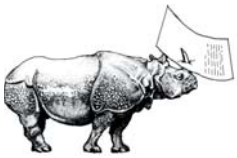

Максим Симоненко

# *STUXNET* И ЯДЕРНОЕ ОБОГАЩЕНИЕ РЕЖИМА МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В центре внимания экспертов и лиц, принимающих решения во многих странах мира, в последнее время оказался вопрос взаимосвязи ядерных и информационных технологий, прежде всего в контексте угроз и вызовов безопасности, внезапно возникших на этом *технологическом перекрестье*. Появление летом 2010 г. компьютерного вируса *Stuxnet*, целью которого, предположительно, являлась ядерная инфраструктура Ирана, резко усилило эту тенденцию. Высказываемые экспертами и СМИ предположения в основном строятся вокруг версии о том, что целью *червя* была автоматизированная система управления технологическим процессом (АСУ ТП) на иранской АЭС в Бушере, а также на обогатительных мощностях в Натанзе.

Однако системы такого типа используются на промышленных объектах самого различного назначения по всему миру: в сетях электропередач, на предприятиях по производству китайских игрушек, в используемых для обогащения урана центрифугах, а технологии управления производственными процессами на разнообразных промышленных объектах ничем принципиально не отличаются друг от друга. Перед экспертным сообществом и политическими управленцами встал вопрос, нужно ли особо выделять безопасность ядерных объектов из прочей промышленной инфраструктуры в смысле обеспечения ее информационной безопасности? От ответа на него зависят национальные и международные политики в части обеспечения информационной безопасности ядерной инфраструктуры — и пока повестка дня в этой сфере выглядит предельно размытой, а международно признанного общего подхода не просматривается.

С другой стороны, в экспертной среде *айтишников* существует убежденность в том, что опыт ядерной эпохи может быть частично применим в целях строительства универсального международного режима информационной безопасности. После обнаружения *Stuxnet* подобные взгляды лишь окрепли. Отнюдь не случайно летом 2012 г. руководитель *Лаборатории Касперского* Е. В. Касперский выступил с идеей создания *киберМАГАТЭ* как некоего межгосударственного механизма, транслирующего опыт работы Международного агентства по атомной энергии (МАГАТЭ) в область информационных технологий. Назначение такого механизма — заложить основы международного режима безопасности киберпространства, основанного на системе мониторинга, взаимных обязательств и призванного не допустить разработку кибероружия и ведение кибервойн.

Такая идея, при всей кажущейся *правильности*, неминуемо провоцирует ряд вопросов. Насколько приемы, методы и стратегические аксиомы теории ядерного сдерживания применимы к киберпространству? Будет ли достаточно для защиты от *Stuxnet* и его аналогов того, что все государства сообща выработают свод норм поведения в киберпространстве и объявят его зоной, свободной от кибероружия?

И возможно ли даже такое взаимодействие, не берущее в расчет негосударственные акторы, сегодня? Ведь, говоря языком метафор, у *здания* международного режима безопасности киберпространства не просто отсутствует фундамент — не утверждено даже *техническое задание* на его строительство и сам его проект. А если ждать, то сколько и чего дожидаться? Ведь сложные вирусы, близкие по уровню к *Stuxnet — Flame, Duqu, Gauss,* уже выявляются раз в несколько месяцев, и никто не знает, когда и с какими последствиями *выстрелит* очередное изощренное кибероружие. Такие вопросы заставляют более подробно и тщательно взглянуть на теперь уже знаменитый вирус, поразивший иранские объекты, чтобы понять, кем и для каких целей он был создан и насколько его реальный *жизненный цикл* совпал с изначальными планами его авторов. Лишь отталкиваясь от знаний об этом, мы можем понять, когда, с кем и какой режим противодействия подобным угрозам необходимо строить, каким содержанием его наполнять и что можно привнести в него от доктрин *ядерной эры*.

## *STUXNET*: *ПРОТИВОЯДЕРНОЕ* КИБЕРОРУЖИЕ

В июне 2010 г. белорусская компания *VirusBlockada*[1], специализирующаяся в области компьютерной безопасности, впервые обнаружила высокотехнологичный компьютерный вирус *RootTmphider* (позднее получивший название *Stuxnet*), направленный против АСУ ТП[2]. К концу 2010 г. в мире уже насчитывалось порядка 100 тыс. компьютеров, зараженных этим вирусом. Наибольшее число заражений было зафиксировано в Иране (58,3 %), Индонезии (17,8 %) и Индии (10 %)[3]. Вместе с тем вирус был обнаружен уже на этапе *разрастания эпидемии*, что не позволяет говорить о том, что страны с наибольшим количеством зараженных компьютерных систем являются первичным очагом распространения вируса[4]. Этот нюанс находит подтверждение в официальной статистике компании производителя АСУ ТП, против которой был направлен вирус, — *Siemens*. Согласно официальному заявлению компании, к марту 2011 г. было обнаружено 24 случая заражений компьютерным вирусом промышленных систем клиентов *Siemens*[5].

*Stuxnet*, вне сомнений, представляет собой высокотехнологичный продукт, над созданием которого работала достаточно большая и высококлассная команда. В качестве подтверждения обычно упоминается, что при разработке вируса использовались четыре ранее неизвестных уязвимости *нулевого дня*, для маскировки применялись несколько украденных официальных сертификатов крупных производителей компьютерной техники, а также привлекались технические компетенции по производственной эксплуатации АСУ ТП. Все это позволило экспертам и СМИ говорить о том, что автором *Stuxnet* было некое государство или группа государств, а сам вирус был представлен в качестве сверхсовременного силового инструмента реализации национальных интересов.

Согласно такой логике, *Stuxnet* — это *кибероружие*, имеющее колоссальную разрушительную мощь, теоретически сравнимую с оружием массового уничтожения. В середине июня 2012 г. исполнительный директор и издатель *Bulletin of the Atomic Sciences* Кеннет Бенедикт сравнила произведенный *Stuxnet* эффект с первыми ядерными взрывами в Хиросиме и Нагасаки[6]. В то же время при рассмотрении угроз из киберпространства очень часто апеллируют к концепциям эпохи холодной войны — сдерживания и возможности ответного ядерного удара. Такой подход даже нашел отражение в официальной киберстратегии Пентагона, в которой кибератаки приравниваются к традиционным военным действиям, в ответ на которые могут использоваться любые доступные средства вплоть до ядерного оружия[7]. Упомянутое выше предложение главы *Лаборатории Касперского* по созданию *киберМАГАТЭ* нацелено именно на предотвращение милитаризации киберпространства по аналогии с *традиционной* гонкой вооружений. С точки зрения российского эксперта, необходимо не просто создать институт по контролю над кибервооружениями, но по возможности «скопировать международную систему ядерной безопасности и сделать [ее] кальку на киберпространство»[8].

