УДК 621.3

Крупнейшие хакерские атаки на АЭС в контексте мировой кибербезопасности

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

В данной статье мы остановимся на системе кибербезопасности ядерных объектов. Здесь под системой обеспечения безопасности мы понимаем совокупность соответствующего оборудования и программного обеспечения, комплекса организационных и технических мер, а также персонала, реализующего эти меры. Актуальность развития и постоянного совершенствования систем кибербезопасности ядерных объектов связана с растущей ролью компьютерных технологий и систем в управлении технологическим процессами ядерного объекта, обращении с информацией, значимой для безопасности ядерного объекта, и в управлении другими системами безопасности. Также безусловным индикатором необходимости развития и совершенствования систем кибербезопасности ядерных объектов является известные случаи кибератак на ядерные объекты. Дальнейшее обсуждение посвящено примерам кибератак, совершенных в отношении ядерных объектов, классификации киберугроз, а также обзору опыта РФ, США и МАГАТЭ в разработке нормативных документов и рекомендаций в области кибербезопасности, в том числе документов и рекомендаций, связанных с кибербезопасностью систем управления технологически процессами ядерных объектов и систем безопасности ядерных объектов.

На сегодняшний день не существует общепринятой классификации кибератак (киберугроз) не только на объекты атомной энергетики, но и более общей. С одной стороны, это осложняет процесс моделирования киберугроз, а с другой – развязывает исследователям руки, позволяя использовать любую удобную для целей исследования модель. В частности, как нам кажется, очень удобной может быть модель, построенная на базе трех ключевых параметров любой угрозы:

– местоположение источника ее возникновения;
– природа источника;
– наличие умысла.

Если проанализировать первый фактор классификации, то самым простым было бы разделить источник на внутренний и внешний. Специалисты по физической ядерной безопасности давно и активно занимаются противодействием внутренним нарушителям. Тому, как принимать персонал на работу, как выявлять нарушителей, как формировать культуру безопасности на ядерных объектах, снижающую опасность инсайдеров, посвящено немало рекомендаций, разработанных МАГАТЭ, и требований отдельных государств. С появлением интернета и подключением отдельных обслуживающих ядерные объекты процессов к всемирной сети (например, появилась электронная почта, из интернета скачиваются обновления от производителей оборудования и программного обеспечения, системы мониторинга и диагностики зачастую работают в Сети) стала нарастать и угроза внешнего вмешательства в работу ядерных объектов.

Источники киберугроз могут иметь как техногенную, так и антропогенную природу. Иными словами, нарушение одного из трех важнейших свойств информации и информационных систем ядерных объектов (доступность, целостность и конфиденциальность) может произойти как по причине воздействия человека на отдельные элементы ядерной инфраструктуры, так и по причине воздействия программного или аппаратного обеспечения. При этом разработчик может и не принимать непосредственного участия в негативном воздействии, либо не предполагать такого воздействия, либо готовить свою акцию для другого объекта.

Наконец, третьим измерением таксономии кибератак на ядерные объекты мы бы выделили наличие умысла. Очевидно, от наличия злого умысла при совершении разрушающего или нарушающего работу ядерного объекта воздействия зависят методы,

используемые источником а так(человеком или программой). При этом отсутствие злого умысла не должно быть основанием для исключения из рассмотрения возникающих в результате кибератаки проблем. Ведь нет разницы, ядерная установка прекратила свою работу по причине направленной на нее кибератаки или по причине вредоносного кода, случайно проникшего на USB-носителе, который принес с собой сотрудник подрядной организации, обслуживающей инфраструктуру установки.

Объединяя все вместе, мы получаем следующую классификацию киберугроз для ядерных объектов, которую легко изобразить в виде куба. Измерения куба отражают три ключевых параметра описания угрозы – местоположение источника, его природу и наличие умысла.

Разумеется, возможна еще большая детализация данной классификации и введение дополнительные параметров. Например, можно учесть объект воздействия – системы управления технологическими процессами (АСУ ТП), завязанные на работу с радиоактивными материалами, системы физической ядерной безопасности, нарушение работы которых может привести к диверсиям или хищениям ядерных материалов, или сопутствующие системы, воздействие на которые может привести к утечкам информации о работе атомного объекта. Можно учесть вид ущерба (утечка радиации, кража ядерных материалов, останов реактора и т.п.). Но такая детализация усложнит задачу и не требуется для целей данной статьи.

