ОБ ОПЫТЕ КОМИССИИ ПО ЯДЕРНОМУ РЕГУЛИРОВАНИЮ США В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Крупчатников Б. Н., советник директора ФБУ «НТЦ ЯРБ»
(krupchatnikov@secnrs.ru)

Дается краткий обзор подходов, на основании которых строится система регулирования кибербезопасности на ядерных объектах США. Определяющим моментом является то, что кибератака декларирована в составе проектной основы для угрозы несанкционированных действий (проектной угрозы). Это определяет логику построения системы кибербезопасности лицензиата, в соответствии с которой система кибербезопасности интегрирована в систему физической ядерной безопасности, а объектом защиты от кибератак являются системы, важные для безопасности, системы физической ядерной безопасности и системы аварийной готовности, а также вспомогательные системы и компоненты, нарушение работы которых может отрицательно сказаться на работе указанных систем безопасности.

Освещены некоторые практические вопросы организации надзора в этой области.

Отмечается, что в настоящее время Комиссия начинает полномасштабные инспекции программ кибербезопасности, что является заключительным этапом по реализации более чем пятнадцатилетней «дорожной карты» по обеспечению кибербезопасности на объектах лицензиатов в США.

Ключевые слова: *физическая ядерная безопасность, регулирование безопасности, ядерные материалы, диверсия, кибербезопасность, проектная угроза, Комиссия по ядерному регулированию США.*

U. S. NUCLEAR REGULATORY COMISSION EXPERIENCE IN CYBER SECURITY

Krupchatnikov B.N., adviser to the Director of SECNRS

A brief overview of the approaches used to build a system for regulating cyber security at U. S. nuclear facilities is given. The defining moment is that the cyber attack is declared as part of the project basis for the threat of unauthorized actions (project threat). This determines the logic of building the licensee's cyber security system, according to which the cyber security system is integrated into the nuclear security system, and the object of protection against cyber attacks are systems important for security, nuclear security systems and emergency preparedness systems, as well as auxiliary systems and components, the violation of which may adversely affect the operation of these security systems.

Some practical issues of the organization of supervision in this area are highlighted.

It is noted that the Commission is currently beginning full-scale inspections of cyber security programs. This is the final stage of a more than fifteen-year road map to ensure cyber security at licensees' facilities.

Keywords: *nuclear security, security regulation, nuclear material, sabotage, cyber security, design basis threat, U. S. Nuclear Regulatory Commission.*

В период с 2001 по 2003 гг., после террористических актов 11 сентября 2001 г. и в связи с информацией, предоставленной разведслужбами, Комиссия по ядерному регулированию США (Комиссия) издала директивы, содержащие повышенные требования к обеспечению безопасности атомных электростанций и других объектов высокого риска, эти требования включали компонент кибербезопасности. Был принят план действий Комиссии на период с 2001 по 2017 гг. в области кибербезопасности, включающий следующее:

• 2001: выпуск рекомендаций по повышению кибербезопасности для энергетических реакторов;

• 2003: определение проектной угрозы (DBT) включено в раздел 10 Свода федерального регулирования (10 CFR 73.1 [1]);

• 2004: опубликование NUREG/CR-6847 «Метод самооценки кибербезопасности для атомных энергетических установок США» [2];

• 2005: одобрение разработанной Институтом ядерной энергии программы кибербезопасности для ядерных реакторов;

• 2006: разработка критериев безопасности для использования компьютеров в системах безопасности (нормативное Руководство RG 1.152 [3]);

• 2007: опубликование руководства по обзору программного обеспечения для цифровых контрольно-измерительных приборов;

• 2009: опубликование документа 10 CFR 73.54 «Защита цифровой вычислительной техники, систем и сетей связи» [4], содержащего требование обеспечить высокую гарантию того, что функции обеспечения безопасности, физической безопасности и готовности к чрезвычайным ситуациям атомной электростанции защищены от кибератаки;

• 2010: опубликование руководства RG 5.71 «Программа кибербезопасности для ядерных объектов» [5], предназначенного для использования лицензиатом при реализации требований 10 CFR 73.54 [4], и руководства «План кибербезопасности для ядерных энергетических реакторов (NEI 08-09)» [6], разработанного Институтом ядерной энергии, которое является приемлемым для использования при реализации требований 10 CFR 73.54 [4];

• 2012: проверка реализации промежуточных этапов плана кибербезопасности;

• 2013 – 2015: инспекции этапов 1 – 7 «Дорожной карты»;

• 2016 – 2017: выявление проблем в области кибербезопасности и их разрешение на эксплуатируемых объектах.

В [7] указывается, что на начальном этапе, признавая факт существования киберугрозы, но не в полной мере оценивая конкретные уязвимости на атомных электростанциях, вопросы кибербезопасности в требованиях Комиссии носили общий характер. С учетом этого и признавая, что нормотворчество для установления требований безопасности потребует времени, Комиссия рекомендовала лицензиатам провести самооценку состояния кибербезопасности и опубликовала рекомендации «Метод самооценки кибербезопасности для атомных электростанций США» (NUREG/CR-6847) [2], которые основывались на существующих общепромышленных стандартах кибербезопасности. Комиссией были разработаны рекомендации («дорожная карта» по кибербезопасности) для поэтапной реализации требований Правил кибербезопасности [8].