Но если говорить о кибероружии, кто или что является его мишенью? В настоящий момент наибольшее распространение получили две совершенно разные точки зрения на вопрос о целях *Stuxnet*. Первая версия появилась после того, как в августе 2010 г. исходный код вируса стал доступен в интернете[9] и к его изучению присоединился широкий круг экспертов в области информационной безопасности. В середине сентября немецкий специалист в области информационной безопасности Ральф Лангнер предположил, что *Stuxnet* был направлен против какой-то определенной цели[10]. Чуть позднее удалось выявить такую цель — производственную цепочка, которая отвечала за обмен информацией между программируемым логическим контролером марки *SIMATIC S7* и рабочими станциями АСУ ТП *SIMATIC WinCC* фирмы *Siemens.* Тогда же были впервые выдвинуты предположения о том, что основной целью вируса могла быть система управления АЭС в Бушере, и уже после этого появляются первые упоминания о *Stuxnet* в контексте иранской атомной станции в неспециализированных СМИ[11].

После того как информация о вирусе просочилась в масс-медиа, проектный менеджер АЭС в Бушере Махмуд Джафари заявил, что *компьютерный червь* заразил лишь персональные компьютеры работников станции[12]. Однако руководитель Совета по информационным технологиям при Министерстве промышленности Ирана Махмуд Лиайи отметил, что «шпионский червь *Stuxnet* был создан в рамках электронной войны Запада против Ирана»[13]. Фактически никто из чиновников не признал, что вирус предназначался против каких-либо систем управления АЭС, а Лиайи вообще отметил, что *Stuxnet* был не более чем шпионским червем. При этом, однако, Д. О. Рогозин, будучи еще постоянным представителем РФ при НАТО в начале 2011 г., призвал представителей Альянса провести тщательное расследование по поводу *Stuxnet* для недопущения «нового Чернобыля»[14].

Немного позднее, по мере более тщательного изучения исходного кода вируса возникла новая версия о его конечных целях — таковыми, как выяснилось, могли быть обогатительные центрифуги на иранском заводе по обогащению урана в Натанзе[15]. В ноябре 2010 г. аналитики одной из крупнейших компаний в области информационной безопасности *Symantec* обнаружили, что *червь* был направлен не только против конкретной модели АСУ ТП, но и против конкретных высокочастотных преобразователей иранской компании *Fararo Paya* и финской компании *Vacon*[16], производственные мощности которой располагаются в Китае[17].

В свою очередь, эксперты из Института науки и международной безопасности (ISIS) предположили, что высокочастотные преобразователи именно такого типа могли использоваться на площадках по обогащению урана в Натанзе[18]. Согласно отчету ISIS, в конце 2008 — начале 2009 г. по неопределенным причинам в Натанзе сократился объем производства низкообогащенного урана[19]. В качестве основной причины сокращения эксперты Института называли возможные инженерные ошибки, допущенные в процессе расширения производственных мощностей. С мая 2008 по ноябрь 2009 г. количество функционирующих центрифуг в Иране увеличилось с 3 280 до 4 920, а затем сократилось до 3936[20]. Именно это сокращение количества находящихся в строю центрифуг на 984 было списано экспертами ISIS на счет *Stuxnet*.

К концу ноября 2010 г. президент Ирана Махмуд Ахмадинежад подтвердил, что «им [неким субъектам, действующим в интересах Запада] удалось создать проблемы для ограниченного количества наших центрифуг с помощью внедрения программного обеспечения в электронные детали»[21]. Однако Ахмадинежад ничего не сказал ни про Натанз, ни про какой-либо компьютерный вирус. А уже в феврале 2011 г. эксперты ISIS, основываясь на обновленной информации о *Stuxnet*, отказались от своей версии о том, что он мог стать причиной сокращения обогатительных центрифуг в Натанзе, поскольку функция, которая теоретически могла это сделать так и не была активирована[22]. В июне 2011 г. Лангнер пошел еще дальше и выразил сомнение в том, что вирус был вообще направлен против систем управления газовыми центрифугами[23].

Но это не помешало версии о Натанзе получить дальнейшее развитие, и в начале июня 2012 г. в *The New York Times* появилась информация о том, что высокопоставленные чиновники США и Израиля участвовали в подготовке кампании кибератак под названием *Олимпийские игры*, направленных против обогатительных центрифуг в Натанзе, и осуществлены, в том числе, посредством *Stuxnet*[24]. По информации СМИ, «в течение недели [после обнаружения вируса] его новая версия вывела из строя порядка тысячи центрифуг». Похоже, что это единственный факт, который поддается проверке в открытых источниках. Но пока нет никакой информации о том, что осенью 2010 г. в Иране были проблемы с газовыми центрифугами; наоборот, дела там идут неплохо. Так, 15 февраля 2012 г. количество центрифуг в Натанзе было в очередной раз увеличено, причем сразу на треть, до девяти тысяч[25], а к концу лета превысило 10 тыс., поэтому говорить о том, что *Stuxnet* был создан для саботажа обогатительных центрифуг в Натанзе, преждевременно, — или же кибероперация провалилась.

В данном случае уже отработанный способ определения заказчиков кибератаки по цели нападения не работает, поскольку *достоверно* ничего не известно даже о целях вируса. Вместе с тем его технологическая сложность в некоторой степени может быть преувеличена. Так, к примеру, некоторые из уязвимостей якобы *нулевого дня*, использованных при написании *Stuxnet*, на самом деле уже были известны. Согласно вирусному досье компании *Symantec*, уязвимость в файлах с расширением *.lnk* была использована еще в конце 2008 г. в составе другого вируса, а информация об уязвимости в очереди печати была опубликована в журнале по информационной безопасности *Hakin9* еще до ее использования в составе *Stuxnet*[26]. Соответственно, вирусописателям оставалось найти две из четырех использованных *Stuxnet* уязвимостей *нулевого дня*, а оставшиеся две можно было приобрести на черном рынке или найти в специализированной литературе. Подписанные сертификаты производителей компьютерной техники *Realtek Semiconductor Corp* и *JMicron Technology Corp* могли быть похищены с помощью стандартных методов, чему благоприятствует расположение офисов обеих компаний в научном парке Хсинчу (Тайвань)[27]. Для этих целей мог также использоваться *троян Zeus*, который специализируется на хищении банковской информации, но также мог применяться и для хищения подобных сертификатов[28].

Что касается технологических компетенций по эксплуатации АСУ ТП, хорошим источником информации в данном случае могла выступить программа *Национальный испытательный комплекс АСУ ТП США* (NSTB), в рамках которой на протяжении 2003–2009 гг. проводились различные мероприятия по обсуждению угроз информационной безопасности для АСУ ТП. По итогам программы весной 2010 г. был опубликован итоговый доклад с детальным описанием возможных киберугроз для АСУ ТП[29]. Применительно к *Stuxnet* эта программа интересна тем, что в ее рамках в 2008 г. был проведен Саммит по системам автоматического контроля и управления *Siemens*. В ходе саммита Марти Эдвардс из Национальной лабора-

**ЛИСТАЯ СТАРЫЕ СТРАНИЦЫ**

Ясно, что запретить разработку и использование информационного оружия на нынешнем этапе вряд ли удастся, как это сделано, например, для химического или бактериологического оружия. Понятно также, что ограничить усилия многих стран по формированию единого глобального информационного пространства невозможно. Поэтому развязки возможны только на пути заключения разумных соглашений, опирающихся на международное право и минимизирующих угрозы применения информационного оружия. Такие соглашения, как реальный вклад в международное право, могли бы только укрепить национальную безопасность подписавших их государств. При это может оказаться даже полезным опыт компромиссов и соглашений, накопленный в политике предотвращения ракетно-ядерной войны и установления стратегической стабильности и баланса сил общего назначения в Европе.

