Подготовлен ПИР-Центром в сотрудничестве с Centre russe d'etudes politiques, Женева в рамках рабочего процесса по кибербезопасности ядерных установок при Совете по глобальной повестке Всемирного экономиечского форума

КИБЕРБЕЗОПАСНОСТЬ ГРАЖДАНСКИХ ЯДЕРНЫХ ОБЪЕКТОВ: ОЦЕНКА УГРОЗ И ОПРЕДЕЛЕНИЕ ДАЛЬНЕЙШИХ ШАГОВ

Резюме доклада*

Подготовлен ПИР-Центром

в сотрудничестве с
Centre russe d'etudes politiques, Женева

В рамках Рабочего процесса по кибербезопасности ядерных установок при Совете по глобальной повестке,

Всемирный экономический форум

Июнь 2016

Москва – Женева

Резюме

Вызовы кибербезопасности стали одной из ключевых проблем для операторов критической инфраструктур (КИ) во всех секторах. Стремительный прогресс в наращивании потенциала проактивных кибероперациий и резкий рост количества инцидентов кибербезопасности на объектах КИ требуют неотложных ответных мер от операторов, регуляторов и международного сообщества. Однако все эти субъекты сталкиваются с общемировыми тенденциями, которые объективно работают на рост уязвимостей кибербезопасности критических инфраструктур. К таким тенденциям относится масштабный и все еще продолжающийся переход на цифровые системы управления производственными и технологическими процессами (ПТП) на критически важных объектах (КВО), а также практика подключения офисных и даже промышленных корпоративных сетей объектов КИ к Интернету, получающая все более широкое распространение по мере внедрения технологий Интернета Вещей и Всеобъемлющего Интернета. Доступ к Сети идет рука об руку с мобильной революцией, благодаря которой в различные секторы КИ приходят концепции «приноси-свое-устройство (BYOD) и «карманная система управления ПТП». Наконец, для большинства секторов КИ общей проблемой стала исключительная сложность трансконтинентальных цепочек поставок систем управления ПТП, программного

* Полный текст доклада будет опубликован на странице cynuc.pircenter.org сайта ПИР-Центра

обеспечения для контроля таких систем (включая автоматизированную систему управления и сбора данных SCADA), а также устройств нижнего уровня.

Хотя эти тенденции проявляются во всех секторах КИ, сектор гражданских ядерных объектов (ГЯО) стоит особняком в силу целого ряда уникальных характеристик. Одна из них – не имеющий аналогов уровень инфраструктурной сложности информационных систем гражданских атомных объектов, которые включают сотни систем управления ПТП и многие тысячи датчиков на каждую атомную электростанцию (АЭС). Фактор инфраструктурной сложности создает три препятствия к обеспечению кибербезопасности ГЯО. Первое препятствие – уникальные и не имеющие аналогов для каждого объекта атомной энергетики архитектурные решения в сфере обеспечения кибербезопасности и сетевой безопасности. Такая особенность существенно ограничивает возможности применения предыдущего опыта и лучших практик. Второе – проблема доверия к вендорам и обеспечения целостности цепочек поставок ИТ-продукции приобретает крайне серьезный характер. В-третьих, сложная инфраструктурная среда требует комплексного и всеобъемлющего подхода к кибербезопасности, включая обеспечение кибербезопасности на этапе проектирования объекта, управления сетевыми событиями в реальном времени, внедрения шифрования данных и, возможно, раскрытия исходного кода программной прошивки устройств нижнего уровня вендорами для операторов ГЯО.

Вторая уникальная особенность сектора ГЯО в плане обеспечения их кибербезопасности состоит в неопределенной роли и месте собственно кибербезопасности по отношению к физической ядерной безопасности. Область кибербезопасности формируется на пересечении промышленной безопасности автоматизированных систем управления производственными и технологическими процессами (АСУ ПТП), физической ядерной безопасности (ФЯБ) и информационной безопасности (ИБ). Интеграция кибербезопасности ГЯО и физической ядерной безопасности на сегодня не завершена, что порождает ряд вызовов, включая нечеткое разделение функций между регуляторами, взаимно противоречащие требования, стандарты и процедуры, а также понятийные и концептуальные зазоры между двумя упомянутыми нишами безопасности.

Если говорить об общей картине на уровне регуляторов, в большинстве государств кибербезопасность ГЯО лишь начинает оформляться в качестве отдельного предмета регулирования на общенациональном уровне. Основные проблемы включают нечеткое распределение регуляторной повестки между государственными органами, а также зазоры и дублирование регуляторных функций. Во многих развивающихся странах такие функции бессистемно рассредоточены между множеством регуляторов, которые недостаточно взаимодействуют друг с другом. Еще одна проблема – отсутствие профильного для сектора регулятора, что обуславливает слабую обратную связь от представителей частного сектора. Кроме того, несмотря на доскональную проработку концепции физической ядерной безопасности, ее негибкость иногда препятствует разработке гибридного регуляторного подхода, который бы охватывал специфические вопросы сектора гражданской ядерной инфраструктуры. К этому зачастую добавляется нехватка интеграции международных рекомендаций, руководств и лучших практик в регуляторные нормы по обеспечению кибербезопасности ГЯО на национальном уровне.