«Дорожная карта» предусматривает следующие этапы:

1. Создание группы по оценке кибербезопасности;

2. Идентификация и документирование критических систем и критических цифровых активов в системах безопасности, физической безопасности и аварийной готовности;

3. Установка защитных устройств между системами с более низкими и более высокими уровнями безопасности;

4. Реализация контроля доступа для портативных переносных цифровых устройств;

5. Наблюдение за кибербезопасностью и идентификация ее событий;

6. Внедрение средств обеспечения кибербезопасности для вспомогательных систем и устройств, которые могут негативно повлиять на работоспособность критически важных средств обеспечения безопасности;

7. Осуществление и начало регулярной деятельности по мониторингу и оценке состояния кибербезопасности;

8. Полное выполнение Правил кибербезопасности (10 CFR 73.54) [4] и начало полномасштабных инспекций сотрудниками Комиссии.

По первым семи этапам «дорожной карты», рассматриваемым как переходные, были выпущены рекомендации, в том числе по составлению плана кибербезопасности, содержащие примерные сроки выполнения каждого из этапов [9]. Наличие у лицензиатов плана и следование установленным в нем срокам явилось предметом проверок сотрудниками Комиссии. Лицензиаты приняли на себя обязательства осуществить мероприятия по этим восьми этапам в срок до 2012 г.

Регулирующая политика Комиссии в отношении кибербезопасности определяет, что лицензиат должен обеспечить высокую степень гарантии того, что критически важные системы, компоненты и активы, находящиеся в ведении лицензиата, надежно защищены от кибератаки, кибератака постулируется одной из угроз в составе проектных основ для угрозы (проектной угрозы) (Design Basis Threat) [1] и определена фактором, который может привести к нежелательным радиационным последствиям в результате диверсии в отношении объекта или вида деятельности или хищения ядерного или радиоактивного материала. Формулировка проектной основы для угрозы приведена в приложении 2. Представляет самостоятельный интерес то, как сочетается общность и конкретика при описании параметров потенциального нарушителя. При этом киберугроза определена крайне лаконично – просто «кибератака» (приложение 1).

Комиссия рассматривает кибербезопасность в качестве одной из компонент, обеспечивающих физическую безопасность[1], и обязывает лицензиата иметь программу (план) обеспечения кибербезопасности, интегрированный в систему физической защиты объекта наряду с планом физической безопасности, планом подготовки и повышения квалификации персонала и планом реагирования на чрезвычайные ситуации. Нормативные требования в отношении кибербезопасности в их сегодняшнем виде закреплены в десятом разделе Свода федерального регулирования (Code of Federal Regulations – CFR), находящегося в компетенции Комиссии, при этом требования по кибербезопасности общего характера присутствуют в нескольких подразделах главы 10 кодов Федерального регулирования, относящихся к компетенции Комиссии (10 CFR) [10], однако предметные требования – Правила кибербезопасности – содержатся в составе 10 CFR 73.54 [4] и отнесены к области физической защиты. Содержание Правил кибербезопасности приведено в приложении 2.

Имея регулирующие полномочия в сфере кибербезопасности, Комиссия во взаимодействии с Национальным институтом по стандартам и технологии (National Institute of Standards and Technology – NIST), Федеральной комиссией по регулированию в электроэнергетике (Federal Energy Regulatory Commission – FERC), Североамериканской корпорацией по надежности (North American Reliability Corporation – NERC), а также в ходе консультаций с эксплуатирующими организациями установила, что подлежащими защите от кибератак в соответствии с Правилами кибербезопасности, находящимися в ведении объекта, являются системы, компоненты, оборудование и иные активы, важные для безопасности, выполняющие функции физической безопасности, связанные с функциями аварийной готовности, а также вспомогательные системы, повреждение которых может отрицательно сказаться на системах безопасности, физической безопасности и аварийной готовности. Такие системы и активы квалифицируются как критически важные. Комиссия также разъяснила, что для целей обеспечения кибербезопасности системы или оборудование, выполняющие важные для безопасности функции, включают в себя структуры, системы и компоненты в составе объекта, которые связаны с радиологическим воздействием и с физической безопасностью или могут прямо или косвенно влиять на реактивность и могут привести к незапланированной остановке реактора или незапланированному переходному процессу [11].

Разделение регулирующих, в том числе надзорных, функций между Комиссией, FERC и NERC было закреплено в меморандумах о взаимопонимании [12, 13], где была определена «линия разграничения», устанавливающая, что Комиссия осуществляет регулирование безопасности по отношению к оборудованию, подлежащему одновременно регулированию по стандартам FERC и Правилам кибербезопасности Комиссии.

