УДК 004.056.53

Вестник УрФО № 1(35) / 2020, с. 72–76

Мухачев С. В.

DOI: 10.14529/secur200108

ИНЦИДЕНТЫ, СВЯЗАННЫЕ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, НА ОБЪЕКТАХ ЯДЕРНОЙ ИНФРАСТРУКТУРЫ

В статье рассмотрена хронология и особенности инцидентов, связанных с информационной безопасностью, на объектах ядерной инфраструктуры. Приводится краткое описание инцидентов в различных странах, мотивы атак, предпринятые для обезвреживания меры и последствия. Выделены особенности, присущие каждой из приведенных кибератак. Показано, что проблема существования инцидентов, связанных с информационной безопасностью, на объектах ядерной инфраструктуры возникла с развитием и внедрением информационных и управляющих систем с использованием компьютерной техники. Это ясно просматривается при анализе хронологии описываемых инцидентов. Принятие федерального закона Российской Федерации «О безопасности критической информационной инфраструктуры Российской Федерации» позволяет правовыми средствами вести борьбу с кибератаками на объектах ядерной инфраструктуры.

Ключевые слова: *информационная безопасность, критическая информационная инфраструктура, ядерный объект, кибератака, вирус.*

Mukhachev S.V.

INCIDENTS RELATED TO INFORMATION SECURITY AT NUCLEAR INFRASTRUCTURE OBJECTS

The article discusses the chronology and features of incidents related to information security at nuclear infrastructure facilities. A brief description of incidents in various countries, the motives of the attacks, measures taken to neutralize the measures and consequences are given. The features inherent in each of the cyberattacks are highlighted. It is shown that the problem of the existence of incidents related to information security at nuclear infrastructure facilities arose with the development and implementation of information and control systems using

computer technology. This is clearly seen in the analysis of the chronology of the described incidents. The adoption of the federal law of the Russian Federation "On the security of critical information infrastructure of the Russian Federation" allows legal means to combat cyber attacks on nuclear infrastructure facilities.

Keywords: *information security, critical information infrastructure, nuclear facility, cyber attack, virus.*

Компьютерные атаки могут нанести вред не только физически лицам владельцам компьютеров, как это было на заре развития компьютерной и информационно-телекоммуникационной техники, но и объектам критической информационной инфраструктуры информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления субъектов критической информационной инфраструктуры. Это могут быть промышленные технологические системы, системы жизнеобеспечения городов, системы управления объектами ядерной инфраструктуры и другие объекты, относящиеся к критической информационной инфраструктуре. Сбои в работе таких систем могут нести пагубные или даже катастрофические последствия.

Современный мир сосредоточен на проблеме обеспечения безопасности инфраструктуры и информационных систем. Частные компании и государственные структуры прогнозируют потенциальные убытки, которые могут быть причинены в случае компьютерной атаки. Причем, часто речь идет об объектах инфраструктуры, от которых напрямую зависит жизнедеятельность целых городов, отдельных регионов и стран. Чтобы противостоять существующим и вновь возникающим угрозам, разрабатываются методы борьбы с ними.

В ответ на существующие угрозы, с целью защиты объектов такой инфраструктуры, в Российской Федерации принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1].

В перечень объектов критической информационной инфраструктуры включены информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфереатомной энергетики.

История вопроса и особенности, присущие объектам ядерной инфраструктуры, освещаются в ряде публикаций, посвященных данной тематике. С точки зрения рассматриваемой темы интересен доклад Королевского института международных отношений ChathamHouse «Кибербезопасность на объектах гражданской атомной инфраструктуры: понимание рисков» [2]. В докладе, опубликованном в 2015 году, подвергаются оценке возможные уязвимости и методы укрепления кибербезопасности. Эксперты провели состояния защищенности ядерных объектов, привели сведения о 50-ти киберинцидентах в различных странах мира.