Тем не менее, с начала 2010-х гг. во многих юрисдикциях наблюдается постепенный

Подготовлен ПИР-Центром в сотрудничестве с Centre russe d'etudes politiques, Женева в рамках рабочего процесса по кибербезопасности ядерных установок при Совете по глобальной повестке Всемирного экономиечского форума

прогресс: ускоряется разработка отраслевого законодательства по кибербезопасности; регуляторная активность в отношении кибербезопасности ГЯО растет даже в тех странах, где эти вопросы не закреплены за каким-либо единым профильным ведомством (например, в России). Наконец, растет интерес правительств к международным дискуссиям и инициативам по кибербезопасности ГЯО. Показателем служит растущее вовлечение правительств в работу профильных международных конференций и диалоговых площадок.

На международном уровне дискуссия о кибербезопасности ГЯО протекает в условиях нормативного вакуума и отсутствия механизмов совместного реагирования на инциденты кибербезопасности и их расследования. Например, не существует обязывающих рамочных норм, за счет которых бы обеспечивалась целостность цепочек поставок АСУ ПТП для АЭС. Кроме того, кибератаки против ГЯО не подпадают под действие международных механизмов противодействия и предотвращения компьютерных преступлений, таких как Конвенция по борьбе с компьютерной преступностью Совета Европы от 2001 г. Также не имеется и специальных международных норм или договоров, разработанных конкретно для обеспечения кибербезопасности ГЯО. Предлагаемые проекты договоров и подходы к адаптации имеющихся норм будут упираться в серьезные ограничения в части применения и соблюдения до тех пор, пока не будут найдены эффективные решения проблемы атрибуции и установления ответственности за действия в киберпространстве. Тем не менее, открытым остается окно возможностей, связанное с деятельностью Группы правительственных экспертов ООН (ГПЭ ООН). Предложенные Группой добровольные необязывающие нормы по запрету кибератак на объекты КИ и соблюдению целостности цепочек поставок ИТ-продукции могут стать значимым шагом к продвижению глобальной дискуссии о кибербезопасности ГЯО.

В части технических руководств, тренингов, наращивания потенциала и повышения осведомленности ключевую – и постоянно растущую роль играет МАГАТЭ. Важным шагом по концентрации международного внимания на проблеме стала Международная конференция по компьютерной безопасности в ядерном мире, впервые проведенная Агентством в 2015 г. Однако для эффективного противодействия угрозам в этой сфере Агентству, по всей видимости, следует подтолкнуть государства-члены к углубленным и более практическим механизмам и форматам трансграничного сотрудничества.

Один из ключевых моментов в разговоре о киберугрозах гражданским ядерным объектам сегодня – отсутствие универсальной таксономии кибернетических воздействий на ядерные установки. МАГАТЭ, ОБСЕ и другие организации пытаются закрыть эту брешь за счет собственных классификаций, но ни одна из них не может быть названа всеобъемлющей. Хотя разработка такой всеобъемлющей таксономии остается задачей на будущее, можно использовать базовую модель классификации по трем параметрам (источник угрозы/характер угрозы/намерение субъекта) для анализа на примере четырех инцидентов кибербезопасности на гражданских ядерных объектах: заражение сети компьютерным червем на АЭС Дэвис-Бессе в 2003 г., *Стакснет* и операция *Олимпийские игры* в 2005-2012 гг., кампания шантажа и кибершпионажа против оператора АЭС KHNP в декабре 2014 г., а также заражение компьютерным червем сети АЭС Гундремминген в Германии в апреле 2016 г. Исследование этих инцидентов позволяет выявить ряд основных тенденций. Во-первых, в отличие от предыдущих десятилетий, в отношении ГЯО теперь преобладают киберугрозы повышенной сложности. Для таких угроз характерно сочетание инструментов кибершпионажа со средствами киберсаботажа и

очень тщательный выбор целей среди критических систем и сотрудников ГЯО. Кроме того, сегодня выявить и расследовать инцидент кибербезопасности может быть уже недостаточно для окончательного устранения угрозы. Современное вредоносное ПО имеет множество модулей и легко модифицируется, а сами кибератаки из краткосрочных спонтанных акций превратились в тщательно продуманные кампании и постоянные угрозы повышенной опасности, «жизненный цикл» которых может достигать многих лет. Наконец, векторы угроз в части инцидентов на гражданских ядерных объектах смещаются все дальше от привычного спектра угроз ФЯБ. Сектор гражданской ядерной инфраструктуры теперь развивается в условиях постоянной и комплексной среды угроз, хотя это происходит и немного позже по сравнению с другими секторами КИ.

Для противодействия этим вызовам необходима взаимосвязанная система мер на уровне технических решений, регуляторных подходов и выработки глобальных политик.