На рис. 1, заимствованном из [14], показано, что цели Комиссии и NERC различны, а именно: в первом случае – недопущение неблагоприятного радиационного воздействия, во втором – обеспечение максимальной надежности единых систем энергоснабжения. Объекты, находящиеся в области пересечения

[1] В документах Комиссии понятия «физическая защита» и «физическая безопасность» фактически приравниваются.

полномочий Комиссии и NERC, в соответствии с установленной соглашениями «линией разграничения», были полностью отнесены к ведению Комиссии. В качестве примера таких систем приводятся системы управления турбиной и системой питательной воды.

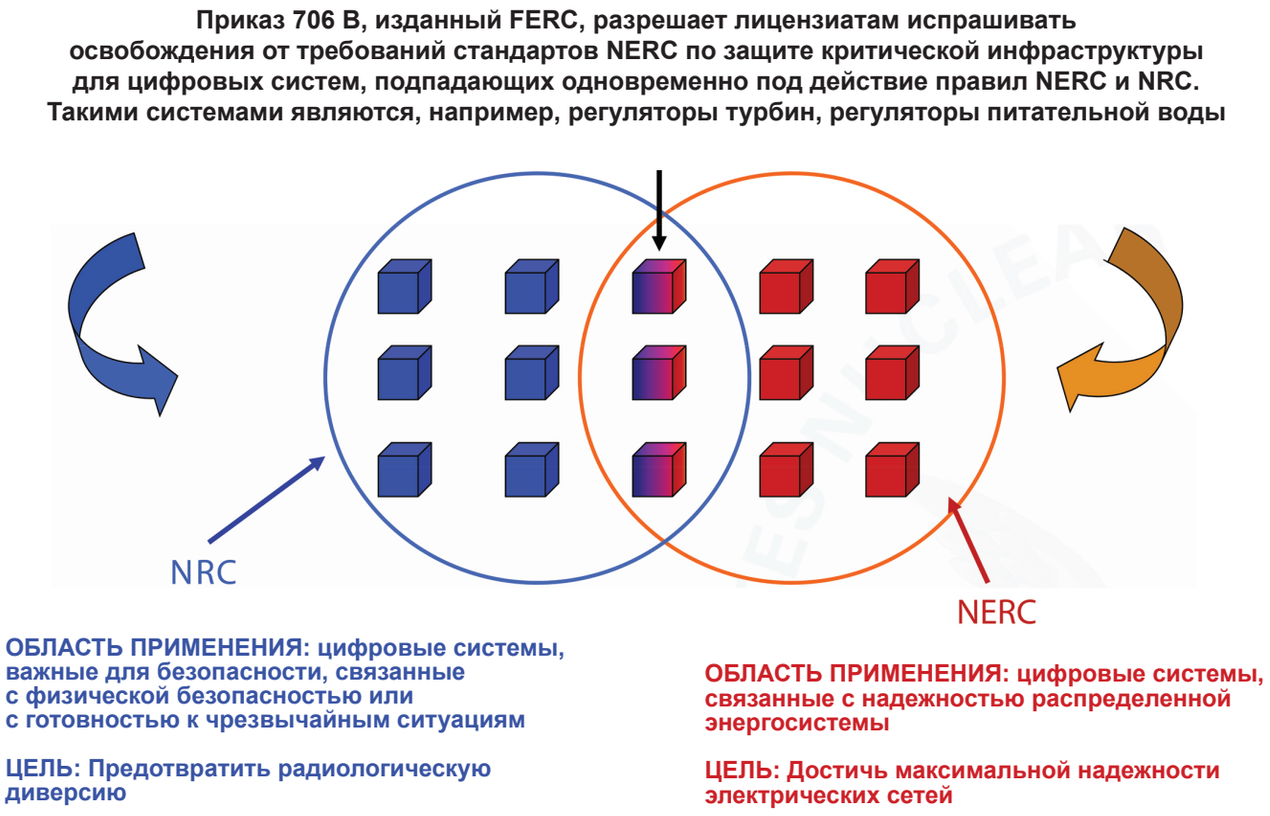

Рис. 1. Распределение регулирующих полномочий по кибербезопасности между NRC и NERC

Определение подлежащих защите от кибератак систем, оборудования, сетей и цифровых активов является исходным шагом. Комиссия одобрила и рекомендовала к использованию разработанное Институтом ядерной энергии (Nuclear Energy Institute – NEI) руководство, содержащее методику установления принадлежности систем или оборудования, или иного актива к категории критически важного «Identifying Systems and Assets Subject to the Cyber Security Rule» (NEI 10-04) [11]. В приложениях указанного документа в табличной форме на примере станции с реактором с водой под давлением приводятся результаты классификации объектовых систем.

Там же приводятся схемы проведения идентификации систем и оборудования с целью определения тех, которые подлежат защите от кибератак (рис. 2). Схема классификации цифровых активов имеет аналогичное содержание.

Еще раз отметим, что критерием отнесения объектов к категории критически важных является их связь с функциями безопасности, физической безопасности, аварийной готовности, а также принадлежность к вспомогательным системам, повреждение которых может отрицательно сказаться на системах безопасности, физической безопасности и аварийной готовности.

