциональные бреши и дублирование функций между регуляторами, отвечающими за кибербезопасность и ядерную безопасность. Такая интеграция также необходима для разработки целостной стратегии обеспечения кибербезопасности на этапе проектирования объектов. Сегодня внимание этой задаче в основном уделяет МАГАТЭ, однако данная тема должна в первую очередь обсуждаться на национальном уровне в рамках диалога между регуляторами и получать должное внимание со стороны государственных органов.

Предпосылкой для успеха такого диалога может стать разработка комплексного законодательства, рассматривающего кибербезопасность ГЯО в качестве отдельного предмета. Развивающимся странам такое законодательство необходимо для того, чтобы определить ключевые приоритеты для государства и заполнить нормативный вакуум, который препятствует разработке операторами ГЯО собственных внутренних стандартов и технических руководств. МАГАТЭ и другие международные площадки сохраняют за собой определяющую роль при содействии такой работе на национальном уровне, поскольку именно они накапливают лучшие практики передовых стран и могут консультировать развивающиеся страны на предмет лучших образцов и моделей подходов.

Сближение парадигм кибербезопасности и ФЯБ также требует проведения масштабной работы над человеческим капиталом. Перед госорганами и операторами ГЯО стоит задача вырастить поколение специалистов с новым профессиональным видением, отличным от традиционного подхода к обеспечению ФЯБ, но при этом способным дополнить и обогатить его. На уровне внутригосударственной политики этому могут способствовать инновации в системе высшего образования и поддержка тренингов, семинаров и диалоговых форматов с участием представителей как сектора ядерной энергетики, так и ИТ-отрасли. Деятельность *мозговых центров* и неправительственных организаций по организации тренингов и повышению осведомленности об этих вопросах также должна получить поддержку. На международном уровне незаменимую роль играют тренинги, практические семинары и мероприятия по повышению осведомленности, организуемые МАГАТЭ.

Международный уровень

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.

Кроме того, некоторые возможности видятся в деятельности формата ГПЭ ООН. В августе 2016 г. стартовали встречи пятого созыва Группы, что дает шанс на достижение договоренностей и выработку добровольных норм ответственного поведения в конкретных секторах КИ. Решение о том, для каких секторов КИ в первую очередь следует разработать нормы, пока не принято, и в этом кроется возможность вынести вопросы обеспечения кибербезопасности ГЯО на самый верх повестки дня Группы. При таком развитии событий в следующий доклад, который готовит ГПЭ, могла бы войти добровольная норма, запрещающая государствам участвовать в кибератаках на ГЯО или предлагающая некий механизм добровольных самоограничений в части таких действий. Даже не имея юридически обязательной силы, такая норма помогла бы продвинуть дискуссию о кибербезопасности и приблизить появление будущего обязывающего межправительственного соглашения. Кроме того, работа ГПЭ может стать определяющей для разрешения вопросов формирования понятийного аппарата и классификации секторов КИ, а также классификации кибератак против объектов в этих секторах, включая ГЯО. Такая работа стала бы вкладом в достижение более широкой цели по разработке общего языка и общего видения для обсуждения вопроса кибербезопасности ГЯО на международном уровне. Наконец, некоторые более ранние предложения ГПЭ могли бы быть доработаны конкретно под сектор ГЯО. Примером может служить норма об обеспечении целостности цепочек поставок для критически важных ИТ-систем.

Помимо ГПЭ ООН, международные государственно-частные партнерства, такие как альянс ИМПАКТ-МСЭ, могут сыграть важную роль в обеспечении обмена данными о киберинцидентах на объектах ГЯО, накоплении лучших практик и создании баз данных уязвимостей, вредоносного ПО и скрытого функционала, используемых для кибератак на объекты ГЯО.

