УДК 004.056.57

© Ромашкина Н.П., Махукова А.В.
Romashkina N., Mahukova A.

КОМПЬЮТЕРНАЯ ВРЕДОНОСНАЯ АТАКА НА ЯДЕРНУЮ ПРОГРАММУ ИРАНА

COMPUTER MALWARE ATTACK ON IRAN'S NUCLEAR PROGRAM

Аннотация. *Вредоносная компьютерная программа Stuxnet известна в СМИ как вирус, причинивший физический вред объектам ядерной программы Исламсой Республики Иран – а именно заводу по обогащению урана в Натанзе и АЭС «Бушер». В статье проведен анализ влияния компьютерных атак с применением вредоносных программ Stuxnet, Duqu, Flame и Wiper на развитие ядерной программы Ирана.*

Annotation. *A computer worm named Stuxnet is believed to harm industrial facilities in Iran, particularly the uranium enrichment facility in Natanz and the Bushehr nuclear power plant. This paper presents an analysis of computer malicious programs Stuxnet, Duqu, Flame and Wiper impact on Iran's nuclear policy.*

Ключевые слова. *Ядерная программа Ирана, Stuxnet, Duqu, Flame, Wiper, кибер-атака, кибер-терроризм, кибер-война, вредоносная программа, компьютерная атака, Договор о нераспространении ядерного оружия (ДНЯО).*

Key words. *Iran's Nuclear Program, Stuxnet, Duqu, Flame, Wiper, Cyber-Attack, Cyber-Terrorism, Cyber-Weapon, Cyber-War, Malicious Program, Computer Attack, Nuclear Nonproliferation Treaty.*

Вредоносные программы (ВП) *Stuxnet*[1], *Duqu*[2] *и Flame*[3] были обнаружены специалистами из разных стран в период 2010-2012 гг. Их объединяет ряд технических параметров, высокая сложность кода и цели, для которых они, по всей видимости, были созданы. Специалисты по информационной безопасности отмечают, что функционал данных ВП отличается от привычного в сфере киберпреступности. В частности, глава «Лаборатории Касперского» Евгений Касперский в сентябре 2010 г. сравнил этот факт с открытием «ящика Пандоры» и заявил, что ВП Stuxnet «была создана не для хищения денежных средств и индивидуальных данных пользователя, не для рассылки

[1]*Stuxnet* — компьютерный червь, вредоносная троянская программа, предназначенная для атаки на компьютеры под управлением системы визуализации производственных процессов Siemens WinCC (Worm.Win32.Stuxnet.a / Все об интернет-безопасности. — URL: http://www.securelist.com/ru/descriptions/15071649/Worm.Win32.Stuxnet.a.). Распространяется на сменных носителях. Название получила от двух драйверов (mrxnet.sys и mrxcls.sys), которые она встраивает в систему ОС Windows (например, c:\windows\system32\drivers\mrxnet.sys) (The Stuxnet Sting / Microsoft Malware Protection Center. TechNet Blogs. -2010. July 16. — URL: http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx.).

[2]*Duqu* — компьютерный сетевой червь, вредоносная троянская программа, предназначенная для кибер-шпионажа. Программа собирает информацию о системе, снимает скриншоты, ищет файлы, перехватывает пароли (А. Гостев. Тайна Duqu: Привет, "Mr. B. Jason" и "Dexter" / Все об интернет-безопасности. — 2011. Ноябрь, 11. — URL: http://www.securelist.com/ru/blog/40855/Tayna_Duqu_Privet_Mr_B_Jason_i_Dexter) и т. д. Распространяется посредством электронной почты: пользователь получает письмо, адресованное конкретно атакуемой компании, открывает приложенный к письму документ, содержащий эксплойт уязвимости и инсталлятор троянца, после чего эксплойт начинает работать, а когда пользовательская активность прекратится, запускается дроппер троянца. Название червь получил из-за префикса «~DQ», который использовался во всех именах файлов, создаваемых им (W32.Duqu. The precursor to the next Stuxnet (Version 1.4) // Symantec Corporation. — 2011. November 23. P. 1).

[3]*Flame* — троянская программа, бэкдор, имеющий также черты, свойственные червям, созданный для кибер-шпионажа. Программа может записывать аудио с помощью микрофонов, подключенных к компьютеру, делать скриншоты, следить за клавиатурой и сетевым трафиком и т. д. (А. Гостев. Flame: часто задаваемые вопросы // Все об интернет-безопасности. — 2012. Май, 30. — URL: http://www.securelist.com/ru/blog/207763998/Flame_chasto_zadavaemye_voprosy). Полученные данные программа отправляет операторам через собственные командные серверы. Программа контролируется оператором и в зависимости от приказа может распространяться по локальной сети или через съемные носители. Имя получила по названию одного из модулей, отвечающих за проведение атак и заражение новых компьютеров. Flame также известен как Flamer (Identification of a New Targeted Cyber-Attack / IrCERT. — 2012. May 28. — URL: http://www.certcc.ir/index.php?name=news&file=article&sid=1894) или sKyWIper (sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks (v1.05) / Technical Report by sKyWIper Analysis Team // CrySyS Lab. — 2012. May, 31. P. 1).

Ромашкина Наталия Петровна – кандидат политических наук, профессор, ЦМБ ИМЭМО РАН, тел. (495)543-36-76;
Махукова Алена Владимировна – аспирантка, институт международных отношений (ИМО) НИЯУ МИФИ.

Romashkina Nataliya– doctor of political sciences, professor, Institute for world economy and international relations of the Russian academy of sciences (RAS), tel. (495)543-36-76.
Mahukova Alyena – graduate student, Institute for international relations of national research nuclear university «MEPhI».

спама, а в целях вредительства на предприятиях и выведения из строя индустриальных систем»[1]. Подобные системы широко используются в нефтепроводах, электростанциях, крупных коммуникационных системах, аэропортах, судах и даже глобальных военных установках.

ВП Stuxnet в июне 2010 г. обнаружил специалист из белорусской фирмы «ВирусБлокАда» Сергей Уласень. Сообщения, впоследствии приведшие к открытию Stuxnet, поступили из Ирана[2].

С. Уласень и его коллеги опубликовали подробное описание ВП, использовавшего электронные подписи компаний Microsoft и Realtek, на специализированных интернет-форумах. Первыми на сообщение С. Уласеня обратили внимание известный IT-журналист Брайан Кребс и специалист по компьютерной безопасности Фрэнк Болдуин. Последний высказал предположение о том, что программа Stuxnet имеет некую связь с системой контроля диспетчерского управления и сбора данных SCADA (Supervisory Control and Data Acquisition) WinCC фирмы Siemens, и о том, что программа была написана для шпионажа[3].

В результате анализа кода Stuxnet выяснилось, что впервые его следы были зарегистрированы еще в 2005 г., а первые образцы поступили в базы данных антивирусных компаний в 2007 г.[4] Эта версия получила название Stuxnet 0.5, и она имела несколько иной функционал, отличающийся от Stuxnet 1.x. Заражение компьютеров Stuxnet 0.5 прекратилось в июне 2009 г.