**Международные вызовы информационной безопасности. М.: ПИР-Центр, 2001.**

тории Айдахо и Тодд Стауффер из *Siemens* выступили с докладом и презентацией по возможным уязвимостям АСУ ТП, на которую был направлен *Stuxnet*[30]. Этими наработками могли уже впоследствии воспользоваться создатели вируса.

В таком случае государства могут быть не единственной категорией потенциальных заказчиков и исполнителей *Stuxnet*. А сам *червь* может быть представлен не только как *цифровой Перл Харбор* или *цифровые Хиросима и Нагасаки* — ведь как простой выстрел не всегда является военным актом, так и любое применение кибероружия не может быть приравнено к акту кибервойны. «Кибератака против энергосистем, может быть частью кибервойны, но и может быть и актом кибертерроризма, киберпреступности или даже… кибервандализма. Оценка и категоризация атаки всегда зависит от мотивации ее авторов и ее конкретных обстоятельств»[31].

Одно из наиболее креативных, но наименее обсуждаемых исследований возможных целей и заказчиков *Stuxnet* было подготовлено генеральным директором *Taia Global* Джеффри Карром в 2010 г. специально для хакерской конференции *Black Hat* в Абу-Даби. В качестве основных сценариев в нем рассматривались возможности кибератак против производств по добыче редкоземельных металлов или урановых руд для осуществления корпоративного саботажа с целью дискредитации *Siemens* или для защиты Китаем Малаккского пролива[32]. В первом случаев некая частная компания могла саботировать деятельность на шахтах конкурентов посредством кибератаки, чтобы установить контроль за глобальными поставками редкоземельных металлов.

В случае с добычей урановых руд инициатором кибератаки могла стать одна из экологических неправительственных организаций, известных своим антиядерным настроем и имеющих достаточно большие финансовые возможности (например, *Greenpeace*). В дискредитации авторитета *Siemens* в преддверии заключения соглашения о создании совместного предприятия между *Siemens* и *Росатомом* могла быть заинтересована французская компания *Areva*. Что же касается Малаккского пролива, то он представляет стратегический интерес для Китая в контексте обеспечения национальной энергетической безопасности и международной торговли.

Таким образом, теоретически не только государственные акторы, но и частные компании и неправительственные организации имели как возможности, так и мотивы для создания подобного вируса. Вместе с тем, как было показано выше, ощутимый вклад в обнаружение, изучение и создания средств защиты против *Stuxnet* был сделан негосударственными акторами — антивирусными компаниями, неправительственными организациями, исследовательскими институтами и даже индивидуальными исследователями, поэтому для создания эффективного режима международной информационной безопасности необходимо учитывать как конструктивное, так и деструктивное влияние негосударственных акторов на киберпространство в целом.



## УРОКИ *STUXNET* ДЛЯ МЕЖДУНАРОДНОГО СООБЩЕСТВА

Появление *Stuxnet* в значительной степени ускорило процесс *милитаризации киберпространства*. В настоящее время происходит институциональное оформление возможностей использования киберпространства в военных целях. При министерствах обороны ведущих мировых держав создаются *киберотделы*, разрабатываются стратегии поведения в киберпространстве, проводятся масштабные учения армии и силовых структур с имитацией кибервойны. Но уже появились первые подозрения в отношении того, что угроза в отношении информационной безопасности намеренно преувеличивается военными и компаниями по обеспечению информационной безопасности[33]. Для такой оценки имеются определенные основания, но какие же уроки стоит извлечь из появления такого высокотехнологичного вируса?

По мнению старшего научного сотрудника аналитического центра *RAND Corporation* Мартина Либицки, кибероружие имеет свою специфику[34]. Во-первых, оно способно действовать *точечно*, не нарушая функционирование других элементов и систем, внутри всей информационной технологической инфраструктуры, которая включает целые пласты человеческой жизнедеятельности, начиная с автомобилей и заканчивая системами наведения высокоточного оружия. Во-вторых, кибероружие по большому счету является *одноразовым* — единожды использованная уязвимость в информационных системах становится известной, а по прошествии времени специалистам в области информационной безопасности удается ее *закрыть*. В-третьих, очень сложно установить конечного заказчика создания кибероружия. В-четвертых, возможность оценки мощности и деструктивных эффектов кибероружия достаточно затруднена из-за недостатка информации о его конечных целях и, с другой стороны, сложности выработки точных критериев оценки эффекта от его применения.

Наибольший интерес для разработки технических мер по сокращению деструктивных эффектов от использования кибероружия является его *одноразовость*. Но как показал случай с компьютерным вирусом *Flame*, который был обнаружен весной 2012 г. и использовал часть функционала *Stuxnet*[35], кибероружие *само по себе* не одноразово. Очевидно, все большее распространение получает *модульный дизайн* изощренных вредоносных программ, причем во многих случаях отдельные модули могут заимствоваться и использоваться по отдельности, а сами программы обладают большим ресурсом модифицирования. Назвать этот ресурс бесконечным не позволяет лишь ограниченное число уязвимостей *нулевого дня*, которые создателям таких вирусов удается выявить и использовать для атаки целевых систем.

Соответственно, уместней говорить о том, что потенциал каждого конкретного кибероружия может быть сведен к *однократному* применению. Такой результат может быть достигнут за счет эффективного управления информационными системами, которые требуют своевременного обновления и обслуживания. Для этого необходимо развивать средства раннего обнаружения кибератак, совершенствовать существующие подходы к обеспечению информационной безопасности, укреплять сотрудничество между государственными органами и частными компаниями для своевременного обновления программного и аппаратного обеспечения. Целесообразно проанализировать, в какой степени подобные меры были реализованы в рамках действий по нейтрализации *Stuxnet*.

Изначально изучение вируса велось в рамках узкого круга частных лабораторий в области информационной безопасности и Центра реагирования на компьютерные инциденты в сфере систем управления промышленными процессами (ICS-CERT). Эффективность реагирования ICS-CERT на появление такой серьезной угрозы со стороны впоследствии получила не слишком высокую оценку со стороны экспертов в области кибербезопасности. Центр не смог своевременно предоставить операторам промышленных систем никаких конкретных рекомендаций по устранению уязвимостей, использованных вирусом для проникновения в системы управления промышленными объектами[36]. Лишь после того, как исходный код вируса был опубликован в интернете, к его изучению подключились исследовательские институты и частные эксперты. Сразу после этого появились первые версии относительно того, против каких технологических процессов АСУ ТП был направлен вирус, а также против каких объектов он *мог быть* направлен. Поэтому широкое распространение информации о вирусе способствовало, а не препятствовало нейтрализации его последствий.