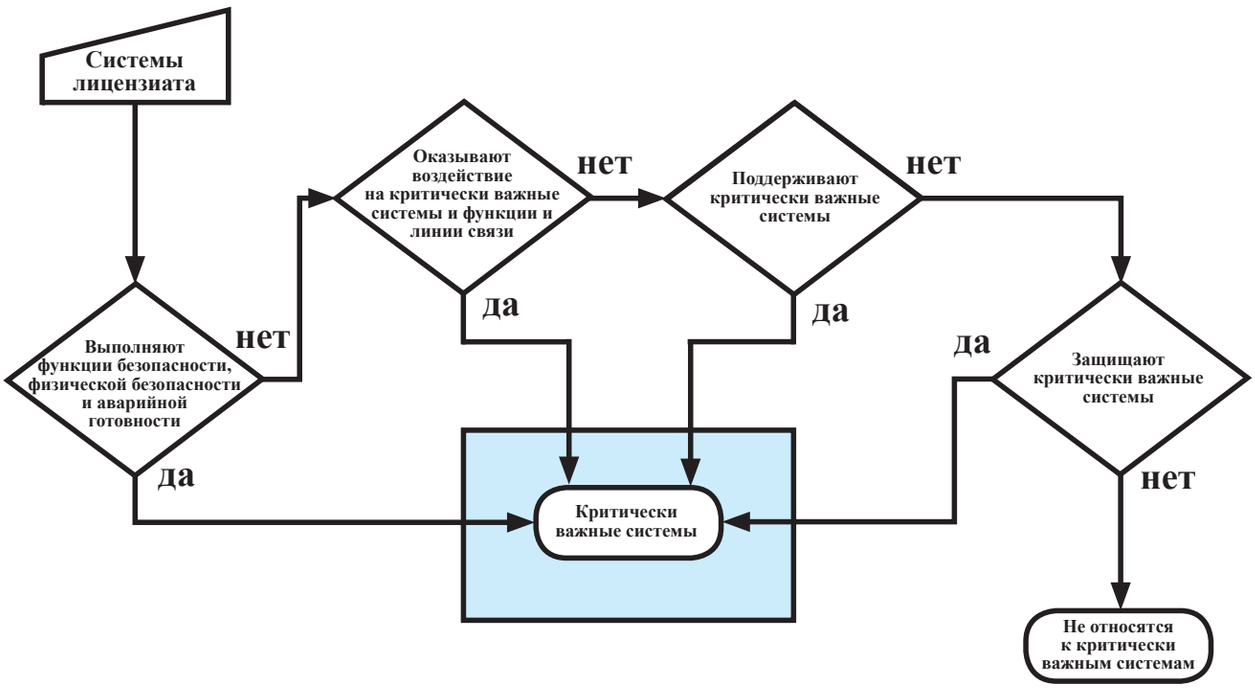

Рис. 2. Процесс выявления и оценки критически важных систем

Как уже отмечалось, Комиссия определила, что основным инструментом по обеспечению кибербезопасности на объекте лицензиата должен быть «План кибербезопасности». Этот основополагающий документ должен содержать исчерпывающее описание того, каким образом и какими средствами лицензиат выполняет «Правила кибербезопасности». План (программа) обеспечения кибербезопасности, а также вносимые в него изменения должны быть представлены на одобрение Комиссии. С целью обеспечить лицензиата приемлемым для Комиссии методом разработки плана обеспечения кибербезопасности Комиссией было выпущено подробное руководство RG 5.71 [5], содержащее следующие разделы:

Описание общих требований по кибербезопасности;

Элементы плана кибербезопасности объекта;

Разработка и внедрение программы кибербезопасности;

Поддержание программы кибербезопасности;

Актуализация и хранение записей.

В приложении к руководству даны подробные примеры (шаблоны) оперативного и общего плана кибербезопасности, плана технических средств контроля безопасности и плана управленческого контроля безопасности. Более подробный перечень основных разделов документа RG 5.71 [5] приведен в приложении 3.

Одним из элементов программы кибербезопасности является осуществление принципа глубокоэшелонированной защиты, предполагающей не только наличие нескольких барьеров безопасности, но и системы эксплуатационных, организационных и управленческих мер, обеспечивающих сохранение функций по выявлению, нейтрализации, восстановлению поврежденных систем, оборудования и активов, устранению или смягчению последствий кибератаки до того, как наступят тяжелые последствия. Одним из технических средств является ограничение коммуникации между системами с различными уровнями защиты. На рис. 3 приведен пример приемлемой архитектуры защиты кибербезопасности. Эта защитная архитектура включает пять концентрических уровней кибербезопасности, разделенных границами, такими как брандмауэры и «диоды», на которых осуществляется мониторинг и ограничение цифровой связи. Системы, требующие наибольшей степени безопасности, расположены в пределах большего числа границ. Логическая модель, показанная ниже, не всегда непосредственно соответствует физическим местоположениям, таким как особо важные, защищенные или контролируемые зоны.