В июле 2010 г. компания Symantec запустила систему мониторинга трафика вируса Stuxnet, что позволило ей отследить число зараженных компьютеров в отдельных регионах. В результате была собрана статистика, показывающая, что больше всего зараженных вирусом Stuxnet компьютеров — почти 60% — расположено в Иране (см. рис. 1). В общей сложности в Иране к сентябрю 2010 г. оказались заражены более 60 тыс. компьютеров. Кроме того, оказалось, что большая часть пораженных компьютеров использует в своей работе ПО Simatic Step 7, разработанное компанией Siemens AG.[5]

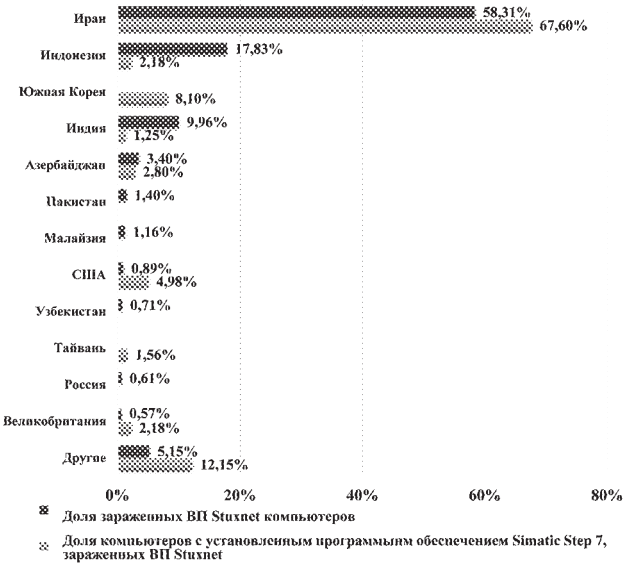

Рис. 1. Распространение компьютеров, зараженных ВП Stuxnet[6]

В ходе анализа заражений компьютеров программой Stuxnet эксперты корпорации Symantec выявили, что изначально ВП была направлена против пяти организаций, каждая из которых имеет представительство в Иране[7].

Первое упоминание о ВП Duqu зарегистрирова-

[1]Kaspersky Lab provides its insights on Stuxnet worm // Kaspersky Lab. — 2010. September 24. — URL (http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm).

[2]The Man Who Found Stuxnet — Sergey Ulasen in the Spotlight // Eugene Kaspersky's Blog. — 2011. November, 2. URL: http://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight.

[3]Rootkit.TmpHider // Post at Wilders Security Forums. — 2010. July, 22. — URL: http://www.wilderssecurity.com/showthread.php?p=1712134#post1712134.

[4]McDonald, G., L. O Murchu, Doherty, S., Er. Chien. Stuxnet 0.5: The Missing Link (version 1.0) // Symantec Corporation. — 2013. February 26. — P. 2. – URL: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf.

[5]Функционал ВП Stuxnet включает в себя: распространение на сменных носителях; мониторинг за работой ПО Simatic Step 7; выполнение SQL-запросов для сбора данных из таблиц определенного типа; сбор информации из файлов со следующими расширениями: .S7P , .MCP и .LDF; отправка собранных данных через Интернет на серверы злоумышленников в зашифрованном виде (Rootkit.Win32.Stuxnet.a. Описание вредоносной программы // Все об интернет-безопасности. — 2010. Сентябрь, 20. — URL: http://www.securelist.com/ru/descriptions/15071647/Rootkit.Win32.Stuxnet.a). В коде Stuxnet содержатся компоненты, указывающие на его направленность против частотных конвертеров, поставляемых либо иранской компанией Fararo Paya, либо финской Vacon, либо и той, и другой (Chien Eric. Stuxnet: A Breakthrough. Symantec Blogs. 2010, November 12. http://www.symantec.com/connect/blogs/stuxnet-breakthrough). При этом Stuxnet конкретно поражает конвертеры, работающие с частотами от 807 до 1210 Гц. Выяснилось, что ВП меняет выходные частоты преобразователей и скорости соответствующих им моторов в течение месяцев, чтобы его работа была незаметна. При этом вирус то повышал частоту вращения ротора выше предельно допустимой, то резко снижал ее (например, с 1410 Гц до 2 Гц) (D. Albright, P. Brannan, Ch. Walrond. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? // ISIS Report. 2010. December, 22. P. 4).

[6]Махукова А. В. Распространение компьютерных вирусов Stuxnet, Flame, Duqu в контексте ядерной проблемы ИРИ. ИМО МИФИ, 2012.

[7]Falliere, L. O Murchu, Er. Chien. W32.Stuxnet Dossier (version 1.4) // Symantec Corporation. — 2011. February. P. 7.

но 1 сентября 2011 г. на сервисе Virustotal.[1] В октябре Лаборатория криптографии и системной безопасности (CrySyS) Будапештского университета технологии и экономики выпустила 60-страничный анализ данной ВП[2]. Одновременно анализом кода ВП занималась «Лаборатория Касперского» (далее «ЛК»), компания Symantec и другие специалисты по информационной безопасности. И венгерские эксперты, и эксперты «ЛК» и Symantec отметили связь Duqu и Stuxnet. В CrySyS полагают, что создатели Duqu по всей видимости имели доступ к исходному коду Stuxnet, а также отмечают похожую структуру и философию построения двух ВП[3]. При этом программы были написаны на одной и той же платформе. Она получила название «Тильда», так как большинство ее файлов начинаются со значка тильды ~. Сотрудник «ЛК» Райан Нарейн отметил, что Duqu, вероятно, был создан для шпионажа за иранской ядерной программой[4].

Также выяснилось, что в каждой атаке Duqu используются уникальные файлы с отличными именами и контрольными суммами, причем цели тщательно выбираются. Большая часть зарегистрированных целенаправленных заражений компьютеров ВП Duqu произошла в Иране (см. рис. 2).

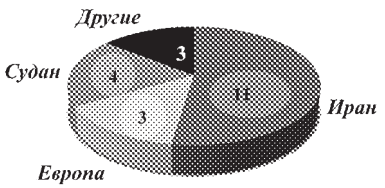

Рис. 2. Географическое распределение инцидентов заражения ВП Duqu[5]

Анализ деятельности организаций-жертв и характер информации, интересовавшей авторов ВП Duqu, свидетельствуют о том, что основной целью атакующих в иранских инцидентах были любые данные о системах управления производством в различных отраслях промышленности ИРИ, а также о торговых отношениях ряда иранских организаций.

В апреле 2012 г. в мировых СМИ появились сообщения о некой ВП, которая предположительно стерла данные с жестких дисков компьютеров в здании Министерства нефти ИРИ. *Программа* была названа *Wiper*. Его массовая атака была зафиксирована 22 апреля 2012 г., после чего иранские власти приняли решение об отключении всех нефтебаз от Интернета.[6] В то же время отмечалось, что нефтедобывающая индустрия не была затронута кибер-атакой, так как она остается преимущественно механической.

