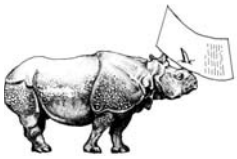


Алексей Лукацкий

КИБЕРБЕЗОПАСНОСТЬ ЯДЕРНЫХ ОБЪЕКТОВ

ВВЕДЕНИЕ

Говоря о безопасности ядерных установок, первое, что вспоминается, — это японская Фукусима и советский Чернобыль. При упоминании безопасности ядерных материалов приходят на ум истории с их кражами и голливудские боевики (например, пятый *Крепкий орешек*). Понятие *ядерная безопасность* прочно ассоциируется с ее физической составляющей. Именно ее обеспечению в настоящее время уделяется значительное внимание как на уровне государств, в которых осуществляется деятельность в области использования атомной энергии, так и на уровне международных организаций. Безопасность ядерных объектов является залогом стабильного развития программ, связанных с использованием атомной энергии в различных отраслях науки и экономики, например в генерации электроэнергии, медицине, судостроении, а также залогом энергетической безопасности регионов, где доля атомной энергетики в энергобалансе велика.

Обеспечение безопасности ядерных объектов является комплексной задачей и включает в себя множество аспектов. Для ее решения на ядерных объектах создаются различные системы защиты, каждая из которых предназначена для предотвращения угроз безопасности определенной природы. Примерами таких систем являются системы ядерной и радиационной безопасности, система учета и контроля ядерных материалов и система физической защиты ядерных материалов и установок — системы физической ядерной безопасности, а также система кибербезопасности.

Состав и структура каждой из систем обеспечения безопасности зависят от целей создания системы, а именно в предотвращении угроз конкретной природы в отношении конкретных объектов. При этом для реализации комплексного подхода к безопасности при проектировании каждой из систем необходимо учитывать влияние других угроз на достижение целей проектируемой системы.

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.

ТАКСОНОМИЯ КИБЕРУГРОЗ

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:

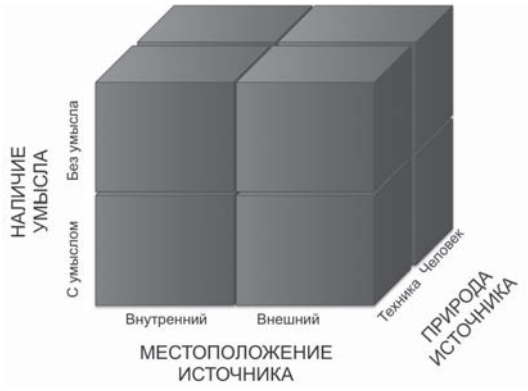
- местоположение источника ее возникновения;
- природа источника;
- наличие умысла.

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 атак (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.

ИЗВЕСТНЫЕ ИНЦИДЕНТЫ НА ЯДЕРНЫХ ОБЪЕКТАХ

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 г.;
- 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 мной 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.

Наконец, последним примером, который мне хотелось бы упомянуть, 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.

ОБЗОР ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ НА ЯДЕРНЫХ ОБЪЕКТАХ

Информационные и автоматизированные системы, которые могут подвергнуться внешним или внутренним, техническим или человеческим, случайным или злоу-

мышленным атакам, могут использоваться в совершенно различных процессах на ядерных объектах — для обогащения, транспортировки ядерных материалов и радиоактивных отходов, выработки электроэнергии, производства ядерного топлива, хранения облученных ядерных материалов и радиоактивных отходов. Такое разнообразие защищаемых процессов и систем требует комплексного подхода к их безопасности, который на протяжении последних лет активно продвигается МАГАТЭ, а также прописан в нормативных документах регуляторов в области атомной энергетики ряда стран (например, США). Речь идет о программе кибербезопасности, которая включает в себя целый комплекс технических и организационных мер, повышающих защищенность и снижающих риски нанесения ущерба ядерным объектам. В обучающем курсе МАГАТЭ по компьютерной и информационной безопасности четко зафиксирована мысль, что не существует ни волшебного решения, ни оборудования, ни программного обеспечения, которые могут сделать организацию защищенной. Безопасность сегодня не гарантирует безопасность завтра. Поэтому список защитных мер, прописанных, например, в RG 5.71 американского NRC, или в американском же NEI 08–09, или в нормативных документах российского Росэнергоатома или ФСТЭК, насчитывает около двух сотен пунктов, планомерная и дифференцированная реализация которых позволяет надеяться, что ни информации, ни автоматизированным системам ядерных объектов, а через них и самим объектам, ядерным материалам и радиоактивным отходам, ядерному топливу не будет нанесен вред.

