

## НОВЫЙ ВИД ИНФОРМАЦИОННОГО ОРУЖИЯ ИСПЫТАН НА ИРАНСКОЙ ЯДЕРНОЙ ИНФРАСТРУКТУРЕ?

Дмитрий Конухов<sup>1</sup>

В многочисленных голливудских фильмах распространена концепция кибер-апокалипсиса: локального, когда хакеры, вооруженные супервирусом, захватывают контроль над объектами городской и промышленной инфраструктуры с целью шантажа или осуществления теракта, или глобального, когда искусственный интеллект со способностью к самообучению начинает войну между человечеством и машинами. До 2010 г. такие сценарии по большей части оставались уделом фантастов и сценаристов голливудских блокбастеров и казались бесконечно далекими от реальности. С проявлением компьютерного вируса *Stuxnet* - впервые – в июне, а затем – масштабно в сентябре 2010 г. - глобальная катастрофа в виде кибер-апокалипсиса перестала казаться такой уж невозможной.

### *Stuxnet* «покоряет» мир

В июне 2010 г. компьютерный вирус атаковал управляющие системы, разработанные немецкой компании *Siemens* и используемые по всему миру<sup>2</sup>. В «зоне заражения» оказались сложные системы, в том числе автоматические, управляющие целыми заводами, а также объектами городской инфраструктуры, включая даже водопровод. Первоначально предполагалось, что вредоносная программа пытается красть данные с зараженных компьютеров с целью их последующей передачи на удаленный компьютер предполагаемого злоумышленника. Такой тип вирусов называется «троян» (по аналогии с Троянским конем) и является средством шпионажа, в данном случае – промышленного. Позже, когда специалисты все-таки смогли изучить вирус подробнее, версия промышленного шпионажа была отвергнута. Но легче не стало.

*Stuxnet* оказался компьютерным червем, то есть самостоятельной программой, способной многократно самовоспроизводить себя на зараженных машинах, вызывая различные негативные последствия: от замедления работы до вывода оборудования из строя. Таким образом, заражение этим вирусом сложных автоматизированных систем управления инфраструктурой могло преследовать только одну цель – промышленный саботаж.

Об этом говорят следующие особенности данного червя<sup>3</sup>. Он начал свою вредоносную работу еще в 2009 г.<sup>4</sup>, но до поры до времени держался в тени,

---

<sup>1</sup> Автор выражает благодарность М.В. Якушеву за помощь в юридической оценке описываемой ситуации.

<sup>2</sup> Fuhrmans Vanessa. Virus Attacks Siemens Plant-Control Systems. *Wall Street Journal (Europe)*. 2010, July 22. <http://online.wsj.com/article/SB10001424052748703954804575381372165249074.html?KEYWORDS=stuxnet+siemens> (последнее посещение - 7 октября 2010 г.).

<sup>3</sup> Clayton Mark. Stuxnet Spyware Targets Industrial Facilities, via USB Memory Stick. *Christian Science Monitor*. 2010, June 23. <http://www.csmonitor.com/USA/2010/0723/Stuxnet-spyware-targets-industrial-facilities-via-USB-memory-stick> (последнее посещение - 7 октября 2010 г.).

дорабатывая инструментарий для вписывания себя в системы *Windows* и защиты от антивирусных программ. Летом 2010 г. он распространился на тысячи компьютеров в Индии, Индонезии, Иране, Китае, Пакистане, США, Тайване и Эквадоре, но широкую огласку получило заражение компьютеров на иранских ядерных объектах, в частности АЭС в Бушере, когда там готовились к физическому пуску энергоблока<sup>5</sup>, и на заводе по обогащению урана в Натанзе.

Распространялся вирус не через Интернет, как обычно происходит с другими червями, а с помощью флеш-дисков при переносе данных с одного компьютера на другой<sup>6</sup>. Попадая на компьютер с «флешки», он перемещался по локальной сети через совместно используемые файлы и общий доступ к принтеру. При этом он повышал свои права доступа к системным ресурсам, собирал данные (версия ОС, IP-адрес зараженного компьютера) и отправлял их удаленному контролирующему серверу, а также целенаправленно искал компьютеры, на которых установлена SCADA-система *Siemens*<sup>7,8</sup>, используемая в системах мониторинга и управления промышленными, инфраструктурными и сервисными процессами на нефтепроводах, электростанциях, крупных системах связи, аэропортах, судах и даже на военных объектах по всему миру<sup>9</sup>, а точнее определенная версия этой программы (*SIMATIC WinCC/Step 7*). Такой нетривиальный на первый взгляд способ доставки может объясняться тем, что целью вируса являлись наиболее важные элементы систем управления, которые обычно в целях безопасности не подключены к внешним сетям.