Обратившись к истории вопроса, можно найти ряд примеров реализации киберугроз на объектах ядерной инфраструктуры. Остановимся на них более подробно, выстроив хронологию, и обратим внимание на особенности инцидентов. Следует обратить внимание на то, что далеко не все инциденты такого рода становятся известны общественности. Компании не заинтересованы в их разглашении по многим причинам: раскрытие особенностей системы безопасности, нежелание имиджевых потерь, разглашение технических секретов и т.д.

Один из первых известных инцидентов произошел в 1995 году на Игналинской атомной электростанции (г. Висагинас, Литва). Произошло заражение вирусом программного обеспечения для управления процессом перезагрузки ядерного топлива. Общепринятая версия связывает инцидент с местной преступной группировкой, которая таким образом пыталась отомстить за жесткий судебный приговор одному из участников группировки[3]. Вредоносная программа была внесена сообщником, который являлся сотрудником электростанции и был занят обслуживанием системы управления станции. Этот инцидент, имеющий связь с криминальным миром, можно отнести к кибертерроризму. Факт заражения был вовремя обнаружен, вирус локализован. Каких-либо последствий заражение не имело.

Другойинцидентимел место в 1998 году, когда кибератаке подвергся индийский Центр ядерных исследований им. Хоми Баба (BabhaAtomicResearchCenter) (Индия). Там террористы угрожали вывести из строя систему управления реактором. Насколько ре-

альнадля исполнения была угроза, в докладе не сообщается. Однако следует обратить внимание на то обстоятельство, что даже в случае угрозы без реальной возможности реализовать кибератаку, не исключена внеплановая остановка ядерно-опасных работ. Кроме того, необходимые проверки всех систем занимают очень продолжительное время (до нескольких месяцев). Поэтому даже имитация кибератаки (например, заражения вирусом систем объекта ядерной инфраструктуры) ведет к серьезным потерям времени, финансовым издержкам, нарушениям сроков выполнения работ.

Примечателен инцидент, зафиксированный в США в 2003 году. На атомной электростанции «Дэвис-Бессе» (Davis-Besse) в американском штате Огайо инженер получил доступ к оборудованию станции с домашнего компьютера, зараженного вирусом Slammer (сетевой червь, вызывающий отказ в обслуживании хостов в Интернете и сильное снижение общего интернет-трафика). Две системы управления оказались поражены вирусом, одна из которых отвечала за мониторинг безопасности. Она была отключена в течение пяти часов. Нужно признать, что в этом случае реальной опасности серьезных последствий, связанных с ядерными технологиями, не было, так как реактор в Дэвиса-Бессе не работал: он был закрыт почти два года после обнаружения отверстия в корпусе реактора.

Еще одна скандальная кибератака на ядерный объект произошла в 2010 году. Вирус Stuxnet, проникший в систему управления центрифугами на заводе по обогащению ядерного топлива в Иране (г. Натанз), парализовал деятельность завода [2,4]. В тот момент на заводе работало 18 каскадов по 164 центрифуги в каждом. В них было загружено около 1240 кг гексафторида урана [5]. Stuxnetдействовал таким образом, что оборудование переходило в нештатный аварийный режим. В результате кибератаки значительная часть центрифуг разрушились. Большинство исследователей считает, что оригинальный компьютерный вирус, получивший название Stuxnet был разработан спецслужбами США и Израиля для уничтожения иранской ядерной программы (официального подтверждения эта версия не имеет, что, впрочем, понятно). Он был создан специально для работы с компьютерами строго определенной конфигурации, то есть имел узкую специализацию. Попав в компьютер, Stuxnet сканировал установленное на нем программное обеспечение, чтобы определить, входит ли данный компьютер в автоматизированную систему управления центрифугами. Такие системы строго специфичны для каждого завода и имеют уникальные системы: датчиков, управления узлами и агрегатами. Stuxnet искал строго определённую цель. Если компьютер был нецелевым, то вирус не проявлял себя и ожидал возможности переместиться далее.

Таким образом, данный инцидент связан с противоборством нескольких государств, а в качестве оружия был применен «боевой» вирус Stuxnet.