В ходе анализа кода Wiper «ЛК» сделала следующие выводы:

- именно *Wiper* ответственен за удаление конфиденциальных данных с компьютеров правительства Ирана;
- ВП *Wiper* использует платформу «Тильда» как *Stuxnet* и *Duqu*;
- в ходе расследования инцидента с удалением данным была найдена еще одна ВП, получившая название *Flame*, причем специалисты отделяют ее от *Wiper*.[7]

Эксперт «ЛК» А. Гостев считает, что *Wiper* может быть связан с израильскими разработчиками. Он указал на то, что *Wiper* создавал и удалял ключ реестра, ссылавшийся на службу Rahdaud 64. В своем микроблоге он предположил, что название модуля Rahdaud 64 образовано от имени великого библейского царя Давида (דָּוִד, в арабской традиции Daud), при котором Древний Израиль присоединил наибольшее количество территорий, и прилагательного Rah (דַּוִד), которое в переводе с иврита

[1] *Stuxnet* — компьютерный червь, вредоносная троянская программа, предназначенная для атаки на компьютеры под управлением системы визуализации производственных процессов Siemens WinCC (Worm.Win32.Stuxnet.a / Все об интернет-безопасности. — URL: http://www.securelist.com/ru/descriptions/15071649/Worm.Win32.Stuxnet.a.). Распространяется на сменных носителях. Название получила от двух драйверов (mrxnet.sys и mrxcls.sys), которые она встраивает в систему ОС Windows (например, c:\windows\system32\drivers\mrxnet.sys) (The Stuxnet Sting / Microsoft Malware Protection Center. TechNet Blogs. -2010. July 16. — URL: http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx.).

[2] Bencsáth B., Pék G., Buttyán L., Félegyházi M. Duqu: A Stuxnet-like malware found in the wild, technical report (v0.93)/ Laboratory of Cryptography of Systems Security (CrySyS). — 14 October, 2011.

[3] Duqu: A Stuxnet-like malware found in the wild, technical report. P. 5.

[4] Ryan Naraine. Duqu First Spotted as 'Stars' Malware in Iran // Все об интернет-безопасности. — 2011. November, 5. — URL: http://www.securelist.com/en/blog/208193211/Duqu_First_Spotted_as_Stars_Malware_in_Iran.

[5] Рисунок выполнен на основании следующих источников: А. Гостев. Тайна Duqu // Все об интернет-безопасности. — 2012. Март, 27. — URL, (http://www.securelist.com/ru/blog/207766975/Tayna_Duqu_chast_desyataya); Махукова А. В. Распространение компьютерных вирусов Stuxnet, Flame, Duqu в контексте ядерной проблемы ИРИ. ИМО МИФИ, 2012.

[6] Th. Erdbrink. Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet // The New York Times. — 2012. April, 23. — URL, (http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html?_r=2&).

[7] Kaspersky Lab Publishes New Research about Wiper, the Destructive Malware Targeting Computer Systems in April 2012 // Kaspersky Lab. — 2012. August, 29. — URL, (http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_Publishes_New_Research_about_Wiper_the_Destructive_Malware_Targeting_Computer_Systems_in_April_2012).

означает «злой, плохой, вредоносный»[1].

Сообщения об обнаружении ВП Flame поступили из разных источников примерно в одно и то же время — 29-30 мая 2012 г. В «ЛК» считают Flame «самым изощренным кибероружием на сегодняшний день»[2]. Сразу же были отмечены детали сходства между Flame и ранее известными Stuxnet и Duqu — это география атак, узкая целевая направленность в сочетании с использованием специфических уязвимостей в программном обеспечении. В то же время в программном коде сходства между Stuxnet и Flame на первый взгляд не было установлено, Flame не использует платформу «Тильда»[3].

Функционал Flame довольно разнообразен, однако сводится преимущественно к похищению данных. Программа направлена на получение доступа к электронным письмам, документам, сообщениям, разговорам на территории секретных объектов.[4]

Распространение Flame происходило в странах Ближнего Востока, причем наиболее активной атаке подвергся Иран (см. рис. 3).

Проводя сравнительный анализ указанных ВП, в

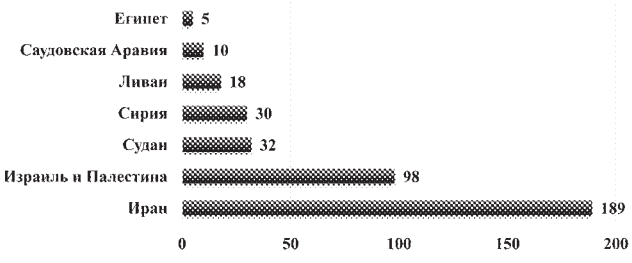

Рис. 3. Географическое распределение инцидентов заражения ВП Flame[5]

«ЛК» сравнивают Stuxnet с ракетой, оборудованной боеголовкой. При этом разгонный модуль — тело компьютерного «червя» — было использовано в Duqu, хотя «боеголовка» (в случае Stuxnet это блок, выводивший из строя центрифуги) не была установлена: ВП могла быть оборудовано дополнительно для воздействия против определенной цели. В Symantec считают, что Duqu была заготовкой для осуществления атаки типа Stuxnet. Схожие черты между Duqu и Stuxnet проявились также в идентичной архитектуре платформы двух ВП. Исходя из этого, команда «ЛК» пришла к выводу, что Duqu и Stuxnet были параллельными проектами, которые поддерживала одна и та же команда разработчиков.

Между Stuxnet и Flame на первый взгляд в программном коде не было связи, позволяющей предположить, что за созданием этих двух ВП стоят одни и те же люди. Тем не менее при более глубоком анализе экспертам «ЛК» удалось установить, что такая связь все же существует.[6] Было установлено, что на момент создания Stuxnet в начале 2009 г. платформа «Flame» уже существовала и на ее основе был написан один из модулей Stuxnet. С 2009 г., как предполагалось, развитие платформы Flame продолжалось независимо от Stuxnet.

Исходя из изложенных фактов, можно сделать вывод о том, что все упомянутые ВП связаны, причем Stuxnet, Duqu и Wiper работают на платформе «Тильда», а Flame (и несколько других) — на платформе «Flame», причем разработчики двух параллельно развивавшихся платформ по всей видимости сотрудничали. В то же вре-

[1]Twitter-аккаунт Александра Гостева. 2012. Август, 29. — URL, (https://twitter.com/codelancer/status/240833555280826368) .

[2]А. Гостев. Flame: часто задаваемые вопросы // Все об интернет-безопасности. — 2012. Май, 30. — URL, (http://www.securelist.com/ru/blog/207763998/Flame_chasto_zadavaemye_voprosy).

[3]А. Гостев. Back to Stuxnet: пропущенное звено // Все об интернет-безопасности. — 2012. Июнь, 11. — URL, (http://www.securelist.com/ru/blog/207767012/Back_to_Stuxnet_propushchennoe_zveno).

[4]Для этого она может записывать аудио с помощью микрофонов, подключенных к компьютеру, делать скриншоты (в частности, установлено, что ВП делает скриншоты при открытых приложениях обмена мгновенными сообщениями), следить за клавиатурой и сетевым трафиком (А. Гостев. Flame// Все об интернет-безопасности. — 2012. Май, 30. — URL, (http://www.securelist.com/ru/blog/207763998/Flame_chasto_zadavaemye_voprosy)). Кроме того, некоторые модули Flame разыскивали на зараженном компьютере офисные документы, документы PDF и чертежи, выполненные в системе AutoCAD («Лаборатория Касперского» проанализировала структуру управления Flame // «Лаборатория Касперского». — 2012. Июнь, 5. — URL, (http://www.kaspersky.ru/news?id=207733773)). Модули ВП целенаправленно искали DWG-файлы (создаются в программе AutoCAD), PDF и текстовые файлы, сообщения электронной почты и другие файлы, указанные в конфигурации Flame.