По мнению специалистов «Лаборатории Касперского», авторы *Stuxnet* обладали глубокими знаниями SCADA-технологии<sup>10</sup>. Об этом говорит и необычная для простого червя сложная и комплексная архитектура программного кода, и то, что вирус использовал украденные цифровые подписи<sup>11</sup> компаний *Realtek* и *JMicron*, что позволило вредоносной программе «прикидываться» легитимным программным обеспечением и долгое время избегать обнаружения. Эти компании, в свою очередь, даже не догадывались об утечке вплоть до момента атаки.

### **Проникновение на Бушерскую АЭС**

*Stuxnet* атаковал объекты инфраструктуры по всему миру, но больше всего случаев было отмечено в Иране (почти 60% всех установленных пораженных

---

<sup>4</sup> Bradbury Danny. Stuxnet Examined at Vancouver Conference. *SC Magazine*. 2010, October 8. <http://www.scmagazineus.com/stuxnet-examined-at-vancouver-conference/article/180654/> (последнее посещение - 19 октября 2010 г.).

<sup>5</sup> Покатаева Елена. Червивый атом. *Итоги*. 2010, 11 октября. № 41 (748). <http://www.itogi.ru/hitech/2010/41/157619.html> (последнее посещение - 19 октября 2010 г.).

<sup>6</sup> Подробное техническое описание механизма распространения червя изложено: Синцов Алексей. Шпионский ярлык: история трояна Stuxnet. 2010, 18 ноября. *Хакер*. №9/10. <http://www.hacker.ru/post/53950/default.asp> (последнее посещение - 21 декабря 2010 г.).

<sup>7</sup> SCADA - Supervisory Control And Data Acquisition (Диспетчерское управление и сбор данных).

<sup>8</sup> Покатаева Елена. Червивый атом. *Итоги*. 2010, 11 октября. № 41 (748). <http://www.itogi.ru/hitech/2010/41/157619.html> (последнее посещение - 19 октября 2010 г.).

<sup>9</sup> Червь Stuxnet: начало гонки кибервооружений? Сайт «Лаборатории Касперского». 2010, 24 сентября. <http://www.kaspersky.ru/news?id=207733327> (последнее посещение - 7 октября 2010 г.).

<sup>10</sup> По сути, SCADA является программным средством автоматизированной системы управления технологическим процессом, АСУ ТП.

<sup>11</sup> То есть электронные сертификаты, позволяющие пользователю установить подлинность загружаемого контента.

вирусом персональных компьютеров<sup>12</sup>, далее с большим отрывом следуют Индонезия (17,4%) и Индия (11,3%); всего – более 50 тыс.<sup>13</sup> ПК<sup>14</sup>.

Также в Иране вирус был впервые официально зарегистрирован. Сделали это 17 июня 2010 г. на одном из предприятий страны специалисты из Белоруссии<sup>15</sup>. В конце лета стало известно, что вирус проник в компьютеры АЭС в Бушере.

Согласно имеющимся данным, вирусом были инфицированы персональные компьютеры станции, однако основная операционная система станции не пострадала<sup>16</sup>. По сообщению пресс-службы ЗАО «Атомстройэкспорт», генерального подрядчика на строительство Бушерской АЭС, распространение компьютерного вируса *Stuxnet* не отразилось на работе систем управления реактора: вирус не получил доступ к АСУ ТП (автоматизированной системе управления технологическим процессом) станции<sup>17</sup>. В конце сентября глава Организации по атомной энергии страны Али Акбар Салехи заявил, что специалистам удалось удалить вирус с «инфицированных» на АЭС машин<sup>18</sup>.