В частности, если дистанцироваться от конкретного нормативного акта (будь то NSS 17 МАГАТЭ, *Общие положения* Росэнергоатома, 31-й приказ ФСТЭК или руководящий документ NRC RG 5.71, о которых еще будет сказано ниже), все защитные меры могут быть разделены на 5 блоков, каждый из которых решает свой спектр задач кибербезопасности:

- идентификация активов и рисков;
- защита от угроз;
- обнаружение угроз;
- реагирование на угрозы;
- восстановление после реализации угрозы.

Каждый из пяти блоков может быть детализирован. Например, первый блок может включать в себя такие защитные меры, как управление защищаемыми активами и оценка рисков. *Защитный* блок включает в себя следующий набор мероприятий:

- контроль доступа;
- обучение и повышение осведомленности;
- защита данных;
- процедуры и процессы защиты информации и информационных систем;
- поддержка защитных мер.

Оставшиеся блоки включают в себя непрерывный мониторинг безопасности, обнаружение атак и аномалий, планирование процесса реагирования на инциденты, сбор доказательств, атрибуция кибератак, коммуникации с заинтересованны-

ми сторонами, анализ инцидента и *разбор полетов*, улучшение системы защиты, восстановление после сбоев и инцидентов и ряд других защитных мер.

Ядерные объекты исторически были изолированными и отделенными от интернета, а информационные системы на них были закрытыми, построенными по проприетарным технологиям и протоколам. Поэтому до недавнего времени никаких особых требований по кибербезопасности таких объектов не предъявлялось; основные мероприятия касались ядерной безопасности. По мере проникновения процессов информатизации на изолированные объекты ситуация начала меняться, а опасность киберугроз возрастать. Поэтому начиная с середины первой декады XXI века нормативные акты, регулирующие вопросы безопасности ядерных объектов, стали включать тематику кибербезопасности. Сначала это было просто упоминание необходимости защиты информации без какой-либо детализации. Более того, даже эти общие требования мало учитывали специфику защищаемого объекта, на котором надо не защитить информацию, а обеспечить бесперебойность функционирования технологических процессов. Однако с течением времени ситуация начала меняться в лучшую сторону, и сейчас многие государства разрабатывают и внедряют собственные программы обеспечения кибербезопасности ядерноых объектов.

МАГАТЭ

Когда МАГАТЭ начинало свою деятельность в области безопасности, оно фокусировалось на вопросах физической защиты ядерных объектов, материалов и радиоактивных отходов. Среди прочего, МАГАТЭ выпускало различные руководящие документы по тем или иным вопросам ядерной безопасности, объединенные в серию изданий МАГАТЭ по физической ядерной безопасности (Nuclear Security Series, NSS). В рамках данной серии были выпущены руководства по формированию культуры безопасности, борьбе с внутренними нарушителями, формированием проектных угроз и множеству других вопросов. Однако до 2009 г. среди этих документов не было ни одного, посвященного вопросам кибербезопасности.

Эта тема понемногу просачивалась в различные документы, но целостного взгляда на нее не было. Например, в NSS № 20 по основам физической ядерной безопасности (*Nuclear Security Fundamentals*) вкратце упоминается тема информационной безопасности и устанавливаются требования по:

- обеспечению конфиденциальности чувствительной информации и защиты активов, обрабатывающих чувствительную информацию;
- обеспечению адекватной защиты при обмене чувствительной информацией;
- обеспечению кибербезопасности в рамках общей атомной безопасности.