В 2016 году обнаружен вирус в системе управления реактором на атомной электростанции Kernkraftwerk Gundremmingen в Германии[6,7]. В ходе плановой проверки в компьютере системы управления тепловыделяющей сборки был обнаружен вирус. Согласно пресс-релизу компании, он был выявлен при проверке съемных носителей данных и устройств программного управления. По информации энергокомпании RWE, которая эксплуатирует ядерный объект, инцидент не создал угрозу безопасности персоналу предприятия и местному населению. Однако надзорные ведомства и Федеральное управление по информационной безопасностибыли проинформированы о случившемся.

В июне 2017 года вирус-вымогатель Petya. А поразил системы радиационного мониторинга и электронный документооборотЧернобыльской атомной электростанции[8].Данная вредоносная программасетевой червь с функциями программы-вымогателя.Она поражает компьютеры под управлением операционной системы Microsoft Windows. Первые разновидности вируса были обнаружены в марте 2016 года. Программа шифруетфайлы нажёстком дискекомпьютера-жертвы, а также перезаписывает и шифрует главную загрузочную запись данные, необходимые для загрузки операционной системы. После срабатывания Petya. Афайлы, хранящиеся на компьютере, становятся недоступными. После этого программа-вымогатель требует выкуп –эквивалент трехсот долларов в биткойнах за расшифровку и восстановление доступа к файлам. Причем, как заявили исследователи «Лаборатории Касперского» после того, как файлы зашифрованы, уже нет возможности расшифровать их [9]. Усилиями персонала удалось справиться с вирусом.

Проблема существования инцидентов, связанных с информационной безопасностью, на объектах ядерной инфраструктуры возникла с развитием и внедрением информационных и управляющих систем с использованием компьютерной техники. Это ясно просматривается при анализе хронологии описываемых инцидентов.

Из описания приведенных инцидентов можно видеть, что угрозы кибер-атак на объекты ядерной инфраструктуры достаточно реальны и относительно многочисленны.

Разнообразны мотивы кибератак на объекты ядерной критической инфраструктуры: борьба государств между собой, терроризм, корыстные побуждения, халатность.

Различны и последствия кибератак. Понятно, что они могут быть очень серьезными, вплоть до катастрофических. В случае серьезного инцидента возможны ядерные аварии с выходом больших доз излучения и загрязнение местности и атмосферы радиоактивными элементами.

Обладание ядерными технологиями является сегодня серьезным политическим аргументом. Поэтому ведется борьба между государствами за право обладания ими. И как последствие такой борьбы уничтожение оборудования для производства ядерных материалов и их использования. Как раз такой случай и имел место в Иране.

В других обсуждаемых инцидентах обошлось без серьезных последствий. Конечно же, защите объектов ядерной критической инфраструктуры всегда уделялось серьезное внимание. Но, тем не менее, как следует из вышеизложенного, инциденты, связанные с кибератаками, до сих пор имеют место. Обусловлено это, прежде всего, стремительным развитием информационных технологий, изменением управляющих программно-аппаратных комплексов. Вместе с этим возникают недокументированные возможности и ошибки, что и обусловливает появлением новых возможностей для организации атак.

Объекты ядерной критической инфраструктуры требуют повышенного внимания ккиберугрозам. Поэтому меры, предпринимаемые государством в сфере защиты объектов критической информационной инфраструктуры крайне важны и актуальны и для защиты объектов ядерной инфраструктуры. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» предъявляет ряд серьезных требований ксубъектам критической информационной инфраструктуры с целью предотвращения киберугроз: определение перечня объектов; предоставление утвержденного перечня объектов во ФСТЭК России; категорирование объектов; предоставление во ФСТЭК России сведений о результатах категорирования объектов. Этот же нормативный актобусловил создание Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), которая предназначена для сбора и обмена информацией о компьютерных атаках на территории РФ. Предпринятые меря должны стать серьезным шагом к предотвращению киберугроз на объектах ядерной инфраструктуры.

Литература

1. Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. Режим доступа: URL:http://www.consultant.ru (дата обращения 05.04.2020).

2. Cyber Security at Civil Nuclear Facilities Understanding the Risks. Chatham House Report Caroline Baylon with Roger Brunt and David Livingstone September, 2015.