Несмотря на то, что вирусная атака была выявлена на этапе подготовительных к физическому пуску работ (в реактор еще не началась загрузка ядерного топлива), до сих пор нет ясности, что могло бы произойти, если бы вирус попал непосредственно в систему управления реактора. В числе возможных последствий эксперты называют сбой в системе охлаждения активной зоны реактора или другой критически важной подсистемы АЭС, каждый из которых мог привести как минимум к вынужденной временной остановке работы всего объекта.

Другой целью кибератаки на АЭС в Иране могло быть затягивание процесса ввода объекта в эксплуатацию<sup>19</sup>. Очевидно, что проверка всех систем после обнаружения вредоносного программного обеспечения на ядерно-опасном объекте занимает не часы и не дни. Уже 9 октября на лентах информагентств

---

<sup>12</sup> Firth Niall. Computer Super-Virus Targeted Iranian Nuclear Power Station but Who Made It? *Daily Mail*. 2010, September 24. <http://www.dailymail.co.uk/sciencetech/article-1314580/Stuxnet-worm-targeted-Iranian-nuclear-power-station-sophisticated-virus-attack-ever.html> (последнее посещение - 7 октября 2010 г.).

<sup>13</sup> Schneier Bruce. The Story Behind The Stuxnet Virus. *Forbes*. 2010, October 7. <http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html> (последнее посещение - 1 декабря 2010 г.).

<sup>14</sup> Laurent Maillard. Iran Denies Nuclear Plant Computers Hit by Worm. *AFP*. 2010, September 26. <http://www.google.com/hostednews/afp/article/ALeqM5izMHSVD4tEUYpQJa7iGAp5vJyTUw> (последнее посещение - 7 октября 2010 г.).

<sup>15</sup> Zetter Kim, Ackerman Spencer. Could Stuxnet Mess With North Korea's New Uranium Plant? 2010 November 22. <http://www.wired.com/dangerroom/2010/11/could-stuxnet-mess-with-north-koreas-new-uranium-plant/> (последнее посещение – 29 ноября 2010 г.).

<sup>16</sup> Сетевой вирус Stuxnet атаковал атомную станцию в Бушере. *Вести* 24. 2010, 26 сентября. <http://www.vesti.ru/doc.html?id=395196> (последнее посещение - 7 октября 2010 г.).

<sup>17</sup> Загрузка ядерного топлива в реактор АЭС "Бушер" планируется в октябре. *РИА Новости*. 2010, 5 октября. <http://eco.rian.ru/business/20101005/282482337.html> (последнее посещение - 7 октября 2010 г.).

<sup>18</sup> Сотрудники АЭС в Бушере очистили систему от компьютерного вируса. *РИА Новости*. 2010, 29 сентября. <http://www.rian.ru/science/20100929/280467410.html> (последнее посещение - 7 октября 2010 г.).

<sup>19</sup> Покатаева Елена. Червивый атом. *Итоги*. 2010, 11 октября. <http://www.itogi.ru/hitech/2010/41/157619.html> (последнее посещение - 19 октября 2010 г.).

появилась информация о том, что Иран откладывает<sup>20</sup> ввод в эксплуатацию АЭС «Бушер» до начала 2011 г., однако нет данных, которые бы подтверждали, что причиной очередного переноса сроков стала вирус *Stuxnet*.

Нельзя пока исключать и возможность того, что вирусная атака была всего лишь имитационным ударом, прикрывающим реальное вредоносное воздействие другого рода, т.е. одним из элементов спецоперации в отношении ядерной инфраструктуры Ирана. 9 октября официальный Тегеран сообщил о раскрытии фактов шпионажа на атомных объектах республики. Согласно заявлению вице-президента Ирана и главы Организации по атомной энергии страны Али Акбара Салехи (ныне – министра иностранных дел), несколько сотрудников атомных объектов были уличены в сборе и передаче иностранным спецслужбам секретной информации, касающейся закупок оборудования за рубежом и коммерческих деталей этих сделок<sup>21</sup>. Несмотря на то, что время, когда происходили описанные события, неизвестно, предположение, что это могло быть каким-либо образом связано с вирусной атакой, напрашивается само собой. Ранее, 3 октября официальными властями Ирана было объявлено о задержании ряда лиц, участвовавших в попытке кибернетического саботажа национальной ядерной энергетической программы<sup>22</sup>.