Рис. 3. Упрощенная схема архитектуры кибербезопасности:
- критические цифровые активы, связанные с безопасностью, важные для функций физической безопасности, а также вспомогательные системы и оборудование, которые в случае их компрометации отрицательно повлияли бы на безопасность, физическую безопасность, отнесены к уровню 4 и защищены со всех нижних уровней;
- допускается только односторонний поток данных с уровня 4 на уровень 3 и с уровня 3 на уровень 2;
- передача сообщений от цифровых активов с более низким уровнем защиты к цифровым активам с более высоким уровнем защиты запрещена;
- данные передаются только с одного уровня на другие уровни через устройства, которые применяют политику безопасности между каждым уровнем;
- поддерживается способность обнаруживать, предотвращать, задерживать, смягчать и восстанавливать последствия кибератак

В [7] отмечается, что правила обеспечения кибербезопасности в большей степени, чем правила или требования по другим направлениям, являются «направленными на конечный результат» (performance based), т. е. не являются предписывающими, не содержат указания конкретных способов достижения результата. Использование этого подхода мотивирует лицензиата проводить постоянный мониторинг состояния кибербезопасности и принимать необходимые меры даже без вмешательства Регулятора.

В обзорных документах [15, 16], выпущенных Офисом генерального инспектора Комиссии, посвященных инспектированию вопросов кибербезопасности на ядерных установках, отмечается, что в настоящее время реализуется восьмой этап «дорожной карты» и обсуждается, насколько существующая структура и ресурсы Комиссии позволят осуществлять полномасштабное инспектирование выполнения программ кибербезопасности на объектах лицензиата. Отмечается, что в инспекции по кибербезопасности планируется участие двух инспекторов, имеющих специальную подготовку, и двух привлекаемых по контракту специалистов.

Эти оценки сделаны исходя из имеющегося опыта, накопленного с января 2013 г., когда Комиссия издала дополнения к Временной инструкции по инспектированию 2201/004 [17], в которой в разделе «Nuclear Security and Incident Response» предусматривалась проверка выполнения этапов 1 – 7 «дорожной карты», и сотрудники Комиссии приступили к проведению проверок кибербезопасности на атомных электростанциях, используя Временную инструкцию, разработанную специально для оценки промежуточных программ кибербезопасности лицензиатов в соответствии с критериями этапов 1 – 7. Инспекционные группы Комиссии проводят две отдельные недели на АЭС для каждой инспекции кибербезопасности. В течение первой недели инспекторы получают и рассматривают документацию, а также знакомятся с программой кибербезопасности станции, персоналом и планировкой. В течение второй недели на месте выполняются последующие проверочные задачи, а также представляются выводы своей работы лицензиатам. Отмечается, в частности, что нарушения по этапу 2 (идентификация критически важных цифровых активов), которые составили 19 % нарушений в 2013 г., увеличились до 31 % нарушений в 2015 г. Примером нарушения по этапу 2 является то, что некоторые лицензиаты не идентифицируют цифровые активы, обладающие уязвимостями к потенциальному вектору кибератаки. В этапе 4 (портативные и переносные устройства (ППУ)) количество нарушений увеличилось с 2013 до 2014 гг. с 25 до 35 %, но в 2015 г. вернулось к 25 %. Примером нарушения по этапу 4 является то, что лицензиаты не поддерживают согласованный уровень безопасности и контроль уровня безопасности на ППУ, связанных с критическим цифровым активом, который поддерживает ППУ. К 2015 г. количество выявленных самими лицензиатами нарушений увеличилось с 37 % в 2013 г. до 42 %. Это увеличение указывало сотрудникам Комиссии на то, что опыт работы лицензиатов в ходе предыдущих инспекций использовался для более эффективного и результативного осуществления их программ кибербезопасности.

В качестве заключения

Исходя из того, что кибератака обусловлена преднамеренными (злонамеренными) действиями человека или группы лиц, и основываясь на том, что результатом кибератаки могут быть нежелательные радиационные последствия, Регулятор относит кибербезопасность к сфере физической безопасности и включает кибератаку в состав проектных основ для угрозы, и устанавливает требование к лицензиату обеспечить высокую степень гарантии того, что критически важные системы, компоненты и активы, находящиеся в ведении лицензиата, надежно защищены от кибератаки.

Регулятор устанавливает, что защите от кибератак подлежат системы, компоненты, оборудование и иные активы, важные для безопасности, выполняющие функции физической безопасности, связанные с функциями аварийной готовности, а также вспомогательные системы, повреждение которых может отрицательно сказаться на системах безопасности, физической безопасности и аварийной готовности.

Требования к обеспечению кибербезопасности общего характера содержатся в составе требований безопасности по различным направлениям, где это уместно, а предметные и конкретные требования по кибербезопасности включены в соответствующий раздел физической защиты (физической безопасности). Требования по кибербезопасности учитывают существующие стандарты по кибербезопасности или основанные на них стандарты, изданные иными компетентными организациями, и сопровождаются рекомендациями по их реализации, содержащими методы, приемлемые для Регулятора. Регулятор осуществляет активное межведомственное взаимодействие с компетентными в сфере кибербезопасности организациями.