[5]Рисунок выполнен на основании следующих источников: А. Гостев. Тайна Duqu // Все об интернет-безопасности. — 2012. Март, 27. — URL, (http://www.securelist.com/ru/blog/207766975/Tayna_Duqu_chast_desyataya);Махукова А. В. Распространение компьютерных вирусов Stuxnet, Flame, Duqu в контексте ядерной проблемы ИРИ. ИМО МИФИ, 2012.

[6]В «ЛК» хранились все обнаруженные ранее варианты «червя» Stuxnet (их было три), в т. ч. самый ранний, вариант сборки от 2009 г. В нем еще не было цифровой подписи, но в нем содержался модуль, получивший код 207, который в двух сборках от 2010 г. был полностью удален. Когда «ЛК» получила экземпляр ВП Flame, специалисты с помощью автоматической системы начали искать, нет ли в архиве старого экземпляра червя, который мог быть получен ранее. Был найден файл Trojan-Spy.Win32.Tocy, который автоматическая система отчего-то классифицировала как Stuxnet. При более детальном анализе оказалось, что ВП Tocy.a практически идентичен модулю 207 из варианта Stuxnet от 2009 г., а также он очень похож на код Flame. Его специалисты определили как прото-Flame. При этом более корректно говорить, что Flame — это целая платформа, на исходных кодах которой был создан модуль 207 в первой сборке Stuxnet.

мя все ВП делятся по функционалу — часть из них шпионит за пользователем, часть стирает информацию с зараженного компьютера, а Stuxnet выводит из строя промышленное оборудование.

Существуют различные *версии о происхождении ВП Stuxnet, Duqu и Flame.* Поскольку с большой долей вероятности за созданием этих ВП стоит одна либо сотрудничающие команды, можно считать, что их анализ касается всех указанных ВП.

Практически сразу после обнаружения Stuxnet в «ЛК», где ее подробно изучили, пришли к мнению, что программа создана при поддержке государственных структур.[1] Анализ работы ВП с учетом многослойности нападения и легальности сертификатов доступа приводит к выводам о том, что Stuxnet был создан командой чрезвычайно квалифицированных профессионалов, обладающих обширными ресурсами и существенной финансовой поддержкой. Кроме того, ВП была нацелена на промышленные объекты, что позволило говорить о ней не просто как о примере кибер-преступности, а как о кибер-оружии, кибер-терроризме или кибер-войне. Это мнение подтвердил и топ-менеджер финской антивирусной компании F-Secure Микко Хиппонен[2].

В 2011 г. в СМИ были названы и конкретные государства-заказчики. Появилась информация о том, что за атакой Stuxnet на объекты завода по обогащению урана в Натанзе стоят Израиль и США. В январе американская газета The New York Times опубликовала, что в Израиле, в пустыне Негев, где предположительно находится исследовательский ядерный центр, была построена точная копия обогатительного завода в Натанзе, чтобы испытывать на ней кибероружие[3], а именно червь Stuxnet. При этом указывалось, что в работе принимали участие не только израильские, но и американские специалисты. Примечательно, что одним из авторов статьи выступил шеф Вашингтонского бюро газеты Дэвид Сангер.

На одной из конференций, посвященных иранской проблеме, координатор администрации США по политике в области оружия массового уничтожения (ОМУ) Гэри Самор уклонился от вопроса о ВП Stuxnet и заявил, что «рад слышать, что у них (иранцев — А.М.) проблемы с центрифугами, а США и их сторонники делают все, что возможно, чтобы сделать их еще более серьезными»[4].

На церемонии проводов уходящего со своего поста главы Армии обороны Израиля Габи Ашкенази в феврале 2011 г. был показан видеосюжет, в котором среди оперативных успехов генерал-лейтенанта Г. Ашкенази указывался и Stuxnet[5].

В декабре 2011 г. в интервью журналу IEEE Spectrum пионер программной инженерии Ларри Константин подтвердил, что основным подозреваемым в разработке Stuxnet по-прежнему считается Израиль[6].

В июне 2012 г. в свет вышла книга упомянутого журналиста The New York Times Д. Сангера «Конфронтация и сокрытие: Тайные Войны Обамы и удивительное использование американской мощи», в которой он раскрывает существование программы «Олимпийские игры», начатой в США еще во время президентства Джорджа Буша-мл. Д. Сангер указывает, что в 2006 г., когда Иран возобновил обогащение урана в Натанзе, президент США Дж. Буш-мл. поручил госсекретарю Кондолизе Райс и советнику по национальной безопасности Стивену Хэдли разработать план действий в отношении иранской ядерной проблемы. Отмечается, что на тот момент у президента существовало лишь два возможных варианта действий: начать войну в ИРИ или позволить этой стране получить ЯО.[7] В итоге зампредседателя Объединенного комитета начальников штабов США генерал Джеймс Картрайт предложил план кибер-атаки на иранские промышленные системы, и сам Дж. Буш-мл. уточнил, что атака должна быть произведена на предприятия в Натанзе[8]. При этом содействие в разработке вредоносного программного обеспечения американцам якобы оказывало «Подразделение 8200» военной разведки Израиля. Ав-

[1]Kaspersky Lab provides its insights on Stuxnet worm // Kaspersky Lab. — 2010. September, 24. — URL: http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm.

[2]Hypponen, M. Why Antivirus Companies Like Mine Failed to Catch Flame and Stuxnet // Wired. — 2012. June 1. — URL: http://www.wired.com/threatlevel/2012/06/internet-security-fail/.

[3]Broad, W. J., Markoff, J. and Sanger, D. E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay // The New York Times. — 2011. January 15. — URL: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[4]Broad, W. J., Markoff, J. and Sanger, D. E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay // The New York Times. — 2011. January 15. — URL: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[5]Williams, Ch. Israel video shows Stuxnet as one of its successes // The Daily Telegraph. — 2011. February 15. — URL: http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8326387/Israel-video-shows-Stuxnet-as-one-of-its-successes.html.

[6]St. Cherry, with L. Constantine. Sons of Stuxnet // IEEE Spectrum "Techwise Conversations". — 2011. December 14. — URL: http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet.

[7]Sanger, D. E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power // Crown Publishers. — New York. — 2012. P. 175.

[8]Ibid. P. 176-177.

тор книги утверждает, что атаки продолжались приблизительно с 2008 г., однако иранские инженеры в тот период не могли понять, что поломки центрифуг в Натанзе связаны именно с кибер-атаками. После прихода к власти в США президента Барака Обамы, курс на подрыв ядерной программы ИРИ со стороны США не поменялся. Более того, Д. Сангер отмечает, что Б. Обама начал предпринимать более активные шаги в этом направлении.[1]

В день выхода в свет книги Д. Сангера 5 июня 2012 г. Федеральное бюро расследований США (ФБР) объявило о намерении выяснить источники информации журналиста, раскрывшего детали секретной программы.[2]

Известно, что подозрения в том, что Израиль может начать кибер-войну против Ирана, появлялись и до того, как был открыт Stuxnet. Так, в 2009 г. специалист некоммерческого исследовательского института США Cyber Consequences Unit Скотт Борг заявил, что на чувствительных к вмешательству иранских предприятиях таких, как завод по обогащению урана, может быть применена какая-либо вредоносная программа.[3] После раскрытия существования Stuxnet С. Борг выразил мнение о том, что Израиль обладает возможностями для создания подобных вирусов.[4]

Вредоносные атаки на ядерные объекты ИРИ. Летом-осенью 2010 г. в СМИ появились предположения о том, что ВП Stuxnet целенаправленно атаковала предприятие по обогащению урана, расположенное в г. Натанз.[5] Эти предположения объясняются, в частности, следующими доводами.