Существуют и другие предположения относительно способов проникновения вируса на компьютеры, расположенные на ядерных объектах Ирана. Например, немецкий эксперт по вопросам информационной безопасности Ральф Лангнер считает, что вирус на Бушерскую АЭС мог быть по неосторожности занесен российскими специалистами, якобы работавшими с флеш-дисками без соблюдения должных мер безопасности<sup>23</sup>. Так же официальные власти Ирана объявили о задержании нескольких иранских специалистов, подозреваемых в попытке саботажа работы АЭС, хотя под этой формулировкой может скрываться та же неосторожность в обращении с «флешками».

По мнению автора данной статьи, этот вопрос сам по себе неоднозначен. С одной стороны, выбранный метод распространения червя (не через Интернет, а с помощью переносных запоминающих устройств) не дает гарантии попадания вируса в нужное место без помощи «своего» человека на объекте. С другой стороны, необходимость умышленного «ручного» внесения вируса в систему противоречит имеющимся фактам: зачем было распространять вирус на большое количество персональных компьютеров и вспомогательных систем, если можно точно заразить центральные системы управления, сбой в функционировании которых даст наибольший разрушительный эффект? Скорее всего, преднамеренное распространение вируса на большее количество систем,

---

<sup>20</sup> Иранские власти заявили о факте шпионажа на своих атомных объектах. 2010, 9 октября. <http://www.rbc.ru/rbcfreeenews.shtml?/20101009224846.shtml> (последнее посещение - 15 октября 2010 г.).

<sup>21</sup> Iran Confirms Espionage by Nuclear Personnel. *Global Security Newswire*. 2010, October 12. [http://www.globalsecuritynewswire.org/gsn/nw\\_20101012\\_4107.php](http://www.globalsecuritynewswire.org/gsn/nw_20101012_4107.php) (последнее посещение - 15 октября 2010 г.).

<sup>22</sup> В Иране задержаны «кибер-террористы». *Вести* 24. 2010, 3 октября. <http://www.vesti.ru/doc.html?id=396695> (последнее посещение - 7 октября 2010 г.).

<sup>23</sup> Bushehr Plant Computer Worm has Language Implicating Israel. *Global Security Newswire*. 2010, September 30. [http://gsn.nti.org/gsn/nw\\_20100930\\_3062.php](http://gsn.nti.org/gsn/nw_20100930_3062.php) (последнее посещение - 7 октября 2010 г.).

чем предполагалось целей для прямого воздействия, было выбрано не случайно и использовалось как маскировка под уже ставшие тривиальными глобальные вирусные атаки.

### ***Stuxnet* против обогащения урана**

По другой версии, приоритетной целью вируса была не АЭС, а иранские предприятия по обогащению урана. Эксперты Института науки и международной безопасности (*ISIS*)<sup>24</sup> предполагают, что вследствие вредоносного воздействия вируса на заводе по обогащению урана в Натанзе вышли из строя и были заменены около тысячи центрифуг *IR-1*. Иранские власти сначала долго оставляли без комментариев<sup>25</sup> вопрос о возможном попадании червя в оборудование завода в Натанзе, который и без того испытывает трудности в работе в связи с нехваткой комплектующих, квалифицированного персонала, а также опыта у иранских специалистов в области управления каскадами центрифуг<sup>26</sup>. Однако выход из строя и замена около 15%<sup>27</sup> оборудования в такой короткий период вряд ли может быть объяснена только лишь недостатками самого оборудования и отсутствием опыта.

Версия о том, как вирус может влиять непосредственно на оборудование завода по обогащению, высказанная аналитиком компании *Symantec*, предполагает, что главная цель *Stuxnet* - частотные преобразователи иранской компании *Fararo Raya* и финской *Vacon*. Конкретно вирус «интересуется» только преобразователями, работающими с частотами от 807 до 1210 Гц. Вирус меняет выходные частоты преобразователей, а значит и скорости соответствующих им моторов, с небольшим шагом в течение месяцев. Это сильно влияет на работоспособность «зараженных» устройств, вместе с тем порождая проблемы, которые гораздо сложнее обнаружить<sup>28</sup>.

