Кибероружие против энергетики

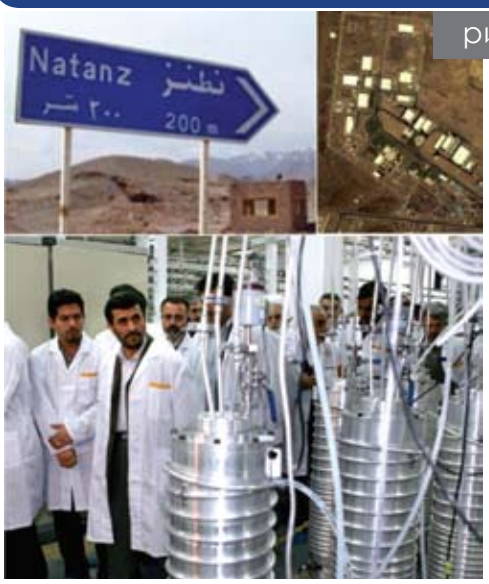
В. Гуревич, канд. техн. наук

Каменный век может вернуться на сияющих крыльях науки

Уинстон Черчилль

В последнее время в Интернете и в средствах массовой информации появилось много публикаций, включая и публикации откровенно спекулятивного характера, обсуждающих новую реальность нашего времени: кибернетические войны в виртуальном пространстве. Вот, например, по утверждению автора статьи [1] «первая кибервойна уже началась: она развязана правительствами США и Израиля против Бушерской АЭС в Иране». Интересно, чем это так не понравился чисто гражданский объект: электростанция «правительствам США и Израиля», когда в том же Иране, в Натанзе, построен целый комплекс газовых центрифуг по обогащению урана до значительно более высокого уровня, чем тот, который необходим для производства электроэнергии, рис. 1. На электростанциях используется уран U235 обогащенный до 2 – 4 %, а для производства атомного оружия степень обогащения урана должна значительно более высокой: от 80 % и выше.

рис. 1



Завод по обогащению урана в Натанзе

Впервые технология газового центрифугирования была разработана в Германии, во время второй мировой войны, но промышленно нигде не применялась до начала 50-х. Процесс обогащения урана по этой технологии заключается в том, что газообразную смесь изотопов пропускают через высокоскоростные центрифуги. При этом центробежная сила разделит легкие и тяжелые частицы на слои, где их и можно будет собрать. Рабочим веществом, в котором собственно и происходит разделение молекул с атомами разных изотопов в данной технологии, является гексафторид урана (UF6) - газообразное соединение природного урана, получаемое на специализированных химических предприятиях (например, на заводе по конверсии урана в иранском городе Исфахан, рис. 2) в результате операции химической конверсии природной закиси-окиси урана. Большое преимущество центрифугирования состоит в зависимости коэффициента разделения от абсолютной разницы в массе, а не от отношения масс.

рис. 2

На химическом заводе по производству гексафторида урана (UF6) в иранском городе Исфахан.

Центрифуга одинаково хорошо работает и с легкими, и с тяжелыми элементами. Степень разделения пропорциональна квадрату отношения скорости вращения к скорости молекул в газе. Отсюда очень желательно как можно быстрее раскрутить центрифугу. Типичные линейные скорости вращающихся роторов 250—350 м/с, а в усовершенствованных центрифугах более 600 м/с. Вращение центрифуги происходит в вакууме. Скорость вращения может быть ниже первой резонансной частоты центрифуги (при которой она может разрушиться от возникающих огромных механических усилий), и тогда такая центрифуга называется «подкритической». При увеличении оборотов центрифуга последовательно проходит частоты, на которых возникают резонансные колебания, обусловленные механическими свойствами вращающейся системы. Центрифуга, работающая на частоте вращения ротора выше резонансной, называется «надкритической». При таких больших скоростях важнейшую роль играют стабилизированные по частоте источники питания для электродвигателей, устройства автоматики для управления работой и автоматической остановки центрифуг и т.д. Отсюда становится понятным, что любое нарушение запрограммированной частоты вращения центрифуги (как увеличение этой частоты, так и внезапный сброс частоты или снижение ее до резонансной частоты, а также ее колебания) приведет к ее механическому разрушению. На этом и была основана идея выведения из строя центрифуг путем вмешательства в алгоритм работы контроллера, управляющего частотой вращения. Именно этим и занимался компьютерный червь Win32/Stuxnet, обнаруженный в контроллерах, управляющих центрифугами на заводах в Натанзе. Согласно опубликованным отчетам международных инспекторов, с 2009 года Иран вынужден был заменить сотни выведенных из строя центрифуг.