3. Вакцина для атома: кибербезопасность АЭС [Электронный ресурс]. Режим доступа: URL: https://russiancouncil.ru/analytics-and-comments/analytics/vaktsina-dlya-atoma-kiberbezopasnost-aes/#7(дата обращения 05.04.2020).

4. Вирус страшнее бомбы. Как хакеры уничтожили ядерный завод в Иране [Электронный ресурс]. Режим доступа: URL: https://life.ru/p/1047800(дата обращения 05.04.2020).

5. Ядерное нераспространение: краткая энциклопедия / [И. А. Ахтамзян и др.]; гл. ред. А. В. Хлопков. Москва: РОССПЭН, 2009.

6. Киберугрозы: защищены ли АЭС? [Электронный ресурс]. Режим доступа: URL: http://atomicexpert.com/page1081638.html (дата обращения 05.04.2020).

7. В компьютере на баварской АЭС обнаружен вирус[Электронный ресурс]. Режим доступа: URL:https://www.dw.com/ru/в-компьютере-на-баварской-аэс-обнаружен-вирус/a-19216272-0 (дата обращения 05.04.2020).

8. Вирус-вымогатель Petya поразил Чернобыльскую АЭС [Электронный ресурс]. Режим доступа: URL: https://ria.ru/20170627/1497397238.html (дата обращения 05.04.2020).

9. Петя стирает память[Электронный ресурс]. Режим доступа: URL: https://www.gazeta.ru/tech/2017/06/29/10752467/petya_the_destroyer.shtml (дата обращения 05.04.2020).

References

1. Federal'nyy zakon № 187-FZ ot 26.07.2017 «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» [Elektronnyy resurs]. Rezhim dostupa: URL:http://www.consultant.ru (data obrashcheniya 05.04.2020).

2. Cyber Security at Civil Nuclear Facilities Understanding the Risks. Cha-tham House Report Caroline Baylon with Roger Brunt and David Livingstone September, 2015.

3. Vaktsina dlya atoma: kiberbezopasnost' AES [Elektronnyy resurs]. Rezhim dostupa: URL: https://russiancouncil.ru/analytics-and-comments/analytics/vaktsina-dlya-atoma-kiberbezopasnost-aes/#7(data obrashcheniya 05.04.2020).

4. Virus strashneye bomby. Kak khakery unichtozhili yadernyy zavod v Irane [Elektronnyy resurs]. Rezhim dostupa: URL: https://life.ru/p/1047800(data obrashcheniya 05.04.2020).

5. Yadernoye nerasprostraneniye: kratkaya entsiklopediya / [I. A. Akhtamzyan i dr.]; gl. red. A. V. Khlopkov. Moskva: ROSSPEN, 2009.

6. Kiberugrozy: zashchishcheny li AES? [Elektronnyy resurs]. Rezhim dostupa: URL: http://atomicexpert.com/page1081638.html (data obrashcheniya 05.04.2020).

7. V komp'yutere na bavarskoy AES obnaruzhen virus[Elektronnyy re-surs]. Rezhim dostupa: URL:https://www.dw.com/ru/v-komp'yutere-na-bavarskoy-aes-obnaruzhen-virus/a-19216272-0 (data obrashcheniya 05.04.2020).

8. Virus-vymogatel' Petya porazil Chernobyl'skuyu AES [Elektronnyy resurs]. Rezhim dostupa: URL: https://ria.ru/20170627/1497397238.html (data obrashcheniya 05.04.2020).

9. Petya stirayet pamyat'[Elektronnyy resurs]. Rezhim dostupa: URL: https://www.gazeta.ru/tech/2017/06/29/10752467/petya_the_destroyer.shtml (data obrashcheniya 05.04.2020).

МУХАЧЕВ Сергей Валентинович, кандидат физико-математических наук, доцент, доцент кафедры информационных технологий и защиты информации, Уральский государственный университет путей сообщения.620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: msv62@yandex.ru

MUKHACHEV Sergey, candidate of physical and mathematical Sciences, associate Professor, associate Professor of the Department of information technology and information security, Ural State University of Railway Transport.