Конкретнее действия вируса в отношении этих устройств можно описать так. Сначала вирус подает команду, увеличивающую частоту вращения ротора

---

<sup>24</sup> Albright David, Brannan Paul, Walrond Christina. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment. *ISIS Reports*. 2010, December 22. <http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/#5> (последнее посещение – 6 января 2011 г.).

<sup>25</sup> Впоследствии 29 ноября официальный Иран признал, что часть центрифуг испытывала проблемы в работе, но они уже выявлены и устранены. При этом причины возникновения таких проблем не упоминались. Iran Admits Cyber Attack on Nuclear Plants. *Reuters*. 2010, November 29. <http://www.reuters.com/article/idUSTRE6AS4MU20101129> (последнее посещение – 18 января 2011 г.).

<sup>26</sup> Bushehr Plant Computer Worm has Language Implicating Israel. *Global Security Newswire*. 2010, September 30. [http://gsn.nti.org/gsn/nw\\_20100930\\_3062.php](http://gsn.nti.org/gsn/nw_20100930_3062.php) (последнее посещение - 7 октября 2010 г.).

<sup>27</sup> 5 ноября 2010 г. в 54 смонтированных каскадах насчитывалось 8426 центрифуг. См.: Осуществление Соглашения о гарантиях в связи с ДНЯО и соответствующих положений и резолюций Совета Безопасности в Исламской Республике Иран. Доклад генерального директора МАГАТЭ Совету управляющих. 2010, 23 ноября. GOV/2010/62. [http://www.iaea.org/Publications/Documents/Board/2010/Russian/gov2010-62\\_rus.pdf](http://www.iaea.org/Publications/Documents/Board/2010/Russian/gov2010-62_rus.pdf) (последнее посещение - 17 января 2011 г.).

<sup>28</sup> Chien Eric. Stuxnet: A Breakthrough. *Symantec Blogs*. 2010, November 12. <http://www.symantec.com/connect/blogs/stuxnet-breakthrough> (последнее посещение - 21 декабря 2010 г.).

центрифуги до 1410 Гц<sup>29</sup> (при том, что рабочая частота ротора – 1065 Гц, а максимально механические части ротора едва выдерживают частоту в 1400 Гц) на 15 минут, после чего возвращает этот параметр в исходное положение. Через 27 дней другая команда понижает частоту до 2 Гц в течение 50 минут, после чего так же возвращает этот параметр к номинальным 1064 Гц. С интервалом в 27 дней эти действия вновь повторяются<sup>30</sup>.

При наличии возможности механически повредить центрифуги сразу (ротор не выдерживает частоты 1410 Гц больше 15 минут), время таких изменений ограничено. Повышение частоты заканчивается до достижения максимальной скорости вращения, то же и с понижением частоты. Видимо, создатели предпочли незаметное постепенное подтачивание оборудования его единоразовому выводу из строя, ведь последнее несомненно бы насторожило бы специалистов завода и повлекло бы более активные действия по поиску неисправностей. Отсюда можно заключить, что если задачей *Stuxnet* в Натанзе был единовременный вывод из строя большинства центрифуг, то с ней он не справился. Если же воздействие вируса было направлено на вывод из строя небольшого количества оборудования, не привлекая при этом к себе внимания и затрудняя обнаружение причины, с целью замедлить или отбросить назад ядерную программу Ирана в целом, то вирус с задачей справился, по крайней мере, на время.

Все же трудно определенно сказать, разрабатывался ли вирус непосредственно с целью вывода из строя оборудования завода по обогащению урана в Натанзе (указанные выше преобразователи имеют и другие сферы применения), и тогда остальные объекты инфраструктуры в других странах оказались под ударом из-за схожести систем управления на базе технологий *Siemens*; или же «целевой аудиторией» *Stuxnet* была именно платформа немецкой компании, как наиболее географически распространенная система управления объектами инфраструктуры, и в этом случае ситуацию на иранских ядерных объектах можно назвать побочным эффектом проведенной акции. В *Siemens* заявляют, что компания не поставляла программное обеспечение в Иран, хотя и не отрицают его присутствие в Бушере<sup>31</sup>. Факт наличия в Иране нелегальных систем *SCADA* доказывает фотография одного из мировых информационных агентств, запечатлевшей сообщение о просроченной лицензии на одном из мониторов АЭС в Бушере<sup>32</sup>.