Адекватная статистика и тем более детальная информация по инцидентам кибербезопасности на критически важных, и тем более ядерных объектах отсутствует, а данные, которые есть в открытом доступе, не могут служить основанием для проведения глубокого анализа причин возникновения инцидентов, атрибуции их авторов и определения способов и методов реализации. Однако, несмотря на нехватку данных, можно составить список основных подтвержденных инцидентов кибербезопасности, произошедших в разное время в разных странах мира. К их числу можно отнести:

– АЭС *Sellafield*, Великобритания, 1991 г.;
– Игналинская АЭС, Литва, 1992 г.;
– АЭС Бредвелл, Великобритания, 1999 г.;
– АЭС *David Besse*, США, 2003 г.;
– АЭС. Япония, 2005 г.;
– АЭС *Browns Ferry*, США. 2006 г.;
– АЭС *Hatch*, США, 2008 п;
– АЭС в Майами, США. 2008 г.;
– АЭС Areva. Франция, 2011 г.;
– АЭС *San Onofre*, США. 2012 г;
– АЭС *Susquehanna*, США. 2012 г.;
– АЭС *Monju*, Япония, 2014 г.;
– АЭС *KHNP*. Южная Корея, 2014 г..

Все указанные инциденты хорошо ложатся в предложенную классификацию. Например, самая последняя из известных атак на атомный объект южнокорейской корпорации *KHNP* (занимает 5-е место в мире по выработке атомной энергии) произошла в декабре 2014 г. В рамках данной атаки пока не установленные (или публично не названные) злоумышленники направили партнерам и бывшим сотрудникам АЭС по электронной почте письмо, содержащее вредоносный код. Открытие данного письма привело к заражению компьютера и утечке данных, касающихся ядерных объектов *KHNP*. Второй стадией атаки стал взлом веб-сайта, на котором располагалось сообщество бывших сотрудников *KHNP*. В результате использования украденной учетной записи бывшего сотрудника была добыта очередная порция материалов, касающихся частной жизни действующих сотрудников корпорации *KHNP*. Наконец, на третьей стадии злоумышленники, воспользовавшись полученными сведениями, направили действующим сотрудникам атомных объектов *KHNP* специально подготовленные письма, которые должны были вызвать доверие и тем самым

повысить шансы на успешное заражение компьютеров во внутренней сети *KHNP*. К счастью, на этом этапе инцидент был остановлен и ущерба ядерным объектам и циркулирующей на них информации нанесено не было. Данный инцидент имел внешнюю природу, исходил от человека (или группы лиц) и очевидно имел злой умысел.

Второй пример, который также хорошо ложится в предлагаемую классификацию, – это инцидент, произошедший в 2003 г. на атомной электростанции David Besse в Огайо (США). Внутренняя сеть компании, обслуживающей АЭС в Огайо, была заражена червем Slammer, который заражал сервера с программным обеспечением *MS SQL Server* 2000. В процессе проведения регламентных работ и в нарушение всех установленных на АЭС политик безопасности сотрудник обслуживающей организации установил прямое соединение между АЭС и сетью своей компании, чем не преминул воспользоваться вредоносный код, попавший внутрь сети АЭС *David Besse*. Неконтролируемое распространение червя привело к перегрузке сети и невозможности компьютеров в ней общаться друг с другом. В итоге система отображения параметров безопасности (*SPDS*) была недоступна в течение 6 часов 9 минут. Согласно предложенной классификации данный инцидент является внутренним, совершенным программой и без злого умысла.

Схожий инцидент произошел во Флориде в 2008 г. Инженер, обслуживающий обычную электростанцию в западном Майами, в обход всех правил отключил основную и резервную системы противоаварийной защиты. В результате последующего сбоя из строя было выведено оборудование подстанции, а система противоаварийной автоматики не смогла его предотвратить. В итоге пострадало свыше 680 тыс. потребителей, оставшихся без электричества. Несколько компаний, продающих электроэнергию, потеряли контроль над своими энергосетями. В том числе пострадала атомная станция *Turkey Point* на юге Майами. В отличие от предыдущего, данный инцидент произошел по вине человека, но по-прежнему оставался внутренним и без злого умысла.

Нельзя сбрасывать со счетов внутренних нарушителей, действующих со злым умыслом, как это было в 1992 г. в Литве, когда программист Игналинской АЭС загрузил вредоносный код в автоматизированную систему, отвечающую за работу одной из подсистем реактора. Данный факт был своевременно обнаружен, для проведения всестороннего расследования АЭС была остановлена. Аналогичная ситуация, когда внутренний нарушитель действовал со злым умыслом, произошла в 1999 г. на АЭС в Бредвелле (Великобритания). В инциденте участвовал сотрудник службы безопасности атомной электростанции.