Список сокращений

BYOD — Bring your own device — «приноси свое устройство»

SCADA — Supervisory Control and Data Acquisition — автоматизированная система управления и сбора данных (конкретный вид АСУ ТП)

АСУ ТП — автоматизированные системы управления технологическими процессами

АЭС — атомная электростанция

ГПЭ ООН — Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

ГЯО — объект гражданской ядерной инфраструктуры

ИБ — информационная безопасность

ИТ — информационные технологии

КВО — критически важный объект

КИ — критическая инфраструктура

МАГАТЭ — Международное агентство по атомной энергии

ИМПАКТ-МСЭ — Альянс «Международное многостороннее партнерство по борьбе с киберугрозами — Международный союз электросвязи»

ОБСЕ — Организация по безопасности и сотрудничеству в Европе

ПО — программное обеспечение

ТП — технологические процессы

ФСТЭК — Федеральная служба технического и экспортного контроля

ФЯБ — физическая ядерная безопасность

ШОС — Шанхайская организация сотрудничества

КИБЕРБЕЗОПАСНОСТЬ АСУ ТП – КОММЕНТАРИИ ЭКСПЕРТОВ

Формирование рынка кибербезопасности АСУ ТП[2]

Процесс становления рынка защиты автоматизированных систем управления технологическими процессами (АСУ ТП) принципиально отличается от схожих процессов на сформированных ранее в России рынках, например, антивирусного рынка или рынка защиты от утечек. Это объясняется рядом предпосылок.

Во-первых, на рынке АСУ ТП существует большое количество конкурирующих поставщиков оборудования и различных технологических решений — рынок сильно зависит от оборудования (hardware). Это базовое отличие от рынка антивирусов, которые, как и вирусы, по большому счету создаются под пару основных операционных систем. Во-вторых, создание универсального программного обеспечения (software) для такого огромного количества систем представляется затруднительным. В-третьих, производители ведут себя закрыто — не стремятся делиться созданными протоколами. Наконец, подавляющее большинство систем, которые предлагаются на российском рынке, импортные. Нужно учитывать, что сотрудничество с иностранными производителями осложняется, потому что зачастую они представлены крупными корпорациями со сложной структурой принятия решений, к которым непросто обратиться с предложением, например, улучшить софт под решение конкретной проблемы конкретного предприятия.

Рынок АСУ ТП, формирующийся сейчас в России, имеет смысл рассматривать с позиций четырех групп. Первую группу представляют клиенты — крупные компании. Складывается интересная ситуация: с одной стороны, компании озабочены информационной безопасностью, собирают по этому поводу внутренние совещания. С другой — как только

речь заходит о внедрении конкретной системы или о проведении проверки, клиенты начинают приуменьшать риски, говоря, что у них все защищено. Позиция директоров по безопасности крупных компаний заключается в том, что вероятность внедрения злоумышленников в систему мала и несущественна, а потому на нее не стоит обращать внимания, то есть налицо массовое непризнание проблемы со стороны клиентов.

Вторая группа состоит из производителей средств АСУ ТП. Производители также не стремятся обсуждать существование проблемы и придавать значение уязвимостям в системах. Порой можно встретить следующее: представители компаний-производителей, рассказывая о том, что последствия от проникновения вируса в систему клиента были устранены за пять дней, позиционируют такой случай как успешный.

Третья группа представлена регуляторами. Первым ведомством в этом списке стоит поставить Федеральную службу по техническому и экспортному контролю (ФСТЭК) — в марте 2014 г. именно эта служба выпустила регулирующий документ как раз по защите критической инфраструктуры. Документ был подготовлен буквально за полгода, что говорит о действительном осознании проблемы. Однако, кроме регулирующих документов ФСТЭК, существуют еще отраслевые регламенты безопасности, а также международные регламенты безопасности — все они, строго говоря, противоречат друг другу. Различия этих регламентов касаются даже количества уровней безопасности, которые они выделяют — от четырех до семи.

Наконец, четвертая группа заинтересованных лиц на рынке состоит из компаний, которые занимаются разработкой средств информационной безопасности — систем, которые защищают от вирусов, от утечек, строят системы контроля доступа и т.д. Именно эти игроки заметили проблему, и именно они привлекают к ней внимание, потому что другие группы в этом менее заинтересованы.

Таким образом, получается, что единого взгляда на проблему у четырех заинтересованных групп нет, а это приводит к тому, что рынок развивается скачкообразно и довольно медленно.