### **Происхождение вируса**

На данный момент нет достаточной информации, позволяющей установить личности авторов вредоносной программы. Однако цель атаки и география

---

<sup>29</sup> Albright David, Brannan Paul, Walrond Christina. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment. *ISIS Reports*. 2010, December 22. <http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/#5> (последнее посещение – 6 января 2011 г.).

<sup>30</sup> Ibid.

<sup>31</sup> Chien Eric. Stuxnet: A Breakthrough. Symantec Blogs. 2010, November 12. <http://www.symantec.com/connect/blogs/stuxnet-breakthrough> (последнее посещение - 21 декабря 2010 г.).

<sup>32</sup> Kheirkhah Mohammad. Iran's Bushehr Nuclear Ppower Plant in Bushehr Port. UPI Photo. 2009, February 25. [http://www.upi.com/News\\_Photos/Features/The-Nuclear-Issue-in-Iran/1581/2/](http://www.upi.com/News_Photos/Features/The-Nuclear-Issue-in-Iran/1581/2/) (последнее посещение – 21 декабря 2010 г.).

распространения червя (преимущественно Иран и объекты его ядерной инфраструктуры) говорит о том, что это дело рук не обычных киберпреступников. Первый вирус, способный выйти за пределы цифрового измерения и выводить из строя реальные объекты, мог быть создан командой высококвалифицированных профессионалов при финансовой поддержке и с одобрения суверенного государства<sup>33</sup>. По оценке экспертов, разработка такого вируса требует около 6 месяцев работы группы из 5-10 высококвалифицированных специалистов<sup>34</sup>. Кроме этого необходима поддержка со стороны специальных служб для установления личностей сотрудников предприятий ядерной промышленности Ирана и последующего контакта с ними с целью получения доступа к системам управления объектами.

Некоторые видят в произошедшем «руку» Израиля, особенно после появлений в прессе сообщений о том, что один из компонентов кода *Stuxnet* может содержать косвенную отсылку на Книгу Есфири, одной из книг Ветхого завета, написанной на древнееврейском языке<sup>35</sup>. Упомянувшийся выше немецкий эксперт Лангер в ходе анализа кода вируса разглядел, что один из файлов программного кода носит название *Myrtus* (мирт), что, с одной стороны, является обозначением семейства растений, а с другой – «может быть прочитано как намек на Есфирь», поскольку на иврите это слово «похоже» на имя Есфири в оригинале - *Hadassah*<sup>36</sup>. В самой же Книге Есфири описывается «превентивный удар» иудеев против заговора персов, из чего Лангер и делает вывод, что подобное упоминание в коде вируса придумано либо создателем вредоносной программы, либо является способом отвести подозрения и направить их на Израиль. Журналисты *New York Times* предполагают, что создание и обкатка вируса могли происходить в секретном израильском ядерном комплексе Димона в пустыне Негев. На территории этого комплекса могли быть созданы практически идентичные копии иранских центрифуг, под параметры которых и был написан вирус<sup>37</sup>.

Однако убедительных доказательств участия Израиля до сих пор не представлено. Шай Блитзблау, глава израильской лаборатории электронной войны, отверг версию об израильском происхождении вируса и предположил,

---

<sup>33</sup> Червь Stuxnet: начало гонки кибервооружений? Сайт «Лаборатории Касперского». 2010, 24 сентября. <http://www.kaspersky.ru/news?id=207733327> (последнее посещение - 7 октября 2010 г.).

<sup>34</sup> Bradbury Danny. Stuxnet Examined at Vancouver Conference. *SC Magazine*. 2010, October 8. <http://www.scmagazineus.com/stuxnet-examined-at-vancouver-conference/article/180654/> (последнее посещение - 19 октября 2010 г.).

<sup>35</sup> Bushehr Plant Computer Worm Has Language Implicating Israel. *Global Security Newswire*. 2010, September 30. [http://gsn.nti.org/gsn/nw\\_20100930\\_3062.php](http://gsn.nti.org/gsn/nw_20100930_3062.php) (последнее посещение - 7 октября 2010 г.).