Совершенно очевидно, что все это не имеет никакого отношения

к электростанции в Бушере, несмотря на многочисленные спекуляции на эту тему. Другое дело, что атакам вируса оказываются подверженными и другие сложные системы, в первую очередь автоматические, управляющие целыми заводами, а также объектами городской инфраструктуры, включая водопровод и системы электроснабжения. Путём изменения кода логических контроллеров (Programmable Logic Controllers - PLC) вирус пытается перепрограммировать устройства управления промышленных систем, в особенности, контроллеры фирмы Siemens, чтобы, незаметно от операторов систем, захватить над ними контроль. По некоторым опубликованным данным этот вирус совершает по всему миру несколько тысяч атак в сутки на контроллеры, работающие под управлением программ Siemens. Вот на это стоило бы, по нашему мнению, обратить внимание технической общественности и в первую очередь руководителей энергетической отрасли, восхищенно и без оглядки ринувшихся в освоение технологий так называемых Интеллектуальных Сетей (Smart Grid), широкое развитие которых в России приобрело статус Государственной программы. Тем более, что случай с заражением опасным вирусом системы управления энергосистемой уже имел место. В 2009 году власти США признали, что обнаружили вирус, который мог отключить энергетические объекты страны.

Речь идет о резком увеличении уязвимости энергосистем, выполненных по технологии Smart Grid, хакерским атакам [2]. Действительно, если все элементы Smart Grid будут управляться по командам, передаваемым по сети Ethernet по протоколам TCP/IP или по беспроводным радиоканалам (как это и предусмотрено концепцией Smart Grid) то возникает огромная потенциальная опасность внешнего вмешательства в работу энергетической системы. На это обращают внимание многие эксперты. Этой теме посвящаются многие международные конференции. Одни лишь апологеты Smart Grid «не

замечают» этих проблем. Что же мы слышим в ответ от апологетов Smart Grid? Обычные отговорки о необходимости изоляции внутренней сети управления Smart Grid от внешней сети Интернет (как это и было сделано, между прочим, в Иране), об использовании паролей доступа и т.п. тривиальных мер по обеспечению безопасности. Все мы хорошо понимаем, что все эти меры защиты могут ограничить доступ к Smart Grid рядовых обывателей, но отнюдь, ни опытных хакеров, проникающих даже в очень хорошо защищенные сети министерств обороны и банков. Да что там хакеры, если в армиях многих стран мира появились специальные подразделения, состоящие из высококлассных профессионалов, предназначенные для ведения кибернетических войн, то есть для проникновения в защищенные компьютерные сети противника и выведение их из строя. Можно с уверенностью утверждать, что компьютерная сеть Smart Grid будет целью номер один для таких подразделений. «Добро пожаловать на войну XXI века, - говорил в одном из своих вступлений Ричард Кларк, в недавнем прошлом советник бывшего президента США Джорджа Буша по вопросам кибербезопасности. - Вообразите себе вспыхивающие электрогенераторы, сходящие с рельсов поезда, падающие самолеты, взрывающиеся газопроводы, системы вооружения, вдруг перестающие работать, и войска, которые не знают, куда им двигаться»[3]. Перед вами не пересказ эпизода из очередного голливудского блокбастера - это краткое описание высококлассного американского эксперта тех последствий, к которым может привести война нового формата – кибервойна.

Активнее всех здесь действуют американцы. В октябре 2010 г. в полную силу заработало Киберкомандование США (US Cyber Command - USCYBERCOM), возглавляемое генералом Китом Александером (Keith B. Alexander), рис. 3.

рис. 3

Эмблема Киберкомандования США и ее глава генерал К. Александер

Структура, ставшая частью сверхсекретного Агентства Национальной Безопасности – АНБ (National Security Agency), объединила все существовавшие ранее подразделения киберзащиты Пентагона. Уже сейчас в системе Киберкомандования работают около тысячи человек, но военные уже объявили о начале масштабной программы рекрутирования специалистов соответствующего профиля. Часть из них будут обеспечивать безопасность не только военной и государственной инфраструктуры, но и наиболее важных коммерческих объектов страны. Об этом было сообщено накануне запущенной в начале февраля программы «Кибервызов для США», в рамках которой планируется отыскать 10 тысяч юных компьютерных гениев [4].