Последним примером, является нашумевший *Stuxnet*, который был разработан спецслужбами США и Израиля специально для атаки на ядерные объекты Ирана. Данный вирус, занесенный извне в изолированную от внешнего мира систему управления заводом по обогащению урана в иранском городе Натанз, вывел из строя около тысячи центрифуг, что привело к существенному снижению объема производства обогащения урана, используемого в ядерной программе Ирана. Данный хорошо изученный пример отличается от вышеприведенных инцидентов тем, что это первый в истории случай, когда мы имеем дело с злоумышленным воздействием на ядерную инфраструктуру извне, которое привело к желаемому результату, продемонстрировав не только возможность, но и всю серьезность кибератак на атомные, да и на вообще на критически важные объекты. Более того, *Stuxnet* стал первым примером вредоносного кода, разработанного специально для атаки на атомный объект. В случае с внешней атакой на АЭС в Южной Корее, описанной выше, злоумышленники использовали традиционные методы заражения компьютеров, применяемые в обычных корпоративных и ведомственных сетях. В Иране же действовала специализированная вредоносная программа, аналогов которой с тех пор обнаружено не было (или нам о них пока неизвестно). Однако, нельзя говорить, что такое повторить невозможно. В 2014 г. было зафиксировано несколько заражений вредоносной программой *HAVEX*, которая, как и Stuxnet, была ориентирована на атаки именно на промышленные сети. В частности, *HAVEX* собирал данные, передаваемые с помощью промышленного протокола OPC, которые затем пересылались владельцам *HAVEX*. С какой целью проводилась эта

разведка и как будут использоваться собранные данные о работе многих промышленных сетей (а то, что она будет использована, не вызывает сомнений), до сих пор непонятно.

К счастью, известные и упомянутые выше инциденты не привели ни к хищению ядерных материалов, ни к облучению людей, ни к радиационному загрязнению окружающей среды. Значит ли это, что таких последствий не может быть в принципе? Увы, с уверенностью утверждать это мы не можем. С учетом процессов информатизации, которые наблюдаются в ядерной отрасли многих стран мира, вероятность кибератак на информационные системы не является нулевой.

Как правильно написано в стандарте по кибербезопасности североамериканской электроэнергетической корпорации NERC, цель ее киберпрограммы «гарантировать. что автоматизированные системы и коммуникационные сети, необходимые для надежной поставки электроэнергии в стране, разумно защищены от атак из различных вероятных источников угроз, а также поддерживают жизнеспособность и эффективность такой защиты». Аналогичная задача может и должна решаться для ядерных объектов. что достигается комплексным внедрением различных защитных мер, организационных и технических, управленческих и юридических, применяемых в правильное время и в правильном месте и только после всестороннего изучения объекта защиты и рисков, которые с ним связаны.

В последние несколько лет при разработке проектных угроз (*design of basic threats*) ядерным объектам многие государства и МАГАТЭ стали всерьез рассматривать кибер-природу совершения противоправных или случайных действий в отношении ядерных установок или ядерных материалов. Также положено начало формированию нормативной и методической базы и единых подходов к обеспечению кибербезопасности, как части мер по обеспечению безопасности ядерных объектов. В связи с относительной новизной проблемы говорить о том, что существует какие-то правильные или неправильные подходы, работающие или неработающие защитные меры, для ядерных объектов не приходится.

Обратившись к России, хочется отметить, что сделан хороший задел в части обеспечения информационной безопасности атомных электростанций, находящихся в ведении Росэнергоатома. Одна из проблем, присутствующих при формировании нормативных требований в области ядерной кибербезопасности – разобщенность регуляторов. Необходима координация действий разных ведомств, которые бы объединили свои усилия в части регулирования вопросов кибербезопасности критических инфраструктур в целом и ядерных объектов в частности.

Необходимы дальнейшие исследования, направленные на оценку эффективности и недостатков тех защитных мер и подходов, которые описаны в документах МАГАТЭ, РФ и США, а также на оценку практики применения самих документов и их полноты и достаточности. На основе полученных результатов могут быть разработаны инструменты оценки достаточности мер, предпринимаемых на уровне конкретного государства и его ядерных объектов для обеспечения кибербезопасности, а также рекомендации по коррекции выявленных недостатков. Наличие таких инструментов будет, помимо прочих, полезно странам, только начинающим разработку своих ядерных программ.