Антивирусные компании также сделали немало для изучения вируса и создания *заплаток* для операционной системы *Windows*. Первые *дыры* были закрыты уже на следующий месяц после обнаружения вируса, а большая часть уязвимостей была закрыта в течение нескольких последующих месяцев. Вместе с тем именно благодаря антивирусным компаниям и их широкой клиентской базе, расположенной по всему миру, стало возможно отслеживать географическое распростране-

ние вирусной эпидемии. Даже несмотря на то что «любые оценки по уровню зараженности могут строиться только на основании тех данных, которые антивирусные компании получают с клиентских станций, в тех странах, где у этой компании есть клиенты»[37], практически все компании сходились во мнении, что в большей степени заражению были подвержены Иран, Индия и Индонезия. Одна из ведущих компаний в области информационной безопасности *Symantec* опубликовала детальное досье по *Stuxnet*, которое стало хорошим справочным материалом для многих экспертов, пишущих о вирусе.

Но все это было сделано в условиях, когда антивирусные компании из США, России, Белоруссии и прочих стран имели доступ к клиентским станциям в различных странах. Вместе с тем после ситуации с *Stuxnet* Иран активизировал свои усилия по созданию собственного антивируса[38], а в феврале 2012 г. появилась информация о том, что Иран запретил ввоз зарубежной продукции по обеспечению информационной безопасности[39]. Все это может привести к тому, что в дальнейшей перспективе объем технической достоверной информации о вновь обнаруживаемых вредоносных программных продуктах существенно сократится.

В качестве одного из стимулов к международному сотрудничеству в сфере информационной безопасности могут выступить неутешительные результаты тестирования ведущих антивирусов журналом *Global Control*[40]. Согласно исследованию, проведенному в конце мая 2012 г., ни один из популярных антивирусов не смог обнаружить все существующие версии уже известного червя *Stuxnet*[41]. Сможет ли в таком случае отдельная компания, пусть и поддерживаемая государством, обнаружить новые, прежде неизвестные вирусы сходного уровня сложности, или, возможно, еще более скрытные и изощренные? Очень маловероятно. То же самое справедливо и в отношении возможностей отдельно взятых государств по обнаружению подобного рода вредоносных программ и борьбе с ними.

Вместе с тем, для того чтобы устранить уязвимости на аппаратном уровне в АСУ ТП компании *Siemens*, которые были использованы *Stuxnet*, различным компаниям и иранскому правительству потребовалось немногим менее двух лет[42]. Между тем продукт уровня *Stuxnet* при наличии должных человеческих и финансовых ресурсов может быть создан с нуля за несколько месяцев. В данном контексте интерес представляет модель использования открытого аппаратного и программного обеспечения[43] для повышения *скорости устранения* возникающих угроз, что позволит увеличить конкуренцию и инновационный потенциал компаний в сфере информационной безопасности.

В результате проведенного обзора неизбежно возникает вопрос, каким образом версия о том, что *Stuxnet* был направлен против ядерной инфраструктуры, обогатит дискуссию в сфере информационной безопасности. Чем может помочь опыт режима ядерного нераспространения при решении задач обеспечения международной информационной безопасности и противодействия разработке кибероружия, подобного *Stuxnet*?

## ЗА РАМКАМИ *STUXNET*: ОПЫТ ЯДЕРНОГО НЕРАСПРОСТРАНЕНИЯ ДЛЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Работа над строительством режима ядерного нераспространения началась практически сразу после первых испытаний атомной бомбы в 1945 г. и велась исключительно узким кругом национальных государств. Такой подход обусловливался в первую очередь крайне высокими экономическими и техническими порогами для создания ядерного оружия (ЯО), преодолеть которые на тот момент были способны лишь передовые державы. Уже в 1946 г. появились первые предложения относительно того, как предотвратить распространение ЯО. В выпущенном в США докладе Ачесона–Лилиенталя содержались предложения поставить под международный контроль все военное направление ядерной деятельности. Для контроля над мирной атомной энергетикой предполагалось ввести механизмы лицензи-

рования и инспекций[44]. В качестве ключевых компонентов распространения ЯО авторы доклада отмечали добычу урановых руд и производство расщепляющихся материалов[45].

К началу 1950-х гг. количество и объем разведанных урановых залежей значительно выросли[46], в результате чего монопольный контроль за ними становился практически невозможнен, поэтому дальнейшие усилия по созданию режима ядерного нераспространения осуществлялись в ключе противодействия распространению технологий производства расщепляющихся материалов оружейного качества. Изначально процесс производства таких материалов был энергоемким и требовал значительных производственных мощностей. Так, к примеру, лаборатория по производству необходимых ядерных материалов в ходе реализации Манхэттенского проекта к 1945 г. потребляла электроэнергии в три раза больше, чем высокоразвитый индустриальный Детройт (США), а в момент наибольшей загруженности на проекте работало порядка 12 тыс. человек[47].

Примерно через десятилетие в СССР появились более простые и дешевые технологии производства ядерных материалов путем обогащения урана в газовых центрифугах. За этим последовало появление целого ряда программ по созданию газовых центрифуг в Израиле и Франции (1960 г.), Китае (1961 г.), Австралии (1965 г.), Швеции (1971 г.), Италии и Индии (1972 г.), Японии (1973 г.) и Бразилии (1979 г.)[48]. Все это привело к тому, что Китай, Франция, Индия, Израиль[49] использовали эти программы для создания ядерного оружия.

Для предотвращения распространения ядерных технологий военного назначения в середине 1950-х гг. было создано Международное агентство по атомной энергии (МАГАТЭ). Предполагалось, что государство, которое хочет использовать мирную атомную энергетику, но не имеет достаточных технологий и компетенций, может получить их у МАГАТЭ. В обмен на это государство должно было заключать соглашение с МАГАТЭ, по которому последнее получало право проведения инспекций на местах для верификации того, что полученные технологии не используются для разработки ядерного оружия. Но неотъемлемой частью любого международного режима, помимо институтов и правил поведения, являются нормы и принципы, в соответствии с которыми выстраиваются взаимодействия между участниками международного общения. Такие нормы и принципы несколько позднее были сформулированы в Договоре о нераспространении ядерного оружия (ДНЯО), который был принят в конце 1960-х гг. А еще позже сформировался механизм экспортного контроля за *чувствительными* технологиями, включая технологии мирного ядерного цикла, которые потенциально могут быть использованы в военных целях.

За последнее десятилетие также был сделан ряд шагов по усилению режима нераспространения. В частности, была принята резолюция ООН № 1540 с призывом к государствам-участникам привести механизмы экспортного контроля на национальном уровне к международным стандартам. Также была принята Инициатива по безопасности в борьбе с распространением оружия массового уничтожения (ИБОР), построен и усилен ряд других финансовых и экспортных режимов.

При рассмотрении этого *краткого резюме* опыта человечества в области ядерного нераспространения возникает закономерное стремление транслировать накопленный опыт на киберпространство и повестку контроля за разработкой кибероружия.

Если при создании ядерной бомбы *точкой отсчета* являются урановые руды, цикл использования которых включает добычу, обработку, обогащение и заканчивается производством ядерной энергии, то для создания кибероружия (информационного по своей природе) такой точкой становятся *сигналы*. Для того чтобы информационные сигналы можно было преобразовать в законченное кибероружие, им потребуется пройти ряд процессов, по смыслу весьма похожих на обогащение урановых руд (см. таблицу)[50].