В настоящее время заметно, что клиенты боятся ставить серьезные системы в разрыв, например, на атомной станции или на крупном транспортном узле. Существующие системы, в основном системы мониторинга, которые помогают лишь обнаружить проблему, но не решить ее. Именно поэтому сейчас рынок АСУ ТП в основном пытается проводить аудит безопасности и на основании этого предлагать решения, которые создаются, по сути, под каждого отдельного крупного клиента. Это объяснимо, потому что система, разработанная, скажем, под РЖД, будет отличаться от системы, созданной для защиты АЭС.

В силу закрытости рынка сложно определить, какие отрасли действительно являются наиболее уязвимыми, а какие — наименее. В целом же представляется, что те предприятия, которые стремятся внедрять у себя промышленный Интернет вещей, сейчас находятся в более уязвимом положении, чем те, которые подходят к этому вопросу консервативно. На мой взгляд, выгоды от более развитого уровня автоматизации промышленных систем меркнут перед возможными катастрофическими последствиями, если в эту систему через интернет проникнет вирус.

Наталья Касперская,
директор InfoWatch

Цифровые угрозы в физическом мире — дешевые и трансграничные[3]

В течение долгого времени физический и цифровой миры не пересекались — так было до появления систем АСУ ТП. Эти цифровые компьютерные системы непосредственно влияют на нашу жизнь, поскольку каждый завод сегодня управляется при помощи компьютерных систем, а также транспорт, электростанции и т. д.

Как мы знаем из опыта, компьютерные системы содержат уязвимости, они подвержены атакам. Таким образом, ситуация, когда два мира соприкасаются, приводит к переносу цифровых угроз в физическую реальность. Сегодня уже известны случаи, когда компьютерные инциденты приводили к нежелательным последствиям в физическом мире. Например, в декабре 2015 г. в шести областях Украины вследствие хакерской атаки произошло отключение электроэнергии — от сети были отключены 225 тыс. пользователей. В том же месяце на сталелитейном предприятии в Германии произошел киберинцидент, в результате которого была выведена из строя доменная печь.

Однако проблема переноса цифровых угроз в физический мир касается не только вмешательства в технологические процессы. Одна из тенденций последнего времени — распространение Интернета вещей. Под этим понятием подразумеваются те же самые устройства, но управляемые высокими технологиями. При этом воздействовать на подобные «умные вещи» можно удаленно, без физического контакта с ними. Также стоит помнить, что цифровые технологии характеризуются очень низкой стоимостью воспроизведения. Если высококвалифицированные исследователи нашли уязвимость и смогли использовать ее, повторение этого вслед за ними не требует высокой квалификации.

Компьютерные технологии трансграничны. Какие бы средства ни были разработаны для защиты от тех или иных компьютерных инцидентов и проблем, они должны согласованно применяться в разных странах мира. Сейчас уже сложилась хорошая практика международного сотрудничества в области расследования инцидентов на базе Интерпола и Европола, но этого недостаточно. В настоящее время отсутствуют соглашения между государствами даже об использовании интернета — практически отсутствует правовое регулирование интернета. Для регулирования отношений в этой новой для человечества области необходимо сотрудничество между государствами.

Андрей Духвалов,
руководитель Управления перспективных технологий,
Лаборатория Касперского

Примечания

1 Приложения к докладу, а также другие аналитические и информационные материалы по теме «Кибербезопасность объектов критической ядерной инфраструктуры» можно найти на сайте проекта http://cynuc.pircenter.org.

2 Текст комментария составлен на основе выступления Н.И. Касперской на международной конференции «Повестка XXI века — новые технологии и вызовы глобальной безопасности», проведенной ПИР-Центром и Дипломатической академией МИД России 29 сентября 2016 г.

3 Текст комментария составлен на основе выступления А.П. Духвалова на международной конференции «Повестка XXI века — новые технологии и вызовы глобальной безопасности», проведенной ПИР-Центром и Дипломатической академией МИД России 29 сентября 2016 г.