Основным инструментом обеспечения кибербезопасности на объекте лицензиата является интегрированная в систему физической безопасности программа кибербезопасности. Программа кибербезопасности, а также изменения к ней должны быть представлены Регулятору и получить его одобрение. Регулятор осуществляет проверку выполнения программы кибербезопасности на объекте лицензиата силами специально подготовленных инспекторов с участием привлекаемых по контракту специалистов в области кибербезопасности.

Приложение 1

Правила кибербезопасности 10 CFR 73.54

Раздел 10 CFR 73.54 «Защита цифровой вычислительной техники, систем и сетей связи» [4] содержит набор обязательных требований по кибербезопасности, основные положения которого следующие (с целью упрощения здесь опущены перекрестные ссылки на пункты 10 CFR [10]):

каждый лицензиат, имеющий в настоящее время лицензию на эксплуатацию атомной электростанции, должен представить план кибербезопасности, удовлетворяющий требованиям настоящего раздела, для рассмотрения и утверждения Комиссией. Каждое представление должно включать предлагаемый график осуществления. Реализация программы кибербезопасности лицензиата должна соответствовать утвержденному графику. Заявители на получение лицензии на эксплуатацию или совмещенной лицензии, которые подали свои заявки в Комиссию до даты вступления в силу настоящего правила, должны внести изменения в свои заявки, чтобы включить план кибербезопасности, соответствующий этому разделу;

(а) каждый лицензиат, подпадающий под требования настоящего раздела, должен обеспечить высокую степень уверенности в том, что цифровые компьютерные и коммуникационные системы и сети надлежащим образом защищены от кибератак, вплоть до проектной основы для угрозы, описанной в § 73.1:

1) лицензиат защищает цифровые компьютерные и коммуникационные системы и сети, связанные с:

i) функциями, связанными с безопасностью и имеющими важное значение для безопасности;

ii) функциями обеспечения физической безопасности;

iii) функциями обеспечения готовности к чрезвычайным ситуациям, включая связь за пределами объекта;

iv) вспомогательными системами и оборудованием, которые в случае нарушения их работы могут оказать негативное воздействие на функции обеспечения безопасности, физической безопасности или готовности к чрезвычайным ситуациям;

2) лицензиат защищает системы и сети, указанные в пункте (a) (1) настоящего раздела, от кибератак, которые могли бы:

i) отрицательно влиять на целостность или конфиденциальность данных и / или программного обеспечения;

ii) нарушать доступ к системам, услугам и / или данным;

iii) отрицательно влиять на работу систем, сетей и связанного с ними оборудования;

(b) для этого лицензиат должен:

1) анализировать цифровые компьютерные и коммуникационные системы и сети и выявлять те активы, которые должны быть защищены от кибератак в соответствии с пунктом (a) настоящего раздела;

2) создать, внедрить и поддерживать программу кибербезопасности для защиты активов, указанных в пункте (b) (1) настоящего раздела;

3) включить программу кибербезопасности в качестве компонента программы физической защиты;

(c) программа кибербезопасности должна быть разработана таким образом, чтобы:

1) осуществлять контроль безопасности для защиты активов, указанных в пункте (b) (1) настоящего раздела, от кибератак;

2) применять и поддерживать стратегии глубокоэшелонированной защиты для обеспечения возможности обнаружения, реагирования и восстановления после кибератак;

3) обеспечивать смягчение негативных последствий кибератак;

4) обеспечить, чтобы функции защищенных активов, определенных в пункте (b) (1) настоящего раздела, не подвергались негативному воздействию в результате кибератак;

(d) в рамках программы кибербезопасности лицензиат обязан:

1) обеспечить, чтобы соответствующий персонал объекта, включая подрядчиков, был осведомлен о требованиях кибербезопасности и прошел подготовку, необходимую для выполнения возложенных на него обязанностей;

2) проводить оценку и управление киберрисками;

3) обеспечить, чтобы изменения в активах, определенные в пункте (b) (1) настоящего раздела, оценивались до их внедрения для целей обеспечения кибербезопасности, определенных в пункте (a) (1) настоящего раздела;

4) проводить уведомления о событиях кибербезопасности в соответствии с положениями § 73.77;

(e) лицензиат должен разработать, внедрить и поддерживать план кибербезопасности, который реализует требования программы кибербезопасности настоящего раздела:

1) план кибербезопасности должен описывать, как будут выполняться требования этого раздела, и должен учитывать специфические для объекта условия, влияющие на реализацию плана кибербезопасности;

2) план кибербезопасности должен включать меры по реагированию на инциденты и восстановлению после кибератак. План кибербезопасности должен описывать, как лицензиат будет:

i) поддерживать потенциал для своевременного обнаружения и реагирования на кибератаки;

ii) смягчать последствия кибератак;

iii) исправлять существующие уязвимости;

iv) осуществлять восстановление затронутых кибератаками систем, сетей и / или оборудования;