Изначально получается (добывается) сигнал, выступающий в роли сырья для создания кибероружия. Затем добытое сырье — *данные* — проходят когнитивное структурирование (обработку) и превращаются в *информацию*. Этап адаптации информации к решению конкретной задачи (обогащение) наиболее *чувствителен*, как и в случае с ядерными технологиями, поскольку именно здесь происходит выбор того, как будут использованы полученные знания — в военных или мирных целях. Этот выбор может происходить как внутри какого-либо института, так и внутри человека. Если в рамках организационных структур теоретически возможно создавать внешние механизмы контроля выбора, в какую сторону преобразовывать информацию, то создать подобные механизмы внутри человека технологическими способами невозможно. По сути, кибероружие — это знания, которые были созданы и агрегированы для достижения определенных целей в киберпространстве, но односторонними де-факто *силовыми* средствами. В таком случае запретить производство кибероружия едва ли возможно, поскольку речь фактически будет идти о запрете на производство знаний в условиях информационного общества.

*Таблица 1.* **Условная схема преобразования сигнала в знания**

| |
|---|
| **Сигналы** (фактически сырье) *поступают в аналоговом виде на датчик* |
| ↓ |
| **Данные** (добытое сырье) *фиксируются в цифровом виде* |
| ↓ |
| **Информация** (обработанное сырье) *когнитивное структурирование* |
| ↓ |
| **Знание** (обогащение сырья) *адаптация к решению конкретной задачи* |



Поэтому опыт технического контроля над обращением ядерных материалов и технологий лишь в малой степени может быть применим для предотвращения распространения кибероружия. Вместе с тем опыт развития мер доверия, обмена информацией, накопленный в *ядерную* эру, может быть использован либо уже используется для противодействия вызовам международной информационной безопасности. В этом плане интересна работа национальных центров по уменьшению ядерной опасности, использовавшихся для обмена информацией об угрозах. Нечто подобное уже реализовано в рамках правительственных и неправительственных компьютерных групп реагирования на чрезвычайные ситуации. Вместе с тем накопленный опыт контроля над ядерными вооружениями отражает преимущественно двусторонний опыт взаимодействия между СССР (впоследствии РФ) и США. Для создания эффективного режима международной информационной безопасности требуется *многосторонний* формат, поскольку природа киберпространства трансгранична. Если в режиме будут *белые пятна*, он не будет эффективным. Кроме того, опыт ядерного нераспространения также не дает ясных ответов на вопрос о том, как можно включать негосударственных акторов в строительство международного режима безопасности.

Но будет преждевременно говорить о том, что режим ядерного распространения завершил свое формирование и справился со всеми актуальными технологическими вызовами. К примеру, установить полный международный контроль над технологиями обогащения урановых руд так и не удалось до сих пор. Главная причина заключается в том, что в силу своих технических характеристик — компактности, легкости производства невозможности провести границу между военным

и мирным использованием — газовые центрифуги становятся беспрецедентным вызовом для существующих институтов нераспространения[51]. Газовые центрифуги являются неотъемлемым элементом инфраструктуры мирного атома. При этом определить, происходит ли обогащение урана для мирных или военных целей без проведения инспекций на ядерных объектах в существующих условиях практически невозможно. Ярким примером такой проблемы, по иронии судьбы, стал нынешний кризис вокруг ядерной программы того же Ирана, ядром которой является деятельность по обогащению урана, ведущаяся и на пораженных *Stuxnet* мощностях в Натанзе.

Сегодняшняя ситуация вокруг Ирана высвечивает и еще одну принципиально важную тенденцию: мощный импульс развития, который был придан режиму ядерного нераспространения в связи с интенсификацией процесса сокращения стратегически арсеналов двух *ядерных гигантов* в 1990-х гг., постепенно начинает *затухать*[52]. Поэтому сегодня возникает потребность в выработке новых мер для дальнейшего развития режима нераспространения, в том числе ядерного разоружения уже на многосторонней основе[53]. Но, как это чаще всего бывает, то, что работает для двоих, не всегда работает должным образом для пятерых и уж тем более для девяти участников. Будет необходимо вырабатывать новые способы верификации соблюдения многосторонних договоренностей как в области более *глубокого* разоружения, так и по вопросам всеобъемлющего запрета ядерных испытаний и производства расщепляющихся материалов для военных целей.

Таким образом, можно увидеть общие проблемные точки как у уже существующего режима ядерного нераспространения, так и у еще не созданного режима международной информационной безопасности. К их числу следует отнести необходимость выработки *социальных* методов предотвращения распространения ядерного и кибернетического оружия, а также потребность в создании многостороннего (а возможно и *многосубъектного*, с участием негосударственных акторов) формата по контролю над вооружениями. Поэтому было бы вполне логично объединить усилия из сообществ *ядерщиков* и *айтишников* для нахождения совместных решений описанных проблем. Начать можно, к примеру, с поиска ответов на вопрос о том, как объекты гражданской ядерной инфраструктуры могут быть вписаны в международный режим информационной безопасности.

В отношении объектов гражданской ядерной инфраструктуры актуальны два направления деятельности, которую в общем справедливо охарактеризовать как обеспечение информационной безопасности:

- с одной стороны, информационная безопасность как таковая (предотвращение распространения чувствительной информации);
- с другой стороны, физическая безопасность, то есть устойчивость функционирования процессов работы с ядерным материалом и прочие элементы информационных систем по обеспечению безопасности объектов[54].

К объектам гражданской ядерной инфраструктуры можно отнести обогатительные мощности, лаборатории и исследовательские институты, исследовательские реакторы и АЭС. Сбои в обеспечении информационной безопасности на таких объектах могут привести, во-первых, к распространению чувствительной ядерной информации, а во-вторых, к недопустимым социальным последствиям. В тех странах, где доля атомной энергии в общем национальном энергобалансе достаточно высока (Франция, Япония, Украина, Германия и др.), речь может идти о негативных экономических эффектах, а также о снижении уровня доверия населения к атомной энергии[55].

На объектах гражданской ядерной инфраструктуры для обеспечения информационной безопасности используется общий для всей сферы ИКТ стандарт ISO 17799 (2000). С 2005 г. была разработана серия обновленных стандартов ISO/IEC 27000, которые получили позитивную оценку МАГАТЭ и будут использо-

ваться при разработке принципов информационной безопасности на объектах мирной гражданской ядерной инфраструктуры. Также в настоящий момент разрабатывается новый стандарт в рамках Международной электротехнической комиссии (МЭК) IEC 62645. Но вместе с тем эти стандарты не учитывают специфику ядерной отрасли по следующим параметрам, которые в первую очередь касаются вопросов физической ядерной безопасности[56]:

- *жизненный цикл* объектов гражданской ядерной инфраструктуры, в котором на каждом этапе подходы к обеспечению информационной безопасности могут различаться;
- *большая требовательность АСУ ТП*, использующихся на ядерных объектах, к точности вычислений, устойчивости работы по сравнению с другими ИТ-системами;
- *наличие удаленных центров управления*, которые в случае чрезвычайной ситуации позволят сохранить контроль за ядерными объектами, что требует создания дополнительных коммуникационных каналов, которые могут быть использованы злоумышленниками;
- необходимость *разработки проверенных процедур обновления программного обеспечения*;
- отработка *процедур закупки качественной компьютерной техники* (без каких-либо закладок или *черных ходов* для получения несанкционированного доступа к компьютерным системам);
- включение *условий в контракты по выполнению работ на субподряде* по недопущению компрометации компьютерных систем со стороны третьих лиц.