Нынешний глава Киберкомандования, он же директор АНБ генерал Александер даже заявил на слушаниях Комитета по делам Вооруженных Сил США Палаты Представителей Конгресса, что кибероружие имеет эффект, сравнимый с эффектом применения оружия массового уничтожения. «Кибероружие развивается с большой скоростью. Многие страны - включая США, Россию, Китай, Израиль, Великобританию, Пакистан, Индию, Северную и Южную Корею - развили сложное кибероружие, которое может неоднократно проникать в компьютерные сети

и способно разрушать их, утверждают специалисты по кибербезопасности», - пишут авторы статьи Шивон Горман и Стивен Фидлер [5]. Некоторые представители американской разведки и аналитики опасаются, что кибероружие может попасть в руки террористов. «Вопрос стоит так: когда это попадет к «Аль-Каиде»?» - говорит Джеймс Льюис, специалист по кибербезопасности Центра стратегических и международных исследований [5].

А один из бывших сотрудников АНБ - Чарльз Миллер даже подсчитал, что на организацию киберструктуры, способной успешно атаковать Америку и полностью парализовать деятельность США, потребуется всего лишь 98 млн. долларов. «Для нас это одно из основных перспективных направлений, - подчеркнул на брифинге с журналистами вице-президент подразделения по разработке разведывательных и информационных систем компании Raytheon Стивен Хокинс. - Мы прогнозируем рост объемов рынка на два порядка, его стоимость составит миллиарды долларов» [4]. Бороться есть за что - кибербюджет в текущем году достиг 8 млрд долларов, а к 2014-му вырастет до 12 млрд. При этом если ежегодное увеличение расходов по другим направлениям в среднем в ближнесрочной перспективе будет на 3 - 4%, то в отношении кибербезопасности - не менее 8% ежегодно. Ведущая роль в войне нового типа, естественно, отведена военным, им же достанется и львиная доля кибербюджета: более 50% из 8 млрд. долларов 2010 года получит Пентагон. В 2011 году США планируют принять новую доктрину кибербезопасности. О ее направленности можно судить по опубликованной в сентябре программной статье заместителя главы Пентагона Уильяма Линна III с символичным названием «Защищая новое пространство». Ее главная мысль: отныне США будут считать киберпространство таким же потенциальным полем боя, как сушу, море и воздух. Параллельно над созданием концепции коллективной кибероборонны начали работать и в НАТО. На ноябрьском 2010 г. саммите альянса было решено разработать «План действий в области кибероборонны». Документ должен быть подготовлен к апрелю 2011, а подписан в июне. Важное место в нем будет отведено созданию центра НАТО по реагированию на киберинциденты. Изначально его предполагалось запустить в 2015 году, но по настоянию США срок сократили на три года, пишет «Коммерсант».

Парализация систем управления, масштабные отключения целых энергосистем, хаос в системах контроля за воздушным и наземным транспортом, нарушение работы банков и бирж, отключение интернета и сотовой связи – так, по мнению американских апологетов выглядит сценарий применения кибероружия.

Еще более осложняет ситуацию тот факт, что современные технологии позволяют создать микрочипы или записать специальные тайные команды в управляющих программах электронной аппаратуры, работающей на основе микропроцессоров, которые по определенному сигналу сделают ее эффективное использование невозможным. Приобретая и устанавливая ответственные импортные электронные системы управления для промышленности и энергетики на основе микропроцессоров сегодня уже нельзя быть абсолютно уверенным, что оно не перестанет функционировать при определенных обстоятельствах или, что еще хуже, не станет функционировать разрущающе на управляемое им оборудование, как это произошло недавно в Иране.

Никакие международные договоры по ограничению кибернетического оружия (такое предложение уже высказывалось Россией и было вежливо отклонено США) не могут быть эффективными по той простой причине, что контролировать их выполнение невозможно. Что же остается? Необходимость оценивать не только преимущества модных технологий, но и тщательно изучать последствия широкого распространения таких технологий, трезво взвешивать потенциальные опасности, особенно в такой чувствительной и важной области, как электроэнергетика, загодя разрабатывать меры по предотвращению преднамеренных разрушающих воздействий и восстановлению поврежденных систем.

ЛИТЕРАТУРА

1. Фридрих Б. Кибервойны XXI века. – Энергетика и промышленность России, 2011, №3 (167).
2. Гуревич В. И. Интеллектуальные сети: новые перспективы или новые проблемы? - «Электротехнический рынок», 2010, № 6 (часть 1); 2011, № 1 (часть 2).
3. Щербаков В. Пространство виртуальное, борьба реальная. – Военно-промышленный курьер, № 40 (356), 13.10.2010.
4. Усов А. США и НАТО мобилизуют 10 тысяч юных хакеров. Гонка кибервооружений стала новым хобби Пентагона. – РИА Новый Регион, 15 февраля 2011.
5. Gorman S., Fidler S. Cyber Attacks Test Pentagon, Allies and Foes. – Wall Street Journal, September 25, 2010.