В ноябре 2009 г. на предприятии в Натанзе были установлены и функционировали 3936 центрифуг, о чем свидетельствует отчет Международного агентства по атомной энергии (МАГАТЭ).[6] При этом в мае того же года уран подавался на 4920 центрифуг.[7] Это означает, что с мая по ноябрь количество центрифуг, работающих на предприятии в Натанзе, уменьшилось на 20%. Исследователи Института проблем науки и международной безопасности (ISIS) предположили, что такое уменьшение числа установок, может быть связано с некими поломками. На это указывал и тот факт, что центрифуги прекратили работу лишь в одном модуле, хотя такие же устройства в другом модуле продолжили работу.[8]

Примечательно, что ранее Израиль дважды предпринимал бомбардировки ядерных объектов в странах Ближнего Востока с целью предотвратить создание в них ЯО. В июне 1981 г. Израиль разбомбил иракский ядерный реактор «Озирак-1».[9] Тель-Авив объявил, что данная акция была проведена согласно провозглашенной израильским премьер-министром Менахемом Бегином доктрины о недопущении разработки арабскими странами собственного ЯО.[10] В сентябре 2007 г. израильские ВВС нанесли удар по объекту в Дейр-эз-Зор, где, как предполагается, строился ядерный реактор, известный как Аль-Кибар.[11] Полтора месяца спустя ISIS выпустил доклад, в котором данный объект был охарактеризован как предположительный ядерный реактор[12], а инспекторы МАГАТЭ, посетившие объект в июне 2008 г., нашли в почве в Аль-Кибар «существенное количество частиц природного урана», который имел «антропогенный характер, то есть этот материал произведен в ре-

[1]Sanger, D. E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power // Crown Publishers. — New York. — 2012. P. 182-184.

[2]Perez, Ev. and Entous, Ad. FBI Probes Leaks on Iran Cyberattack // The Wall Street Journal. — 2012. June 5. — URL: http://online.wsj.com/article/SB10001424052702303506404577448563517340188.html.

[3]Williams, D. Wary of naked force, Israelis eye cyberwar on Iran // Reuters Analisys. — 2009. July 7. — URL: http://www.reuters.com/article/2009/07/07/idUSLV83872.

[4]A worm in the centrifuge: An unusually sophisticated cyber-weapon is mysterious but important // The Economist. — 2010. September 30. — URL: http://www.economist.com/node/17147818.

[5]Yossi Melman. Computer virus in Iran actually targeted larger nuclear facility // Haaretz. — 2010. September, 28. — URL: http://www.haaretz.com/print-edition/news/computer-virus-in-iran-actually-targeted-larger-nuclear-facility-1.316052.

[6]Документ GOV/2009/74. Осуществление Соглашения о гарантиях в связи с ДНЯО и соответствующих положений резолюций1737 (2006), 1747 (2007), 1803 (2008) и1835 (2008) Совета Безопасности в Исламской Республике Иран. Прим. 2. (URL: http://www.iaea.org/Publications/Documents/Board/2009/gov2009-74.pdf).

[7]Документ GOV/2009/35. Осуществление Соглашения о гарантиях в связи с ДНЯО и соответствующих положений резолюций1737 (2006), 1747 (2007), 1803 (2008) и1835 (2008) Совета Безопасности в Исламской Республике Иран. Прим. 2. (URL: http://www.iaea.org/Publications/Documents/Board/2009/Russian/gov2009-35_rus.pdf).

[8]D. Albright, P. Brannan, Ch. Walrond. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? // ISIS Report. 2010. December, 22. P. 3.

[9]Саруханян, С.Н. Россия и Иран. 10 лет ядерного сотрудничества — Ер.: «Нораванк», 2006. — С. 16.

[10]Там же. С. 23.

[11]06 September 2007 Airstrike / Global Security. — URL, (http://www.globalsecurity.org/military/world/war/070906-airstrike.htm).

[12]Albright, D. and Brannan, P. Suspect Reactor Construction Site In Eastern Syria: The Site Of September 6 Israeli Raid? // ISIS. — 2007. October 23. P. 1.

зультате химической обработки»[1].

В 2007 г. генерал-майор ВВС Израиля в резерве И. Бен-Исраэль, принимавший участие в планировании уничтожения реактора «Озирак», заявил, что у Израиля есть возможность отбросить иранскую ядерную программу назад, нанеся удары по нескольким ключевым целям, среди которых — Центр по переработке урана около Исфахана, предприятие по обогащению урана в Натанзе, где устанавливаются центрифуги, и реактор на тяжелой воде в Араке, где в будущем можно будет произвести плутоний в количестве, достаточном для бомбы.[2]

Таким образом, Израиль был готов к решительным шагам в отношении ядерной программы Ирана, и атака могла произойти по иракско-сирийскому сценарию — лишение стран возможности производства ЯО путем разрушения соответствующих промышленных объектов. При этом объект в Натанзе указывался как одна из возможных целей атаки, хотя и неофициально.

Смог ли вирус навредить предприятию в Натанзе и остановить переработку и обогащение урана? В СМИ появлялись прогнозы, что ВП Stuxnet «отбросил ядерную программу Ирана на два года назад». К такому выводу пришел ранее упомянутый немецкий эксперт Р. Лангер, который заявил, что избавиться от вируса крайне сложно, а потому Ирану придется отправить на свалку все зараженные компьютеры. «Чтобы заставить свои системы снова работать, им (иранцам — А.М.) придется избавиться от вируса. Это займет время, и, возможно, им придется заменить оборудование, заново построить центрифуги в Натанзе и, вероятно, закупить новую турбину [для АЭС] в Бушере».[3]

Бывший директор службы внешней разведки Израиля генерал-майор Меир Даган отметил превосходство атаки на предприятие в Натанзе с помощью ВП Stuxnet по сравнению с обычной противобункерной бомбардировкой. Он заявил, что Stuxnet отбросил ядерную программу Ирана на четыре года назад, а после бомбардировки он восстановился бы за три года.[4]

Тем не менее в 2012 г. европейские и американские эксперты пришли к выводу о том, что Ирану удалось справиться с Stuxnet, и в настоящее время ни один компьютер данной программой не заражен.[5]

Логично предположить, что, если бы вирус нанес предприятию в Натанзе большой ущерб, обогащение урана в ИРИ замедлилось бы. Тем не менее отчеты МАГАТЭ за данный период говорят об обратном (см. рис. 4, 5).

Как видно из графиков, в период 2007-2013 гг. количество урана, обогащенного на заводе в Натанзе, равномерно росло. Более того, обогащение урана до 20% началось как раз в период, когда, по мнению экспертов, некоторая часть центрифуг была выведена из строя.

