ПЕРСПЕКТИВЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ ЯДЕРНОЙ ЭНЕРГЕТИКИ В ПРЕДДВЕРИИ САММИТА ПО ЯДЕРНОЙ БЕЗОПАСНОСТИ В 2014 Г.

После прецедента Stuxnet киберугрозы безопасности объектов критической инфраструктуры стали восприниматься экспертами, лидерами государств и международным сообществом в целом серьезнее и острее, чем когда-либо прежде. В особенной степени эта тенденция проявилось в отношении инфраструктуры ядерной электроэнергетики – Stuxnet довольно четко показал, насколько высоки могут быть ставки. Однако вместе с тем, рост внимания к проблеме еще не означает ее успешного решения. Может ли кибератака действительно вывести из строя АЭС? Насколько уязвимо оборудование объектов ЯТЦ к компьютерным сбоям? И как развивается международное сотрудничество по обеспечению безопасности объектов ядерной инфраструктуры от киберугроз? Экспертное видение этих проблем изложила в своем комментарии Наталья Пискунова, руководитель проекта Международного форума по ядерному страхованию, эксперт Рабочей группы по международной информационной безопасности и глобальному управлению интернетом при Экспертно-консультативном совете ПИР-Центра.

***

Пискунова Наталья Александровна

Руководитель проекта,
Международный форум по ядерному страхованию

Вопросам кибербезопасности критически важных объектов инфраструктуры уделяется все большее внимание. Повсеместное внедрение информационных технологий, нарастание числа вредоносных компьютерных кодов, а также настораживающие примеры успешного вмешательства через киберпространство в работу критически важных объектов инфраструктуры высветили потенциальную уязвимость цифровых систем контроля и управления.

Кибербезопасность ядерной энергетики долгое время рассматривалась в свете этой общей проблемы. Всплеск внимания тема получила после обнаружения вируса *Stuxnet* в 2010 г. и раскрытия в нем специфических кодов, нацеленных на выведение из строя программируемых контроллеров фирмы Siemens, регулирующих скорость вращения центрифуг на заводе по обогащению урана в Натанзе. Успех кибератаки, заключающийся в скрытом выведении из строя около тысячи иранских центрифуг, вызвал серьезную озабоченность возможностью повторения подобных инцидентов на других объектах. На волне резонанса рассматривались угрозы кибернападений на атомные станции с последствиями ядерной или радиационной аварии, в том числе, в связи с возможным вторым назначением *Stuxnet* – нанесении ущерба Бушерской АЭС. В дальнейшем такие предположения не подтвердились и были подвергнуты критике со стороны экспертного сообщества. Тем не менее, угроза кибератак на объекты ядерной инфраструктуры была поднята на международный уровень обсуждения и воспринята со всей серьезностью.

Однако случаи вмешательства вредоносных компьютерных программ в работу ядерных объектов имели место и до *Stuxnet*. Так, в США в 2003 г. червь *Slammer* проник на АЭС Дэвис Бесс (Davis-Besse) и вызвал сбой в цифровой системе мониторинга параметров безопасности. Причиной послужила связь корпоративной сети компании и цифровой системы контроля и управления АЭС. Дублирование функций мониторинга аналоговой системой позволило персоналу получать необходимые данные о состоянии станции на протяжении почти пяти часов сбоя и избежать серьезных последствий.

В 2006 г. была произведена вынужденная остановка третьего блока АЭС Браунс Ферри (Browns Ferry) в связи с неисправностью рециркуляционных насосов и контроллера опреснителя конденсата. Устройства имели встроенные микропроцессоры и обменивались данными через Ethernet. Выход их из строя вызван избыточным трафиком в сети, с которым микропроцессоры не смогли справиться. Этот случай показывает взаимозависимость и уязвимость компонентов АЭС при объединении их в сеть для управления. В 2008 г. произошла автоматическая остановка второго блока на АЭС Хэтч (Edwin I. Hatch Nuclear Power Plant) вследствие поступления сигнала о внезапном падении запаса воды в резервуарах. Срабатывание аварийной защиты вызвало обновление программного обеспечения на компьютере, используемом одновременно как для сбора данных о процессах, так и для корпоративной сети АЭС. Несмотря на то, что все эти случаи не являются целенаправленными кибератаками, они демонстрируют потенциальную уязвимость объекта ядерной энергетики к вмешательству в работу цифровой системы контроля и управления.

Для атомной станции характерна особая опасность – риск ядерной или радиационной аварии, на возникновение или развитие которой может повлиять любая дополнительная ошибка оператора или отказ оборудования, вызванные сбоем в цифровой системе контроля и управления. Учитывая современный уровень проектирования атомных станций, основанный на концепции глубокоэшелонированной защиты, изолированности компьютерных сетей от интернета, дублирования цифровых систем аналоговыми в соответствии с принципом разнообразия, не представляется реальным непосредственное

воздействие кибератаки на потерю одной из функций безопасности – контроль цепной реакции деления, отвод тепла или удержание радиоактивных материалов.