<sup>36</sup> Немецкий эксперт узрел в компьютерном вирусе след библейских пророчеств, грозящих карой Ирану. 2010, 30 сентября. <http://hitech.newsru.com/article/30sep2010/biblestuxnet> (последнее посещение - 7 октября 2010 г.).

<sup>37</sup> Broad William, Markoff John, Sanger David. Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *New York Times*. 2011, January 15. [http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?\\_r=3&pagewanted=1&hp](http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3&pagewanted=1&hp) (последнее посещение – 17 января 2011 г.).

что он был создан для шпионажа против *Siemens* или в качестве академического эксперимента<sup>38</sup>.

### **Противодействие кибертерроризму**

Угрозы или попытки проведения диверсий на АЭС имели место и ранее. В большинстве случаев<sup>39</sup> опасность исходила извне, и с ней успешно справлялись. Но разработанные меры защиты объектов атомной энергетики не в состоянии полностью предупредить нетрадиционные виды угроз, особенно, когда опасность исходит не снаружи, а изнутри.

Подобный инцидент произошел в 1995 г. на Игналинской АЭС (Литва), когда террористы в отместку за осужденного в 1994 г. к смертной казни члена их группы через «агента» среди персонала, обслуживающего систему управления станции, сумели внести изменения в программу управления процессом перегрузки ядерного топлива<sup>40</sup>. Угроза была своевременно выявлена и устранена усилиями персонала станции, но по сути это был чистый акт кибертерроризма, так как он был реализован через информационную систему и информационными же средствами<sup>41</sup>. В 1998 г. подобной атаке подвергся индийский Центр ядерных исследований им. Хоми Баба (*Bhabha Atomic Research Center*), где террористы угрожали вывести из строя систему управления реактором<sup>42</sup>. Отличием истории со *Stuxnet* является то, что атака на объекты критической инфраструктуры с помощью этого вируса может быть актом терроризма государственного.

Важно правильно оценить угрозу, которую несет *Stuxnet* и подобное вредоносное программное обеспечение в целом. Если она реальна, и речь идет о проблеме международной стабильности, тогда речь должна идти о выработке международной конвенции, которая смогла бы регулировать проблемы кибертерроризма на глобальном уровне.

Подобные механизмы в сфере регулирования киберпространства уже существуют, но пока лишь на региональном уровне. В качестве примера можно привести Европейскую конвенцию по киберпреступлениям 2001 г., которая неприменима к данной ситуации напрямую, поскольку подписана и

---

<sup>38</sup> В коде вируса *Stuxnet* обнаружили фрагмент из книги Есфирь. *InterRight*. 2010, 1 октября. [http://www.inright.ru/news/headlines/20101001/id\\_4412/](http://www.inright.ru/news/headlines/20101001/id_4412/) (последнее посещение - 7 октября 2010 г.).

<sup>39</sup> Так, предполагается, что намеченной целью одного из угнанных в США в сентябре 2001 г. самолетов была АЭС под Питтсбургом. В 1973 г. террористической группой был захвачен аргентинский реактор в Атуче, который находился в то время в стадии строительства. В 1982 г. во Франции экотеррористами был совершен обстрел из гранатометов строящейся АЭС «Суперфеникс» в г. Крейс. В декабре 1995 г. во Франции в ходе волны протестов против эксплуатации АЭС «Блэйс» экстремистки настроенные участники совершили попытку вывести из строя второй контур третьего энергоблока этой станции. В 1980 г. пуэрториканские сепаратисты угрожали, что взорвут американские АЭС. – См. Супертерроризм: новые вызовы нового века. Под ред. А.В. Федорова. *Научные записки ПИР-Центра: национальная и глобальная безопасность*. №2 (20). М.: «Права человека», 2002.

<sup>40</sup> Там же. С. 64.

<sup>41</sup> Там же. С. 94.

<sup>42</sup> Там же. С. 103.