Поэтому в 2011 г. в рамках Технической рабочей группы МАГАТЭ по контрольно-измерительным системам АЭС (TWG-NPPIC) была запущена Координированная исследовательская программа (CRP) по безопасности цифровых контрольно-измерительных систем. В рамках инициативы МАГАТЭ было выпущено несколько технических руководств по информационной безопасности, в текущем году планируется публикация более широкого и обзорного доклада *Technical Challenges and Solutions in Application of Digital I&C Systems in NPP.*

Но, как уже отмечалось ранее, одних технологических методов предотвращения киберугроз будет недостаточно, поэтому необходимо развивать международное сотрудничество в этой сфере. Первые шаги в этом направлении были сделаны уже в этом году. В итоговое коммюнике Сеульского саммита по ядерной безопасности в марте 2012 г. вошел раздел, посвященный информационной безопасности на ядерных объектах. Основной акцент в документе делается на меры по предотвращению распространения чувствительной ядерной информации, тогда как проблемы информационной безопасности на уровне физической ядерной безопасности не затрагиваются. Об этом можно судить по тому, что в разделе по информационной безопасности делаются ссылки на резолюцию Генеральной конференции МАГАТЭ по ядерной безопасности GC (55)/Res/10 и резолюцию Международного союза электросвязи № 174[57], которые посвящены сугубо вопросам безопасности чувствительной информации. Это предположение также находит подтверждение в презентации представителя посольства Великобритании[58] в США Кейна Полларда на конференции PONI Spring Conference в апреле 2012 г. [59].

МАГАТЭ, в свою очередь, оценивает такой характер угроз для элементов гражданской ядерной инфраструктуры как низкий или средний[60]. А источники угроз, представляющие наибольшую опасность для ядерных объектов и располагающиеся на уровне физической ядерной безопасности, не вошли в раздел итогового коммюнике по информационной безопасности. Поэтому необходимо учесть это обстоятельство и привлечь к нему внимание мирового сообщества. Одной из под-

ходящих для этого площадок видится предстоящий в 2014 г. Саммит по ядерной безопасности в Нидерландах.

С другой стороны, возникает не менее важный вопрос о том, каким образом гарантии безопасности для объектов гражданской ядерной инфраструктуры могут быть *инкорпорированы* в международный режим информационной безопасности? Для поиска ответа на этот вопрос требуется более широкое обсуждение проблематики среди экспертов в сфере ядерных и информационных технологий. Изначально это может быть сделано на какой-либо разовой площадке, но впоследствии может потребоваться более тесное сотрудничество между представителями обеих сфер, а также полноценная институционализация такого взаимодействия. По этому пути уже пошли США, где в начале 2009 г. в рамках Министерства обороны был создан Отдел заместителя министра обороны по глобальным стратегическим вопросам. В повестку новой структуры вошли задачи по выработке политики в сфере предотвращения распространения оружия массового поражения, обеспечения ядерной и информационной безопасности, а также решении вопросов, связанных с космосом. Такой опыт релевантен и для России; кроме того, со временем он может быть опробован и на международном уровне, к чему российскому руководству стоит приложить активные усилия.

## ЗАКЛЮЧЕНИЕ

*Stuxnet* вывел целый ряд проблем и сюжетов на авансцену международной дискуссии о будущем режима МИБ и взаимосвязи цифровых и ядерных технологий. Во-первых, *червь* показал, что вопросы создания сколь угодно сложных вредоносных программ, равно как и задачи борьбы с ними, решаются не только силами государств и требуют вовлечения негосударственных акторов. Как дает понять анализ, возможности и мотивы для создания *Stuxnet*, наряду с государствами, имели частные компании, а коммерческие лаборатории сыграли ключевую роль в борьбе с ним. Отсюда вытекает первый вывод: для создания эффективного режима международной информационной безопасности необходимо учитывать разнонаправленное (конструктивное и деструктивное) влияние негосударственных акторов на весь процесс разработки кибероружия и средств защиты от него. Этот фактор обусловливает принципиальное отличие будущих режимов информационной безопасности и контроля над кибероружием от режима контроля над ядерными вооружениями, в которых роль негосударственных акторов была и остается скорее маргинальной.

Второе отличие заключается в диаметрально противоположном сочетании свойств *потенциала применения* и *авторства* ядерного и кибероружия. Ядерное оружие всегда рассматривалось как средство однократного применения, при этом по умолчанию подразумевалась полная ясность относительно того, кто владеет им и применяет его. Без четкой и однозначной атрибуции ядерных арсеналов были бы невозможны любые варианты сдерживания. В случае со *Stuxnet* Иран и другие страны столкнулись с нерешенной проблемой атрибуции, когда подозрения в отношении США и Израиля не могут быть доказаны, а круг потенциальных агрессоров практически неограничен. При этом модификации и переработанные версии вируса едва ли не до сих пор продолжают поражать компьютерные сети в различных странах, а модульный принцип написания превращает кибероружие в *гидру,* способную вновь и вновь поражать системы, находя новые уязвимости и меняя используемые модули. Подобные различия делают идеи прямой *репликации* механизмов ядерного нераспространения и контроля кибертехнологий (*киберМАГАТЭ* Е. В. Касперского) в значительной степени условными.

В то же время понятно, что перспективный режим МИБ должен быть сфокусирован на цели снижения потенциала каждого конкретного кибероружия до *однократного* применения. Затянувшаяся борьба со *Stuxnet* выявила острую потребность в международных механизмах раннего обнаружения кибератак, системах глобального информирования о киберугрозах, привлечении частных компаний для

борьбы с кибероружием в рамках централизованных международных площадок типа ООН.

Однако кейс *Stuxnet* доказывает, что у режима ядерного нераспространения и у перспективного режима МИБ имеются принципиально общие моменты. К их числу относится потребность в *многостороннем* формате обоих режимов. По мере *диффузии* и удешевления атомных технологий снижаются барьеры реализации ядерных программ, вопросы нераспространения и контроля над ядерными вооружениями с новой остротой встают перед *ядерным клубом,* тщащимся сдержать импульс *ядерной пролиферации*. В этих условиях диалог по военным ядерным вопросам, некогда бывший скорее эксклюзивным правом двух сверхдержав и их союзников, превращается в многостороннюю дискуссию, где голос каждой страны имеет вес. Та же ситуация еще более четко прослеживается в сфере информационной безопасности, так как более половины стран мира обладают возможностями по развитию кибервооружений. Таким образом, опыт ядерного нераспространения, не имея параллелей с режимом МИБ в части *многосубъектности*, представляет ценный багаж в плане согласования *многосторонних* решений и подходов различных стран.