В пятой версии рекомендаций по физической безопасности ядерных материалов и ядерных установок (*Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*) появился раздел 4.10, в котором было установлено требование по защите компьютерных систем ядерных объектов от компрометации (например, кибератак, манипуляций и фальсификаций).

Однако комплексно к данной теме МАГАТЭ стало подходить, когда была сформирована программа по информационной и компьютерной безопасности (*Information*

and Computer Security Program), цель которой — предоставить государствам и ядерным объектам необходимые ресурсы, которые могут понадобиться при разработке и внедрении собственных программ по информационной и компьютерной безопасности, повышающих общий уровень обеспечения безопасности ядерных объектов. Фокусируется данная программа на трех темах, имеющих свое преломление в области информационных и телекоммуникационных технологий:

- неавторизованное уничтожение ядерных или иных радиоактивных материалов;
- диверсия против ядерных материалов или ядерных объектов;
- кража чувствительной информации по ядерной тематике.

Ресурсы, предоставляемые МАГАТЭ в рамках данной программы, включают:

- технические руководства;
- форумы по обмену технической информацией;
- региональные обучающие мероприятия;
- поддержку в проведении региональных и международных учений;
- экспертизу при реагировании на инциденты.

В части разработки технических руководств в серии изданий МАГАТЭ по физической ядерной безопасности в 2011 г. был разработан документ под номером 17 *Компьютерная безопасность на ядерных объектах* (*Computer Security at Nuclear Facilities*). Работа над ним была непростой и длилась целых 8 лет — первые наработки по нему появились еще в 2003 г., задолго до того, как в других государствах вплотную подступились к этой тематике. Переведен этот документ был на 6 рабочих языков Агентства.

На этом работа не остановилась, и в феврале 2015 г. был опубликован еще один документ, NSS 23-G *Безопасность информации по ядерной тематике* (*Security of Nuclear Information*), посвященный реализации принципа конфиденциальности и иных аспектов информационной безопасности (целостности и доступности) в сфере безопасности ядерных объектов. Данный документ по сути перекинул мост между существующими государственными и индустриальными требованиями по кибербезопасности и их применимостью в ядерной отрасли.

Еще два документа уже подготовлены и должны быть опубликованы ближе к концу 2015 г.:

- NST 037 *Обеспечение оценки защищенности на ядерных объектах* (*Conducting Computer Security Assessments for Nuclear Facilities*);
- NST 038 *Планирование реагирования на инциденты для событий компьютерной безопасности* (*Incident Response Planning for Computer Security Events*).

Наконец, последний документ, NST 036 *Меры компьютерной безопасности для контрольно-измерительных приборов и систем управления ядерных установок* (*Computer Security Controls to for Instrumentation and Control Systems at Nuclear Facilities*) разработан и разослан на согласование всем членам МАГАТЭ. Его публикация запланирована на 2016 г.

Также в разработке в Департаменте ядерной безопасности МАГАТЭ находятся еще два документа:

- NST 045 *Компьютерная безопасность для физической ядерной безопасности* (*Computer Security for Nuclear Security*). Данный документ должен пересмотреть и уточнить положения NSS 17;
- NST 047 *Методы компьютерной безопасности для ядерных объектов* (*Computer Security Methods for Nuclear Facilities*).

В разное время заявлялось о планах разработки еще ряда документов, но в настоящий момент об их судьбе авторам ничего неизвестно:

- *Развитие нормативно-правовой базы для обеспечения компьютерной безопасности ядерных объектов (Developing a Regulatory Framework for Computer Security for Nuclear Facilities)*;
- *Проведение учений по реагированию на инциденты в области компьютерной безопасности ядерных объектов и объектов, на которых используются радиоактивные материалы (Computer Security Incident Response Exercises for Nuclear/Radiological Facilities)*;
- *Обеспечение кибербезопасности при закупках (Ensuring Cyber Security in Procurement Processes)*;
- *Оценка угроз в области кибербезопасности (Cyber Threat Assessment)*.