После раскрытия информации о ВП Stuxnet немецкий эксперт по кибер-защите промышленных систем Ральф Лангнер предположил, что «червь» мог быть направлен и против АЭС в Бушере. Он провел собственное исследование кода программы и, также, как впоследствии эксперты Symantec[6], заявил, что Stuxnet является инструментом для вредительства на промышленных объектах[7]. Кроме того, он обратил внимание на фотографию UPI, сделанную на АЭС в Бушере в феврале 2009 г.[8], на которой было видно, что на станции используется система SCADA с просроченной лицензией. При этом в Siemens заявляют, что компания не поставляла программное обеспечение в Иран.[9] К тому моменту уже было известно, что Stuxnet предназначен для атаки на системы SCADA, вследствие чего Р. Лангнер выразил уверенность, что ВП была нацелена именно на Бушерскую АЭС.[10]

Другой специалист по кибер-защите систем управления Дейл Питерсон согласился с доводами Р. Лангнера

[1]Док. GOV/2008/60. Осуществление соглашения о гарантиях в связи с ДНЯО в Сирийской Арабской Республике / Доклад Генерального директора. — 2008. Ноябрь, 19. С. 3.

[2]Кузнецов, Д. В. Проблема нераспространения ОМУ и общественное мнение: в 2-х частях. Ч.I: Ядерная программа Ирана. — Благовещенск: Изд-во БГПУ, 2009. — С. 260.

[3]Katz, Y. Stuxnet virus set back Iran's nuclear program by 2 years / The Jerusalem Post. — 2010. December, 15. — URL: http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475.

[4]Lemos, R. Stuxnet attack more effective than bombs / InfoWorld. — 2011. January 19. — URL: http://www.infoworld.com/t/malware/stuxnet-attack-more-effective-bombs-888.

[5]Hosenball, M. Experts say Iran has "neutralized" Stuxnet virus / Reuters. — 2012. February 14. — URL: http://www.reuters.com/article/2012/02/14/us-iran-usa-stuxnet-idUSTRE81D24Q20120214.

[6]N. Falliere, L. O Murchu, Er. Chien. W32.Stuxnet Dossier (version 1.4) // Symantec Corporation. — 2011. February. P. 2.

[7]R. Langner. Stuxnet logbook, Sep 16 2010, 1200 hours MESZ / Langner Communications. — 2010. September 16. — URL: http://www.langner.com/en/2010/09/16/stuxnet-logbook-sep-16-2010-1200-hours-mesz/.

[8]The Nuclear Issue in Iran / UPI. — URL: http://www.upi.com/News_Photos/Features/The-Nuclear-Issue-in-Iran/1581/2/.

[9]Конухов, Д. Новый вид информационного оружия испытан на иранской ядерной инфраструктуре? / Ядерный клуб. — 2011. — № 3(10). — Май-июнь. С 13-18.

[10]R. Langner. Stuxnet logbook, Sep 16 2010, 1200 hours MESZ / Langner Communications. — 2010. September 16. — URL: http://www.langner.com/en/2010/09/16/stuxnet-logbook-sep-16-2010-1200-hours-mesz/.

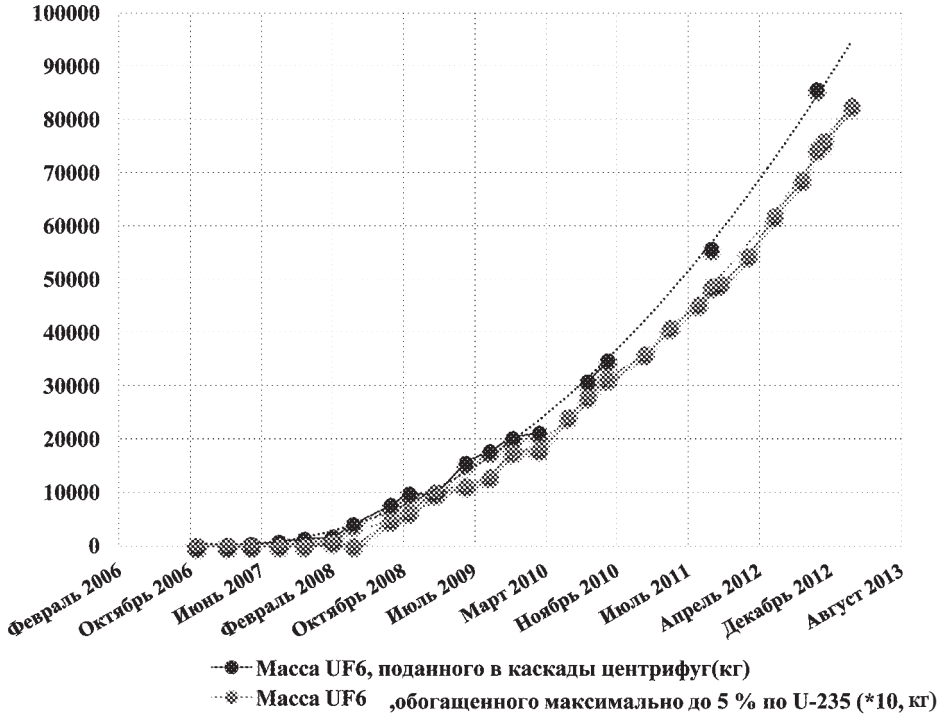

Рис. 4. Масса урана, обогащенного на заводе в Натанзе в 2006-2013 гг. (в кг)[1]

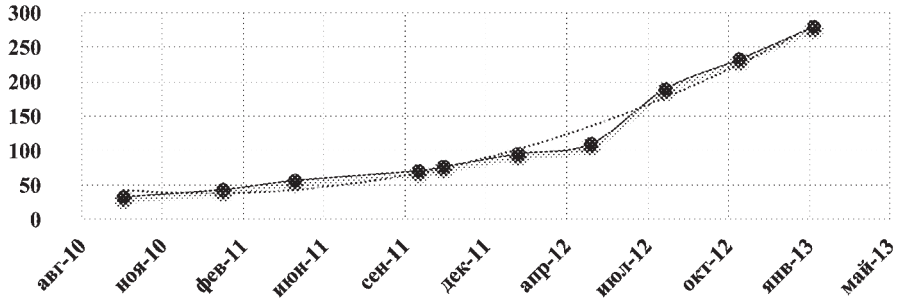

Рис. 5. Масса урана, обогащенного на заводе в Натанзе приблизительно до 20% (в кг)[2]

и отметил заинтересованность Израиля в прекращении или приостановке иранской ядерной программы, а также высокий уровень подготовки израильских специалистов по информационной безопасности.[3] При этом он напомнил, что в коде Stuxnet есть указание на одну из книг Ветхого Завета — книгу Эсфири. В коде драйверов руткита содержится авторское название этого проекта: b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb[4]. На иврите «мирт» звучит как Hadassah, и это настоящее имя Эсфири, о которой в Ветхом Завете рассказывается, что она раскрыла

[1]Рисунок выполнен на основании следующих источников: документы GOV/2007/8; GOV/2077/22; GOV/2007/48; GOV/2007/58; GOV/2008/5; GOV/2008/15/; GOV/2008/38; GOV/2008/59; GOV/2009/8; GOV/2009/8; GOV/2009/35; GOV/2009/55; GOV/2009/74; GOV/2010/10; GOV/2010/28; GOV/2010/46; GOV/2010/62; GOV/2011/7; GOV/2011/29; GOV/2011/54; GOV/2011/65; GOV/2012/9; GOV/2012/23; GOV/2012/37; GOV/2012/55; GOV/2013/6 / IAEA Reports // Сайт МАГАТЭ. – URL, (http://www.iaea.org/newscenter/focus/iaeairan/iaea_reports.shtml); Махукова А. В. Распространение компьютерных вирусов Stuxnet, Flame, Duqu в контексте ядерной проблемы ИРИ. ИМО МИФИ, 2012.