(f) лицензиат разрабатывает и поддерживает письменную политику и процедуры для реализации плана кибербезопасности. Правила, процедуры внедрения, анализ конкретных объектов и другая вспомогательная техническая информация, используемая лицензиатом в рамках плана кибербезопасности, должны периодически проверяться сотрудниками Комиссии, но не должны представляться на рассмотрение и утверждение Комиссии;

(g) лицензиат рассматривает программу кибербезопасности как компонент программы физической безопасности в соответствии с требованиями § 73.55 (m), включая требования периодичности;

(h) лицензиат сохраняет все записи и подтверждающую техническую документацию, необходимые для удовлетворения требований настоящего раздела, в качестве записи до тех пор, пока Комиссия не прекратит действие лицензии, для которой были разработаны записи, и сохраняет замененные части этих записей в течение не менее трех лет после замены записи, если Комиссия не установит иное.

Приложение 2

Проектные основы для угрозы (Design Basis Threat – DBT, 10 CFR 73.1)

§ 73.1. Цель и сфера применения

В этой части предписываются требования в отношении создания и поддержания системы физической защиты, которая будет иметь возможности для защиты специального ядерного материала на стационарных объектах и при транспортировании, а также установок, на которых используется специальный ядерный материал. Нижеследующие проектные угрозы, если они упоминаются в последующих разделах настоящей части, используются для разработки систем безопасности для защиты от актов радиологической диверсии и предотвращения хищения или переключения на незаявленные цели специального ядерного материала.

(1) Радиологическая диверсия:

(i) определенное как насильственное внешнее нападение, скрытое нападение, или обманные действия, в том числе и диверсионные действия силами нарушителя, способными действовать следующими способами: одной группой атаковать через одну точку проникновения, несколькими группами нападающих через несколько точек проникновения, комбинация из одной или более групп и одного или более лиц нападающих через несколько точек проникновения или лиц, атакующих через отдельные точки проникновения, со следующими атрибутами, поддержкой и оснащением:

A) хорошо подготовленные (включая военную подготовку и навыки) и самоотверженные лица, готовые убивать или быть убитыми, обладающие достаточными знаниями для выявления конкретного оборудования или мест, необходимых для успешного нападения;

B) активные (например, способные облегчить вход и выход, отключение сигнализации и связи, участвовать в вооруженном нападении) или пассивные (например, способные предоставить информацию), или оба варианта, или хорошо осведомленные внутренние соучастники;

C) подходящее оружие, включая ручное автоматическое оружие, оснащенное глушителями и имеющее достаточную дальность прицельного огня;

D) перевозимое вручную оснащение, включая реагенты и взрывчатые вещества, для использования в качестве средств разрушения и выведения из строя оборудования с целью проникновения или для иного уничтожения целостности реактора, установки, транспортного средства или контейнера, или элементов системы гарантий;

E) наземные и водные транспортные средства, которые могут использоваться для перевозки персонала и перевозимого им оборудования в непосредственной близости от особо важных зон;

(ii) внутренняя угроза;

(iii) взрыв бомбы на наземном транспортном средстве, который может координироваться с нападением извне;

(iv) взрыв бомбы на водном транспортном средстве, который может координироваться с нападением извне;

(v) кибератаки.

(2) Хищение или переключение на незаявленные цели формульных количеств стратегического специального ядерного материала:

(i) определенное как насильственное внешнее нападение, скрытое нападение или обманные действия, в том числе и диверсионные действия силами нарушителя, способными действовать следующими способами: одной группой атаковать через одну точку проникновения, несколькими группами нападающих через несколько точек проникновения, комбинация из одной или более групп и одного или более лиц, нападающих через несколько точек проникновения или лиц, атакующих через отдельные точки проникновения, со следующими атрибутами, поддержкой и оснащением: *разделы не приводятся, поскольку повторяют соответствующие разделы части (1) «Радиологическая диверсия».*

Приложение 3

Перечень разделов рекомендаций по составлению Плана кибербезопасности ядерного объекта RG 7.41