При этом МАГАТЭ не забывает и про другие свои рекомендации, внося в них изменения, касающиеся вопросов кибербезопасности. Например, с 2012 г. начинается активный учет вопросов кибербезопасности при определении проектных угроз (Design Basis Threat), которые раньше не учитывались в рамках публикации NSS 10 *Разработка, использование и поддержка процесса моделирования проектных угроз* (*Development, Use and Maintenance of a DBT*).

В июне 2015 г. в Вене прошла конференция МАГАТЭ, целиком посвященная вопросам кибербезопасности ядерных объектов. По сути, это было первое мероприятие такого масштаба (около трехсот докладов), на котором представители разных стран делились своим опытом в области кибербезопасности. Можно предположить, что это мероприятие послужит толчком к развитию данного направления в национальном законодательстве стран-участниц МАГАТЭ.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

Исторически вопросы защиты информации в России регулировались Федеральной службой по техническому и экспортному контролю (ФСТЭК), которая унаследовала от своей предшественницы, Гостехкомиссии России, право устанавливать соответствующие требования. Они были установлены как для сведений, составляющих государственную тайну, так и для конфиденциальной информации, обрабатываемой в различных автоматизированных и информационных системах. При этом основной акцент российским регулятором делался именно на сохранности защищаемой информации, то есть на конфиденциальности. В 1992 г., а именно тогда появились первые несекретные требования по защите информации, никто не задумывался о таких свойствах информационных систем, как доступность

и целостность, которые имеют первоочередное значение для ядерных и любых других объектов, на которых функционируют автоматизированные системы управления технологическими процессами (АСУ ТП), в том числе и в ущерб конфиденциальности.

Так продолжалось более двадцати лет. Организации, имеющие отношение к ядерной отрасли, сначала самостоятельно, а позже через соответствующий орган управления использования атомной энергии, *Росатом*, также использовали требования ФСТЭК в качестве руководства к действию. И хотя данные требования исходили из совершенно иной парадигмы, мало применимой к атомным объектам, это не мешало применять к ним принципы защиты обычных ведомственных и корпоративных сетей.

Так, приказом Федерального агентства по атомной энергии от 4 августа 2006 г. № 395 была разработана и утверждена Типовая инструкция по защите информации в автоматизированных системах предприятий и организаций Федерального агентства по атомной энергии. Спустя 5 лет был утвержден приказ ОАО *Концерн Росэнергоатом* от 9 февраля 2011 г. № 119 *О мерах по исключению неконтролируемого доступа к ПТС АСУ ТП*.

В конце 2012 г. когда ФСТЭК решила разработать новые требования по защите информации и информационных систем, лучше соответствующие текущему уровню развития информационных технологий. Такой приказ, получивший название *Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах* (Приказ № 17), был утвержден 11 февраля 2013 г. Спустя месяц был утвержден схожий приказ ФСТЭК (Приказ № 21), ориентированный на защиту информационных систем, содержащих персональные данные граждан. Эти документы мало чем отличались по своей идеологии и списку защитных мер, которые оператор информационной системы волен был выбирать самостоятельно. Во главу угла была поставлена конфиденциальности информации, но при этом впервые в официальном документе регулятора нашли свое отражение требования обеспечения целостности и доступности защищаемой системы и циркулирующей в ней информации.

Спустя год, 14 марта 2014 г. был утвержден еще один приказ ФСТЭК (Приказ № 31) *Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды*. Схожий по набору защитных мер с 17-м и 21-м приказами, новый документ был ориентирован на защиту АСУ ТП, в том числе на ядерных объектах. При этом в качестве основной задачи этот приказ постулировал необходимость обеспечения бесперебойного функционирования технологических процессов. Доступность и целостность были поставлены во главу угла.