[2]Рисунок выполнен на основании следующих источников: документ GOV/2010/62; док. GOV/2011/7; док. GOV/2011/29; док. GOV/2011/54; док. GOV/2011/65; док. GOV/2012/9; док. GOV/2012/23; док. GOV/2012/37; док GOV/2012/55, GOV/2013/6. / IAEA Reports // Сайт МАГАТЭ. - URL (http://www.iaea.org/newscenter/focus/iaeairan/iaea_reports.shtml); Махукова А. В. Распространение компьютерных вирусов Stuxnet, Flame, Duqu в контексте ядерной проблемы ИРИ. ИМО МИФИ, 2012.

[3]Peterson, D. Stuxnet Target Theory / Digital Bond. — 2010. September 16. — URL: http://www.digitalbond.com/blog/2010/09/16/stuxnet-target-theory/.

[4]Гостев. Мирт и гуава: Эпизод 3 / Все об интернет-безопасности. — 2010. Июль, 15. — URL: http://www.securelist.com/ru/blog/34302/Mirt_i_guava_Epizod_3.

и предупредила заговор персов против евреев.[1]

Официальный Иран не сразу подтвердил заражение компьютеров внутри страны ВП Stuxnet. Только в сентябре 2010 г. глава Совета по информационной технологии министерства промышленности ИРИ Махмуд Лиайи заявил о том, что в общей сложности заражению в ИРИ подверглись около 30 тыс. компьютеров.[2] В то же время официальное новостное агентство IRNA процитировало слова руководителя проекта Бушерской АЭС Махмуда Джафари, который заявил, что ВП Stuxnet поразила некоторые персональные компьютеры работников АЭС. Арабоязычный телеканал Al-Alam показал интервью с М. Джафари, в котором он говорит, что АЭС в Бушере не пострадала от ВП: «Вирус не причинил никакого вреда главным системам Бушерской АЭС. Все компьютерные программы на станции работают в штатном режиме»[3]. Информацию об этом подтвердил замглавы ОАИЭ по вопросам защиты и обеспечения безопасности Ашгар Зареан. «Мы предприняли собственное расследование и не нашли следов проникновения вируса в наши системы».[4]

В начале октября 2010 г. министр разведки и национальной безопасности ИРИ Хейдар Мослехи объявил об аресте «нескольких» шпионов, следивших за ядерными объектами на территории Ирана.[5] Он также заявил, что «враги разработали и запустили через Интернет компьютерных червей, которые могли бы подорвать ядерную программу Ирана».[6] При этом объекты, на которых работали шпионы, не назывались. В конце ноября президент Ирана Махмуд Ахмадинежад признал, что предприятие по обогащению урана испытало кибер-атаку.[7] Примечательно, что при этом он не назвал само предприятие, (хотя второй иранский обогатительный центр, расположенный вблизи города Кум, был готов к работе только в октябре 2012 г.).[8] Также не было названо и орудие кибер-атаки — то есть, как предполагается, ВП Stuxnet.

Нельзя исключать и версию, что власти ИРИ не проигнорировали полностью, а все же публично отреагировали на то, что некий вирус повредил предприятие по обогащению урана лишь для отвода глаз: так они могли бы добиться смягчения западной стороны в переговорах «шестерки» по ядерной программе Ирана.

В декабре 2011 г. замглавы Генштаба вооруженных сил Ирана по вопросам культуры связей с общественностью Массуд Джазайери заявил о создании штаба по ведению «мягкой войны» в ответ на то, что «Враги превосходят себя, чтобы создать препятствия для успеха и прогресса Ирана в опыте ведения кибер-войны». А в феврале 2012 г. глава Организации пассивной обороны Ирана, генерал Голамреза Джалали заявил о создании штаба по противодействию кибернетическим угрозам и о намерении в будущем организовать первую в истории Ирана кибер-армию.[9]

По данным израильских СМИ, на создание оборонительного киберпотенциала Иран намерен потратить $1 млрд.[10]

Отметим, что неофициальная «иранская киберармия», состоящая по всей видимости из так называемых хактивистов[11] существовала еще в 2009 г. В декабре 2009 г. хакерам удалось взломать сервис микроблогов Twitter[12] — в течение нескольких часов на главной странице сайта висело изображение зеленого флага с надписью на фарси, заявлением относительно вмешательства США в дела

[1]Гуава также является растением семейства миртовых.

[2]Бушерская АЭС в Иране подверглась кибератаке / Русская служба BBC. — Последнее обновление: 2010, 26 сентября. — URL: http://www.bbc.co.uk/russian/international/2010/09/100926_iran_virus.shtml.

[3]Бушерская АЭС в Иране подверглась кибератаке / Русская служба BBC. — Последнее обновление: 2010, 26 сентября. — URL: http://www.bbc.co.uk/russian/international/2010/09/100926_iran_virus.shtml.

[4]L. Maillard. Iran denies nuclear plant computers hit by worm / AFP. — 2010. September, 26. — URL: http://www.google.com/hostednews/afp/article/ALeqM5izMHSVD4tEUYpQJa7iGAp5vJyTUw.

[5]Iran nabs several 'nuclear spies' / Press TV. — 2010. October 2. — URL: http://www.presstv.ir/detail/144871.html.

[6]Iran says cyber foes caused centrifuge problems / Reuters. — 2010. November, 29. — URL: http://www.reuters.com/article/2010/11/29/iran-ahmadinejad-computers-idAFLDE6AS1L120101129.

[7]Iran filling nuclear bunker with centrifuges — diplomats / Reuters. — 2012. October 25. — URL: http://www.reuters.com/article/2012/10/25/nuclear-iran-fordow-idUSL5E8LOFQ220121025.

[8]Jazayeri: Soft war headquarters established by Iranian Armed Forces / IRNA. — 2011, December 1. — URL: http://www.irna.ir/en/News/80437009/Politic/Jazayeri__Soft_war_headquarters_established_by__Iranian_Armed_Forces.

[9]Iran set to build first cyber army / Press TV. — 2012. February 20. — URL: http://www.presstv.ir/detail/227739.html.

[10]Katz, Y. Iran embarks on $1b. cyber-warfare program / The Jerusalem Post. — 2011. December, 18. — URL: http://www.jpost.com/Defense/Article.aspx?id=249864.

[11]Хактивизм — сетевая активность хакеров, выражающаяся в форме акций прямого действия. (Определение дано автором работы на основании документа Фр. Паже «Хактивизм. Киберпространство стало новой средой для выражения политических взглядов». — URL: http://www.mcafee.com/ru/resources/white-papers/wp-hacktivism.pdf.).

[12]Arrington, M. Twitter Hacked, Defaced By "Iranian Cyber Army" / TechCrunch. — 2009. — December 17. — URL: http://techcrunch.com/2009/12/17/twitter-reportedly-hacked-by-iranian-cyber-army/.

ИРИ и электронным почтовым адресом Iranian.Cyber.Army@gmail.com. В январе 2010 г. та же группировка атаковала китайский поисковик Baidu — на этот раз на главной странице сайта появился иранский флаг на черном фоне, надпись на фарси и на английском о том, что сайт атакован «иранской кибер-армией».[1]

Летом 2012 г. власти Ирана выразили намерение создать собственный национальный Интернет.[2] В рамках этого решения от обычного Интернета начали отключать компьютеры в министерствах и на госпредприятиях. По словам министра информационных технологий и коммуникаций ИРИ Резы Тагипура, такая сеть поможет решить проблемы безопасности. По мнению представителей неправительственной организации Freedom House, такие меры являются следствием общеиранского подхода к ужесточению политики в отношении глобальной сети.[3] Однако можно предположить, что пойти на такой шаг власти ИРИ заставили именно вирусы группы Flame, и прежде всего Wiper, который стер данные с компьютеров иранского правительства.