Кроме того, опыт контроля над вооружениями может использоваться для развития *социальных механизмов* обеспечения МИБ, то есть предотвращения утечек чувствительных знаний о программных разработках и системах защиты, по аналогии с *ядерным знанием*. Сегодня импульс ядерного нераспространения начинает несколько ослабевать, а сам режим находится на том рубеже, когда требуется создать и запустить новые механизмы для его дальнейшего развития. При этом частичная схожесть проблем в сферах ядерных и информационных технологий позволяет предположить, что взаимодействие экспертов из обеих областей повысит эффективность находимых решений и позволит достичь *синергии* в преодолении вызовов ядерной и информационной безопасности. В числе перспективных институциональных площадок для такого взаимодействия — Саммит по ядерной безопасности 2014 г. в Нидерландах и другие подобные мероприятия.

Наконец еще одной темой для обсуждения должно стать обеспечение гарантий безопасности объектов гражданской ядерной инфраструктуры в рамках режима МИБ. В силу ряда особенностей, выделяющих ядерные объекты на фоне прочей критической инфраструктуры, — что, опять же, проиллюстрировал *Stuxnet*, — этот вопрос должен получить отдельную нишу в рамках международного режима информационной безопасности. России стоит присмотреться к опыту других стран и начать собственное движение в этом направлении, создавая постоянные структуры, отвечающие за информационную безопасность обширной ядерной инфраструктуры страны.

КОММЕНТАРИИ

**Примечания**

[1] *VirusBlockada* также имеет офис в Москве и соответствующие лицензии на деятельность по защите конфиденциальной информации от ФСТЭК. См.: ВирусБлокАда. Официальный вебсайт. http://www.virusblokada.ru/about/(последнее посещение — 31 августа 2012 г.).

[2] Falliere N., Murchu L., Chien E. W32.Stuxnet Dossier, V1.4. Symantec. February. 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (последнее посещение — 31 августа 2012 г.).

[3] Там же.

[4] Гостев А. Мирт и гуава: Эпидемия в динамике. 2010. http://www.securelist.com/ru/blog/34361/Mirt_i_guava_Epidemiya_v_dinamike (последнее посещение — 31 августа 2012 г.).

[5] SIMATIC PCS 7: Information about Malware. Handling Stuxnet. *Siemens International.* http://support.automation.siemens.com/WW/adsearch/resultset.aspx?region=WW&lang=en&ne

tmode=internet&ui=NDAwMDAxNwAA&term=stuxnet&ID=43876783&ehbid=43876783 (последнее посещение — 31 августа 2012 г.).

[6] Benedict K. Stuxnet and the Bomb. *The Bulletin*. 2012. June 15. http://thebulletin.org/web-edition/columnists/kennette-benedict/stuxnet-and-the-bomb (последнее посещение — 31 августа 2012 г.).

[7] Department of Defense Strategy for Operating in Cyberspace. U. S. Department of Defense. July 2011. http://www.defense.gov/news/d20110714cyber.pdf (последнее посещение — 31 августа 2012 г.).

[8] Касперский Е. Net voine! Nota Bene. Евгений Касперский об интересном, приятном и наболевшем. 2011. 21 ноября. http://eugene.kaspersky.ru/2011/11/25/net-voine/(последнее посещение — 31 августа 2012 г.).

[9] Our Stuxnet timeline. Langner. 2010, December 9, http://www.langner.com/en/2010/12/09/our-stuxnet-timeline/(последнее посещение — 31 августа 2012 г.).

[10] Langner R. Stuxnet is a directed attack — 'hack of the century. 2010, September 13, http://www.langner.com/en/2010/09/13/stuxnet-is-a-directed-attack-hack-of-the-century/(последнее посещение — 31 августа 2012 г.).

[11] Автор искал информацию по запросам «*stuxnet*» и «*stuxnet bushehr*» (использовались первые 100 результатов вывода поиска) в поисковой системе *Google Статистика поиска* за периоды с 1 сентября 2010 г. по 20 сентября 2010 г. и с 21 сентября 2010 г. по 21 октября 2011 г. Количество упоминаний *Stuxnet* начинает расти именно с 21 сентября 2010 г.

[12] Stuxnet worm hits Iran nuclear plant staff computers. *BBC*. 2010, September 26, http://www.bbc.co.uk/news/world-middle-east-11414483 (последнее посещение — 31 августа 2012 г.).

[13] Hafezi P. Iran says Bushehr nuclear plant not damaged by Stuxnet. *Reuters*. 2010, September 27, http://www.reuters.com/article/2010/09/27/us-iran-cyber-bushehr-idUSTRE68Q39Z20100927 (последнее посещение — 31 августа 2012 г.).

[14] Brunnstrom D., Ireland L. Russia says Stuxnet could have caused new Chernobyl. *Reuters*. 2011, January 26, http://www.reuters.com/article/2011/01/26/us-iran-nuclear-russia-idUSTRE70P6WS20110126 (последнее посещение — 31 августа 2012 г.).

[15] Melman Y. Computer virus in Iran actually targeted larger nuclear facility. Haaretz. 2010. September 28. http://www.haaretz.com/print-edition/news/computer-virus-in-iran-actually-targeted-larger-nuclear-facility-1.316052 (последнее посещение — 31 августа 2012 г.).

[16] Falliere N., Murchu L. O., Chien E. Op. Cit.

[17] Carr J. Stuxnet's Finnish-Chinese Connection. Forbes. 2010, December 14, http://www.forbes.com/sites/firewall/2010/12/14/stuxnets-finnish-chinese-connection/(последнее посещение — 31 августа 2012 г.).

[18] Albright D., Brannan P., Walrond C. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment. ISIS. 2010. December 22. http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant (последнее посещение — 31 августа 2012 г.).

[19] Albright D., Walrond C. Iran's Gas Centrifuge Program: Taking Stock. ISIS. 2010, February 11, http://isis-online.org/isis-reports/detail/irans-gas-centrifuge-program-taking-stock (последнее посещение — 31 августа 2012 г.).

[20] Там же.

[21] Hafezi P. Iran admits cyber attack on nuclear plants. *Reuters*. 2010, November 29, http://www.reuters.com/article/2010/11/29/us-iran-idUSTRE6AS4MU20101129 (последнее посещение — 31 августа 2012 г.).

[22] Albright D., Brannan P., Walrond C. Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report. ISIS. 2011. February 15. http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/(последнее посещение — 31 августа 2012 г.).

[23] Langner R. Enumerating Stuxnet's exploits. 2011, June 7, http://www.langner.com/en/2011/06/07/enumerating-stuxnet%E2%80%99s-exploits/(последнее посещение — 31 августа 2012 г.).

[24] Sanger D. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*. 2012. June 1. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all (последнее посещение — 31 августа 2012 г.).

[25] Иран увеличил число центрифуг по обогащению урана в Натанзе до 9 тысяч. *UkraNews*. 2012. 15 февраля. http://ukranews.com/ru/news/world/2012/02/15/64131 (последнее посещение — 31 августа 2012 г.).