Помимо множества несомненных достоинств у 31-го приказа есть и недостаток, причем перевешивающий все его достоинства. Юридическая сила этого приказа неочевидна. Дело в том, что он разрабатывался по прямому распоряжению Президента России и не опирается ни на один федеральный закон, который был делал этот приказ обязательным к применению всеми организациями, которые пере-

числены в его введении. Подготовленный в 2013 г. законопроект *О безопасности критической информационной инфраструктуры* так пока и не принят.

В таком правовом вакууме за дело взялся концерн *Росэнергоатом*, который в январе 2014 г. выпустил обязательный при обеспечении безопасности атомных электростанций документ под названием *Общие положения по обеспечению безопасности информации автоматизированных систем контроля и управления технологическим процессом на АЭС*. Данный документ опирался не на 31-й приказ ФСТЭК, а на 17-й, имеющий ряд недостатков, связанных с тем, что акцент делается на защите информации, а не на технологических процессах и системах управления и контроля.

В 2015 г. концерн *Росэнергоатом* планировал принять еще два обязательных документа *Системы контроля и управления, средства автоматизации АЭС. Защита информации от несанкционированного доступа и воздействий. Требования информационной безопасности при монтаже, наладке и эксплуатации АСУ ТП* и *Системы контроля и управления, средства автоматизации АЭС. Защита информации от несанкционированного доступа и воздействий. Требования информационной безопасности при проектировании, конструировании и изготовлении АСУ ТП*, которые схожи по своей идеологии с 31-м приказом ФСТЭК.

Общие положения, утвержденные *Росэнергоатомом* в 2014 г., определяют общие принципы, критерии и требования в области обеспечения кибербезопасности АСУ ТП АЭС и предполагают разработку необходимых мер и действий (организационных мероприятий и технических решений) по обеспечению информационной безопасности и координации требований по кибербезопасности АСУ ТП применительно к отдельным элементам и системам контроля и управления, а также АСУ ТП в целом. Такая разработка более детальных технических требований к обеспечению информационной безопасности АСУ ТП АЭС начата и позволит конкретизировать специально разрабатываемые технические требования к процедурам проверки комплектующих, разработки, изготовления и испытаний ПТС систем контроля и управления АЭС и технические требования к монтажу, наладке и эксплуатации (включая внесение изменений, техническое обслуживание и ремонты) ПТС систем контроля и управления АЭС.

В целом, надо признать, что текущие требования, разработанные ФСТЭК или *Росэнергоатомом,* являются, с одной стороны, обязательными к применению, а с другой, достаточно техническими, мало учитывающими управленческие и организационные вопросы обеспечения информационной безопасности, упомянутые в документах МАГАТЭ. С другой стороны, никто не мешает применять документы МАГАТЭ в России, которые только дополнят упомянутые выше требования ФСТЭК и *Росэнергоатома*.

США

В США вопросы гражданского применения ядерных материалов регулирует NRC, который так же, как и МАГАТЭ, как и *Росатом*, на первых порах основное внимание уделял традиционным вопросам физической ядерной безопасности ядерных установок, материалов и радиоактивных отходов. Например, среди документов выпущенных NRC, есть такие:

- Регулирующее руководство 5.66 *Авторизация доступа персонала на атомные электростанции* (*Personnel Access Authorization for Nuclear Power Plants*),
- Регулирующее руководство 5.77 *Программа нейтрализации воздействия внутренней угрозы* (*Insider Mitigation Program*),

которые имеют свои аналоги в свыше чем 100 странах — членах МАГАТЭ.

Однако с начала 2000-х гг. NRC начинает учитывать вопросы кибербезопасности в своей деятельности. В 2001 г. был опубликован бюллетень с рекомендацией допускать к обеспечению кибербезопасности на атомных объектах только те организации, которые имеют соответствующую лицензию. В 2002 г. эта рекомендация превращается в обязательный приказ (NRC Order EA-02-026 *Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants*). Кстати, лицензирование деятельности в области защиты информации, — это то, что объединяет США и Россию; в России третьим лицам также требуется получить специальное разрешение на предоставление услуг в области защиты информации. Правда, в России такое требование распространяется на услуги любой организации во всех отраслях экономики, в отличие от США, где это оно ограничено только критическими отраслями, включая атомную энергетику.