рекомендована к исполнению в странах-участницах Совета Европы<sup>43</sup>. Помимо этого упомянутая конвенция работает неэффективно (некоторые страны, в т.ч. и Россия<sup>44</sup>, не ратифицировали или вышли из конвенции по политическим соображениям, считая недопустимым право участвующих государств на расследование киберпреступлений в других странах без согласия властей последних) и не включает понятие «государственный кибертерроризм». Создание более глобального и универсального международного документа восполнило бы нишу юридического противодействия ситуациям, подобным истории со *Stuxnet*. Впрочем, по состоянию на начало февраля 2011 г. практических шагов по выработке подобного документа ни одним из государств предложено не было. Возможно, угроза *Stuxnet* могла быть переоценена и умышленно преувеличена в СМИ?

Однозначно ответить на этот вопрос сейчас не представляется возможным. Существует мнение, что появление *Stuxnet* ознаменовало третью эпоху гонки кибервооружений, и на смену любителям, пишущим вирусы ради развлечений, а потом и киберпреступникам, вымогающим или крадущим деньги, пришли люди, воспринимающие информационные системы как поле боя. И с учетом все большего внедрения информационных систем в человеческую жизнедеятельность, всеобщей автоматизации и компьютеризации систем управления различных объектов инфраструктуры (в т.ч. и критических) подобные кибератаки могут стать более распространенным и достаточно опасным явлением.

### **Заключение**

История со *Stuxnet* – событие из ряда вон выходящее, хоть и появляющиеся все новые подробности появления вируса в информационной системе Бушерской АЭС и завода по обогащению урана в Натанзе не способствуют однозначному пониманию ситуации. Уже собранный объем информации ставит ряд частных и системных задач.

1. Необходимо тщательное изучение архитектуры вируса, дающее более полное определение свойств, целей и задач *Stuxnet*. Следует убедиться, что вредоносное ПО не имеет более сложную структуру и не сможет еще раз проявить себя, в частности на более позднем этапе работ по физическому пуску АЭС и ее эксплуатации, или своевременно выявить обратное. Согласно имеющимся данным, вирус предусматривает самоуничтожение только 24 июня 2012 г.<sup>45</sup>.

---

<sup>43</sup> По состоянию на 2010 г. Европейскую Конвенцию по киберпреступлениям подписали 43 государства, 39 из которых члены Совета Европы. Конвенцию подписали также Канада, Япония, Южная Африка и США, хотя они и не являются членами Совета Европы.

<sup>44</sup> Россия отказывается ратифицировать Будапештскую конвенцию, параллельно продвигая идею разработки глобальной конвенции. По инициативе России Комиссия ООН по противодействию преступности и уголовному правосудию в мае 2010 г/ учредила межправительственную группу экспертов, создание которой предусматривает появление в ближайшее время предложений по совершенствованию международной нормативно-правовой базы в этой области.

<sup>45</sup> Schneier Bruce. The Story Behind The Stuxnet Virus. *Forbes*. 2010, October 7. <http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html> (последнее посещение - 1 декабря 2010 г.)

2. Следует дополнительно изучить вопрос формата, объема использования и регулирования использования иностранного ПО на объектах критической инфраструктуры России. В частности, необходима оценка уязвимости российских АЭС и других чувствительных объектов, которые также могут использовать системы *Siemens*. Это особенно важно с учетом того, что до недавнего времени иранские специалисты проходили подготовку на Нововоронежской АЭС в России, в связи с чем вредоносное ПО могло быть внесено, к примеру, на компьютеры Нововоронежского учебного центра.

3. Если *Stuxnet* действительно является предвестником появления нового вида оружия, необходимо изучить и то, как события описанные в данной статье повлияют в будущем на возможность использования кибератак на объекты критической инфраструктуры, подготовленных с участием государств. Заставит ли взаимная уязвимость государств проявлять сдержанность в этой области (как, например, применение ядерного оружия в Хиросиме и Нагасаки дало осознание возможных последствий ядерной войны), или, наоборот, откроет «ящик Пандоры», и тогда срочно потребуются соответствующие международные инструменты, регулирующие эту сферу.

4. Необходимо инициировать выработку универсального международного документа, который бы позволил создать правовые основы для противодействия ситуациям, подобным описанной в данной статье, осуществлять международное взаимодействие в этой области, в том числе в рамках расследования актов кибертерроризма. Естественно, с учетом сложности такой задачи, необходимо разрабатывать меры противодействия подобным ситуациям и на национальном уровне.