[26] Falliere N., Murchu L. O., Chien E. Op. Cit.

[27] Matrosov A., Rodionov E., Harley D., Malcho J. Stuxnet Under the Microscope Revision 1.1. ESET. 2010. http://eset.ru/.company/.viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf (последнее посещение — 31 августа 2012 г.).

[28] Там же.

[29] NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses. DOE Idaho Operations Office. May 2010. http://www.fas.org/sgp/eprint/nstb.pdf (последнее посещение — 31 августа 2012 г.).

[30] Edwards M., Stauffer T. Control System Security Assessments. 2008 Siemens Automation Summit. http://graphics8.nytimes.com/packages/pdf/science/NSTB.pdf (последнее посещение — 31 августа 2012 г.).

[31] Schneier B. Cyberwar. 2007, June 4, http://www.schneier.com/blog/archives/2007/06/cyberwar.html (последнее посещение — 31 августа 2012 г.).

[32] Carr J. Dragons, Tigers, Pearls, and Yellowcake: 4 Stuxnet Targeting Scenarios. 2010, November 16, http://nanojv.files.wordpress.com/2011/03/dragons_whitepaper_updated1.pdf (последнее посещение — 31 августа 2012 г.).

[33] Brito J., Watkins T. Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. Mercatus Center at George Mason University. April 2011. http://jerrybrito.com/pdf/3HNSJ39.pdf (последнее посещение — 31 августа 2012 г.).

[34] Libicki M. «Pulling Punches in Cyberspace» in Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U. S. Policy. National Academy of Sciences. 2010. http://www.nap.edu/openbook.php?record_id=12997&page=123 (последнее посещение — 31 августа 2012 г.).

[35] Подробнее см. комментарий в этом номере *Индекса Безопасности*: Демидов О., Симоненко М. Пожар в киберпространстве. С. 229–232.

[36] Peterson D. ICS-CERT: Stuxnet Lessons Learned. *Digital Bond*. 2010. http://www.digitalbond.com/2010/10/22/ics-cert-stuxnet-lessons-learned/(последнее посещение — 31 августа 2012 г.).

[37] Гостев А. Мирт и гуава: Эпидемия в динамике. 2010. http://www.securelist.com/ru/blog/34361/Mirt_i_guava_Epidemiya_v_dinamike (последнее посещение — 31 августа 2012 г.).

[38] Isayev S., Jafarov T. Iran starts making own anti-virus software. *Trend*. 2012, May 3, http://en.trend.az/regions/iran/2021650.html (последнее посещение — 31 августа 2012 г.).

[39] Isayev S., Jafarov T. Iran bans import of foreign computer security software. *Trend*. 2012, February 20, http://en.trend.az/regions/iran/1994160.html (последнее посещение — 31 августа 2012 г.).

[40] Журнал *Control Global* — одно из авторитетных изданий, специализирующихся на глобальных рынках автоматизации промышленных процессов.

[41] What's the Best Defense Against Stuxnet? A Comparison of Which Tools Are the Best for Finding Stuxnet in a System. 2012, May 28, http://www.controlglobal.com/articles/2012/stuxnet-iranian-view.html?page=full (последнее посещение — 31 августа 2012 г.).

[42] Peterson D. Stuxnet Clock Stops At 625 Days. *Digital Bond*. 2012, May 31, http://www.digitalbond.com/2012/05/31/stuxnet-clock-stops-at-625-days/(последнее посещение — 31 августа 2012 г.).

[43] Кларк У., Левин П. Обеспечение безопасности информационной магистрали. *Россия в глобальной политике.* 2010, № 3. http://www.globalaffairs.ru/numbers/74 (последнее посещение — 31 августа 2012 г.).

[44] The Acheson-Lilienthal Report: Report on the International Control of Atomic Energy. Washington, D. C.: U. S. Government Printing Office, 1946. http://www.learnworld.com/ZNW/LWText.Acheson-Lilienthal.html (последнее посещение — 31 августа 2012 г.).

[45] Там же.

[46] NPT Briefing book. Centre for Science & Security Studies, James Martin Center for Nonproliferation Studies. Monterey Institute of International Studies. 2012. http://www.kcl.ac.uk/sspp/departments/warstudies/research/groups/csss/2012nptbook.pdf (последнее посещение — 20 августа 2012 г.).

[47] AEC Handbook on Oak Ridge. Oak Ridge National Laboratory, 1955.

[48] Kemp R. Centrifuges: A new era for nuclear proliferation Nonproliferation Policy Education Center Monograph, 2012. http://npolicy.org/article_file/Centrifuges_A_new_era_for_nuclear_proliferation.pdf (последнее посещение — 31 августа 2012 г.).

[49] По сегодняшний день официальный Тель-Авив не подтверждает и не опровергает информацию о наличии у него военной ядерной программы. Официально Израиль не является членом *ядерного клуба*.

[50] Rowley J. The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science*. 2007. No 33. C. 163–180. http://jis.sagepub.com/content/33/2/163.abstract (последнее посещение — 31 августа 2012 г.).

[51] Kemp R. Centrifuges: A new era for nuclear proliferation Nonproliferation Policy Education Center Monograph, 2012. http://npolicy.org/article_file/Centrifuges_A_new_era_for_nuclear_proliferation.pdf (последнее посещение — 31 августа 2012 г.).

[52] Acton J. Low Numbers: A Practical Path to Deep Nuclear Reductions. Carnegie Endowment for International Peace, 2011. http://carnegieendowment.org/files/low_numbers.pdf (последнее посещение — 31 августа 2012 г.).

[53] Лавров С. Новый договор о СНВ в матрице глобальной безопасности. *Международная жизнь*. 2010. № 7, июль.

[54] За основу взята классификация технического руководства МАГАТЭ *Computer Security at Nuclear Facilities*, выпущенного в 2011 г. Для целей настоящей статьи классификация была упрощена и адаптирована.

[55] Announcement of a new IAEA Co-ordinated Research Programme (CRP). IAEA. 2011. http://www.iaea.org/NuclearPower/Downloads/Engineering/meetings/2011-05-TWG-NPPIC/CRP-CyberSecurity.pdf (последнее посещение — 31 августа 2012 г.).

[56] Computer Security at Nuclear Facilities. IAEA Nuclear Security Series No. 17, 2011. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf (последнее посещение — 31 августа 2012 г.).

[57] Seoul Communique. Seoul Nuclear Security Summit, 2012. http://www.thenuclearsecuritysummit.org/userfiles/Seoul%20Communique_FINAL.pdf (последнее посещение — 31 августа 2012 г.).

[58] Великобритания является автором предложений по включению раздела по информационной безопасности в итоговое коммюнике Саммита по ядерной безопасности в Сеуле в 2012 г.

[59] Pollard K. The UK Contribution to the 2012 Nuclear Security Summit. British Embassy in Washington D. C. 2012. https://csis.org/images/stories/poni/120417_Pollard.pdf (последнее посещение — 31 августа 2012 г.).

[60] Computer Security at Nuclear Facilities. IAEA Nuclear Security Series No. 17, 2011. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf (последнее посещение — 31 августа 2012 г.).