В 2004 г. NRC выпускает еще один документ, посвященный самооценке АЭС в области кибербезопасности (NUREG/CR-6847 *Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants*). Спустя год Институт по атомной энергетике США (NEI) выпускает руководство по построению программы информационной безопасности на атомных электростанциях (NEI 04-04 *Cyber Security Program for Power Reactors*). По сути, именно с этого документа начинается планомерное включение темы с приставкой *кибер* в документы американского регулятора NRC. Однако само руководство NEI 04-04 так и не было согласовано с регулятором, который начал самостоятельно готовить документы по информационной безопасности. NEI же позже выпустило второй документ, получивший поддержку NRC и названный *План кибербезопасности для ядерных реакторов* (NEI 08-09 *Cyber Security Plan for Nuclear Power Reactors*).

В 2007 и 2009 гг. соответственно NRC выпускает документы в смежных темах — обновленное руководство по выбору программного обеспечения для контрольно-измерительных систем (*Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems*, NRC BTP 7-14) и *Руководство по защите компьютеров, коммуникаций и сетей* (*Protection Of Digital Computer and Communication Systems And Networks*, 10 CFR 73.54).

В 2008 г. NRC начинает разработку проекта всеобъемлющего документа по кибербезопасности ядерных объектов. Проект этого документа (DG-5022) получил много отзывов и комментариев и уже в 2010 г. превратился в основополагающий и обязательный руководящий документ для всех подрядчиков ядерной отрасли США. Это RG 5.71 *Программа кибербезопасности для ядерных объектов* (*Cyber Security Programs for Nuclear Facilities*). Данное руководство базировалось на уже существующих в США и принятых Национальным институтом стандартизации (NIST) специальных публикациях SP00-53 и SP800-82, описывающих защитные меры, которые должны быть реализованы в государственных информационных системах. RG 5.71 транслировал эти требования на атомную энергетику. По сути,

Россия пошла тем же путем, когда *Росэнергоатом* и ФСТЭК взяли за основу своих документов по защите критических инфраструктур и, в частности, АЭС уже имеющиеся документы, учтя в них специфику отрасли.

Если сравнивать RG 5.71 с предыдущими документами (NIST и NEI), то соотношение будет следующим:

- NIST SP800-53 rev.4 содержит 237 защитных мер (против 198 в предыдущей версии): 91 техническую, 97 операционных и 49 управленческих;
- NEI 08-09 R6 содержит уже 139 защитных мер, из них 71 техническую, 61 операционную и 7 управленческих;
- NRC RG 5.71 содержит 147 защитных мер, из них 71 техническую, 67 операционных и 9 управленческих.

Именно RG 5.71 является сегодня обязательным документом по кибербезопасности атомных объектов в США, наряду с другими документами выпущенными NRC по другим вопросам ядерной безопасности.

ЗАКЛЮЧЕНИЕ

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 у нас сделан хороший задел в части обеспечения информационной безопасности атомных электростанций, находя-

щихся в ведении *Росэнергоатома*. Однако ядерные объекты не ограничены только епархией *Росэнергоатома* или даже *Росатома*. Есть и такие, которые находятся под эгидой минпромторга (например, какой-нибудь завод битумных материалов, который производит кокс, нефтепродукты и ядерные материалы). И особых требований по информационной безопасности для таких объектов у минпромторга нет. 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. Пока это недостижимая мечта. Видимо, русская поговорка *пока гром не грянет, мужик не перекрестится* как нельзя лучше подходит к описанию этой ситуации.

Необходимы дальнейшие исследования, направленные на оценку эффективности и недостатков тех защитных мер и подходов, которые описаны в документах МАГАТЭ, РФ и США, которые обсуждались в статье, 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.