Однако существует ряд моментов, не позволяющих сбрасывать киберугрозу для АЭС со счетов. Это риск скрытых подключений к интернету в корпоративной сети и ненадлежащее изолирование ее от системы управления и контроля; трудность оперативного детектирования кибератаки и отсутствие антивируса; угроза внутреннего нарушителя; риск невыполнения сотрудниками процедур безопасности; присутствующие уязвимости «нулевого дня» и редкое обновление программного обеспечения; логические бомбы и дефекты от изготовителя. Эти факторы создают техническую возможность вмешательства в цифровую систему контроля и управления при недостаточной организации системы безопасности, а вероятность наложения киберугрозы на другие исходные события, в том числе, психологическое воздействие на персонал, могут привести к развитию последствий по непредвиденному сценарию.

Таким образом, независимо от целей, масштаба и области проникновения вредоносного кода, он будет являться своеобразной проверкой на прочность для оборудования и персонала. Ядерная энергетика является привлекательным выбором для множества стран, однако нельзя уверенно гарантировать одинаковый уровень киберзащищенности всех АЭС. Поэтому кибератаки на АЭС должны рассматриваться, в первую очередь, как угрозы, которые необходимо избегать и предотвращать, дабы не испытывать безопасность ядерного объекта игрой в жребий. Последствия такой «игры» могут носить весьма неприятный характер, в том числе, трансграничный, и оказать влияние на развитие всей отрасли.

Эти выводы применимы и к другим объектам ядерного топливного цикла: предприятиям по обогащению урана, хранению и переработке ОЯТ, изготовлению топлива. Технологические процессы имеют тенденцию переводиться на компьютерное управление, а создаваемые при этом уязвимости не всегда должным образом учитываются. Отдельной угрозой можно рассматривать кибератаку на систему управления и базу данных с целью получить несанкционированный доступ к ядерным материалам при их транспортировке или хранении. Выделяют кибератаки, направленные на сбор чувствительной информации о ядерном объекте или персональных данных для последующего использования при физическом проникновении.

Вопросы кибербезопасности могут быть рассмотрены в ракурсе физической безопасности ядерного объекта. Однако кибератака может не иметь цели последующего физического проникновения на объект с целью кражи ядерного материала или диверсии. В этом специфическая особенность киберпространства и киберугроз – возможность удаленного воздействия или скрытого вмешательства в работу объекта. С этой точки зрения использование кибератак может быть выгодно действующим лицам, не рассматриваемым обычно в контексте физической безопасности ядерных объектов. Это могут быть другие государства, желающие притормозить ядерную программу без военного вмешательства или нанести экономический ущерб, или негосударственные игроки, не обладающие возможностью физического нападения на ядерный

объект, например, радикальные националистические или общественные объединения. Нахождение источников кибератаки на территории сразу нескольких стран также не позволяет перехватить или остановить нападающих в виртуальном пространстве.

Международное агентство по атомной энергии (МАГАТЭ) в настоящее время реализует проект по безопасности информационных систем, в рамках которого разрабатываются руководства по безопасности, проводятся обучающие семинары и обмен лучшим опытом предприятий атомной отрасли. В 2011 г. издано Руководство по компьютерной безопасности на ядерных предприятиях, в ближайшие годы ожидается выпуск еще трех документов. На 2015 г. запланировано проведение первой международной конференции МАГАТЭ по киберугрозам безопасности ядерных объектов. Таким образом, мероприятия по повышению кибербезопасности включены в деятельность МАГАТЭ на регулярной и долгосрочной основе.

Однако необходимо учитывать, что все документы МАГАТЭ носят лишь рекомендательный характер и не включают проведение инспекций для проверки их исполнения, как это делается в случае с гарантиями нераспространения. Анализ состояния кибербезопасности возможен, например, в рамках миссий МАГАТЭ по оценке безопасности, которые проводятся с добровольного согласия стран. При этом также надо понимать, что рекомендации по безопасности МАГАТЭ неизбежно носят запоздание по отношению к появлению новых технологий и киберугроз, поскольку они вырабатываются на основе изучения и обобщения мирового опыта, с учетом уже пройденных ошибок и найденных решений. Для атомной отрасли этот опыт нарабатывается не быстро. Поэтому технические и организационные меры сами по себе могут оказаться не способны остановить киберугрозы во всем многообразии их проявления и темпа развития новейших информационных технологий.

На полях предстоящего Международного саммита по ядерной безопасности в Гааге можно ожидать продолжение развития внимания к кибербезопасности ядерных объектов. Безусловно, поддержку получат дальнейшие инициативы по разработке руководств, обмену лучшим опытом, укреплению международного сотрудничества. Однако назревает повестка дня о сотрудничестве по предотвращению кибератак на ядерные объекты, включая отказ от разработки и собственного участия, меры по пресечению кибератак с национальных территорий и содействие в расследовании инцидентов. Условия для того, чтобы взглянуть на проблему под более широким углом, включающим источники кибератак и потенциальный интерес стран к их проведению, существуют. Остается надеяться, что возможность договориться о правилах поведения в области ядерной кибербезопасности будет использована, не дожидаясь очередного случая, когда это станет острой необходимостью.

17.10.2013