1. Общие требования.
2. Элементы плана кибербезопасности.
3. Создание и реализация программы кибербезопасности.
3.1. Анализ цифровых компьютерных систем и сетей.
3.1.1. Оценка безопасности и права доступа.
3.1.2. Определение ролей и обязанностей и формирование группы по кибербезопасности.
3.1.3. Идентификация важнейших цифровых активов.
3.1.4. Рассмотрение и утверждение.
3.2. Стратегии глубокоэшелонированной защиты.
3.2.1. Архитектура защитных мер в системе безопасности.
3.3. Управление безопасностью.
3.3.1. Технические меры.
3.3.1.1. Контроль доступа.
3.3.1.2. Аудит и отчетность.
3.3.1.3. Системы коммуникаций.
3.3.1.4. Идентификация и аутентификация.
3.3.1.5. Усиление системы.
3.3.2. Оперативный контроль.
3.3.2.1. Защита носителей информации.
3.3.2.2. Меры безопасности (режима) в отношении персонала.
3.3.2.3. Целостность информации и систем.
3.3.2.4. Техническое обслуживание.
3.3.2.5. Защита (критически важных активов) от физического доступа и внешних воздействий.
3.3.2.6. Реагирование на инциденты.
3.3.2.7. Планирование действий в чрезвычайных ситуациях.
3.3.2.8. Повышение осведомленности и подготовка кадров.
3.3.2.9. Управление конфигурацией.
3.3.3. Административные меры.
3.3.3.1. Приобретение оборудования и получение услуг.
3.3.3.2. Оценка безопасности и управление рисками.
3.4. Включение программы кибербезопасности в программу физической защиты.
3.5. Правила и процедуры их выполнения.
4. Поддержание программы кибербезопасности.
4.1. Непрерывный мониторинг и оценка.
4.1.1. Текущие оценки мер безопасности.
4.1.2. Анализ эффективности управления безопасностью.
4.1.3. Сканирование и оценка уязвимостей.
4.2. Контроль изменений.
4.2.1. Управление конфигурацией.
4.2.2. Анализ воздействия на безопасность.
4.3. Обзор программы кибербезопасности.
5. Хранение и обработка записей.

Литература

1. Code of Federal Regulations 10 CFR § 73.1 Purpose and scope. URL: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html (дата обращения: 27.02.2020).

2. U. S. Nuclear Regulatory Commission, Cyber Security Self-Assessment Method for U. S. Nuclear Power Plants, NUREG/CR-6847, NRC (2004).

3. U. S. Nuclear Regulatory Commission Regulatory Guide 1.152 Criteria for use of Computers in Safety Systems of Nuclear Power Plants. URL: https://www.nrc.gov/docs/ML0530/ML053070150.pdf (дата обращения: 27.02.2020) (ADAMS: ML102870028)*.

4. Code of Federal Regulations 10 CFR § 73.54. Protection of Digital Computer and Communication Systems and Networks. URL: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html (дата обращения: 13.02.2020).

5. U. S. Nuclear Regulatory Commission Regulatory Guide 5.71 Cyber Security Programs For Nuclear Facilities. URL: https://www.nrc.gov/docs/ML0903/ML090340159.pdf (дата обращения: 13.02.2020).

6. Nuclear Energy Institute, Cyber Security Plan for Nuclear Power Reactors, 2010, URL: https://www.nrc.gov/docs/ML1011/ML101180437.pdf (дата обращения: 27.02.2020).

7. Regulatory Efforts to Improve Cyber Security. Wiggins J., Erlanger C., Harris T. U. S. Nuclear Regulatory Commission Office of Nuclear Security and Incident Response, Washington D. C., United States ML13156A251, 2013. URL: https://www.nrc.gov/docs/ML1315/ML13156A251.pdf (дата обращения: 13.02.2020).

8. The Nuclear Regulatory Commission Cyber Security Roadmap Policy Issue Information. June 25, 2012 SECY-12-0088. URL: https://www.nrc.gov/reading-rm/doc-collections/commission/secys/2012/2012-0088scy.pdf (дата обращения: 13.02.2020).

9. Guidance on Cyber Security Plan Implementation Schedule (ADAMS: ML110600218).

10. NRC Regulations Title 10, Code of Federal Regulations. URL: https://www.nrc.gov/reading-rm/doc-collections/cfr/ (дата обращения: 27.02.2020).

11. Identifying Systems and Assets Subject to the Cyber Security Rule. Nuclear Energy Institute. NEI 10-04. Rev. 2 (ADAMS: ML12180A081).

12. Memorandum of Understanding between the U.S. Nuclear Regulatory Commission and the North American Electric Reliability Corporation (ADAMS: MLl093510905).

13. Memorandum of Understanding between the U.S. Nuclear Regulatory Commission and the Federal Regulatory Commission Regarding the Treatment of Critical Energy / Electrical Infrastructure Information. North American Electric Reliability Corporation (ADAMS: ML1816 / ML18164A182).

14. Материалы презентации "NRC and NERC Interactions", Williamson L., 2003 (ADAMS: ML13336A577).

15. Audit of NRC'S Cyber Security Inspections at Nuclear Power Plants (OIG-19-A-13). June 4, 2019. URL: http://www.nrc.gov/reading-rm/doc-collections/insp-gen (дата обращения: 13.02.2020).

16. Audit of NRC'S Cyber Security Inspection Program for Nuclear Power Plants (OIG-14-A-15) (ADAMS: ML14127A138).

17. Closeout of NRC Temporary Instruction 2201/004, Inspection of Implementation of Interim Cyber Security Milestones 1 – 7 (ADAMS: ML18192B090).

* Здесь и далее указаны идентификационные номера документов (MLXXXXXXX) в информационной системе ADAMS (The Agencywide Documents Access and Management System), посредством которой NRC предоставляет доступ к имеющимся в ее распоряжении документам.