Хотелось бы отметить, что на протяжении последних лет Иран неоднократно заявлял о возможности выхода из ДНЯО в случае, если на его ядерную программу будет оказываться давление извне.[4] В декабре 2012 г. посол ИРИ в МАГАТЭ Али Асгар Солтание не исключил, что его страна выйдет из ДНЯО, если на ядерные объекты страны будет произведена какая-либо атака.[5] Тем не менее после обнаружения в Иране ВП Stuxnet ни один официальный представитель не делал каких-либо заявлений относительно угрозы ядерной программе Ирана или выхода из ДНЯО. Нельзя исключать, что Тегеран не стал настаивать на нелегальности кибер-атаки из-за того, что побоялся более агрессивной реакции вероятного противника, либо в руководстве ИРИ сочли, что мировое сообщество не обратит внимания на их заявление, как ранее НАТО не уделило должного внимания атаке хактивистов на правительственный сектор инфраструктуры Интернета в Эстонии, несмотря на официальное обращение властей этой страны.[6] В то же время Иран мог скрыть реальный ущерб, чтобы создать собственную кибер-армию — подтверждением данной гипотезы служит заявление генерала Г. Джалали о создании штаба по противодействию кибернетическим угрозам.

Если провести параллели между намерением ИРИ завладеть ядерным оружием и кибер-оружием, можно предположить, что после серьезной кибер-атаки (сюда относятся все упомянутые ВП, принесшие в той или иной мере вред государственной ядерной программе), которая, по мнению специалистов, были спонсированы государственными структурами соответствующих заинтересованных стран, Иран также захочет завладеть мощным кибер-оружием. Ведь стремление правительства Исламской Республики к обладанию ОМУ связывают, в частности, с тем, что в ходе ирано-иракской войны против Ирана было применено химическое оружие. С другой стороны, не исключено, что теперь ИРИ может выступить на международной арене с предложением о создании особого договора о нераспространении кибер-оружия.

Если принять за факт то, что именно Израиль запустил ВП Stuxnet, чтобы атаковать предприятие по обогащению урана в Натанзе, то можно предположить, что Израиль в борьбе с распространением ЯО в регионе начал применять новую стратегию применения не только вооруженных действий (обстрелов с воздуха, как это было в Ираке и Сирии), но и виртуального нападения. Таким образом, ядерной программе ИРИ, которую Израиль считает наибольшей ядерной угрозой на Ближнем Востоке[7], возможно, придется столкнуться с новым типом войны, к которой Иран пока не готов. Стоит ожидать, что если ИРИ не откажется от ядерной программы, как того от него требует ООН и МАГАТЭ, Израиль может предпринять ряд кибер-шагов как по отношению к заводу в Натанзе, так и к другим ядерным объектам Ирана: к обогатительной установке «Фордо» (в сентябре 2012 г. глава ОАЭИ Ферейдун Аббаси заявил о саботаже в «Фордо»: были взорваны линии электропередачи, снабжающие за-

[1]Baidu hacked by "Iranian cyber army" / BBC News. — 2010. — January 12. — URL: http://news.bbc.co.uk/2/hi/8453718.stm.

[2]Iran to launch national data network / Press TV. — 2011. August 10. — URL: http://www.presstv.ir/detail/193306.html.

[3]Kelly, S., Cook S., Truong, M. Freedom On the Net 2012. A Global Assessment of Internet and Digital Media // Freedom House. — 2012. — September 24. P. 269.

[4]Iranian Parliament to Study Withdrawal from NPT / Fars News Agency. — 2011. December 11. — URL: http://english.farsnews.com/newstext.php?nn=9007273077.

Iran threat to quit atomic treaty / BBC News. — 2006. May 7. — URL: http://news.bbc.co.uk/2/hi/4981940.stm.

[5]Iran will never halt uranium enrichment, Soltanieh says / Press TV. — 2012. December 1. — URL: http://www.presstv.com/detail/2012/12/01/275485/iran-will-not-halt-uranium-enrichment/.

[6]Защита от кибератак // НАТО от А до Я / Организация Североатлантического договора. — URL: http://www.nato.int/cps/ru/SID-92E08946-72618772/natolive/topics_49193.htm.

[7]Israel angered over IAEA vote on nuclear arsenal / Press TV. — 2012. August 27. — URL: http://www.presstv.ir/detail/2012/08/29/258819/israel-angered-over-iaea-vote-on-nukes/.

вод энергией[1]), заводу и строящемуся реактору в Араке, АЭС в Бушере.

В любом случае после атак вредоносных программ Ирану, вероятно, станет сложнее скрывать текущую стадию своей ядерной программы. С другой стороны, компьютерная агрессия может подвигнуть Иран впредь существенно больше внимания уделять информационной безопасности на своих объектах.

* * *

Можно выделить следующие факторы влияния ВП Stuxnet, Flame, Duqu на ядерную проблему ИРИ.

1. Атаки ВП Stuxnet, Duqu, Flame и Wiper могли быть нацелены на торможение ядерной программы Ирана. В настоящее время трудно оценить эффективность этих действий. Однако вред, связанный как минимум, с хищением данных, безусловно, был нанесен.

2. Можно предположить, что наибольший вред из рассматриваемых вредоносных программ в ближайшей перспективе может принести Stuxnet, которая предположительно вывела из строя несколько центрифуг на обогатительном предприятии в Натанзе и Wiper, которая удалила большое количество данных с компьютеров правительства Ирана. Опасность Duqu и Flame, которые занимались хищением данных, а значит, могли и передать разведслужбам других стран сведения о состоянии и о планах по ее развитию, а также о банковских счетах и других финансовых документах, скорее всего, будет возрастать.

3. Обнаружение ВП на территории ИРИ могло быть использовано руководством страны для смягчения переговорного процесса в рамках «шестерки». Не исключено, что руководство страны заявило о кибер-угрозе ядерной программе, чтобы произвести впечатление, что программа действительно отброшена на несколько лет назад.

4. Несмотря на вирусную атаку, вероятно, проведенную в отношении ядерного объекта в Натанзе, публичных заявлений руководства Ирана о выходе из ДНЯО не последовало.

5. Ядерная программа ИРИ столкнулась с новым видом угрозы – кибер-терроризмом или кибер-войной, к которой Иран пока не готов.

6. Военно-стратегическое руководство ИРИ уже рассматривает и будет планировать в перспективе ответы на кибер-угрозы, направленные против ядерной программы Ирана. Таким образом, даже не обладая ЯО, ИРИ в результате, вероятно, сможет получить мощное оружие, способное нанести существенный ущерб развитым странам. В первую очередь, такое оружие может быть направлено против США и Израиля.

[1] Iran nuclear chief reveals sabotage at Fordow facility / Press TV. — 2012. September 17. — URL: http://www.presstv.ir/detail/2012/09/17/262119/aeoi-chief-reveals-fordow-sabotage/.

Материал поступил в редакцию 12. 08. 2013 г.