

Электромагнитный терроризм - новая реальность 21 века

В. И. Гуревич, канд.техн.наук

Впервые теория так называемой "электронной бомбы" (*Е-бомбы*) была предложена в 1923 физиком Артуром Холли Комптоном (1892-1962). Работая одно время в Кавендишской лаборатории Кембриджского университета А. Комптон изучал рассеяние и поглощение гамма-лучей, которые представляют собой высокоэнергетическое рентгеновское излучение, испускаемое радиоактивными ядрами. Обнаружив некоторые новые эффекты, он сформулировал теорию, (которая получила название "эффект Комптона") согласно которой в результате рассеяния рентгеновских лучей электроны, на которых происходило это рассеяние, вылетают из атомов с большой скоростью. Такие "электроны отдачи", как их называл Комптон были обнаружены и экспериментально проверены позднее в этом же году Чарльзом Вильсоном, чье изобретение конденсационной (или пузырьковой) камеры (камера Вильсона) позволяло визуально наблюдать треки электрически заряженных частиц. Работы А. Комптона и Ч. Вильсона стали ключевыми в понимании свойств атома, поэтому за эти работы в 1927 году им была присуждена Нобелевская премия по физике. Конечно, А. Комптон был всего лишь теоретиком и в то время еще ничего не слышал ни о каких электронных бомбах. Вообще, А. Комптон был очень религиозным человеком и много лет возглавлял Лейменское миссионерское движение активно участвовал в работе Национальной конференции христиан и иудеев. Правда, это не помешало ему позднее, в период с 1942 по 1945 год возглавить одно из подразделений так называемого "Манхэттенского проекта" по созданию первой атомной бомбы, скрываемого в то время под вывеской "Металлургической лаборатории Чикагского университета". Именно в ней под руководством Энрико Ферми был построен первый ядерный реактор.

Об эффекте Комптона пришлось вспомнить, когда после испытательного взрыва в 1958 году над Тихим океаном первой водородной бомбы возникли неожиданные осложнения на расстоянии сотен миль от места взрыва: погасли уличные фонари на Гавайях, были полностью нарушены системы радионавигации в Австалии, была нарушена радиосвязь во многих других регионах. Вот тут-то и вспомнили о Комптоне. Вспомнили и схватились за голову: оказывается, мощный поток электронов создает в электрических и электронных приборах даже на большом расстоянии такой электромагнитный импульс который выводит из строя эти приборы и может быть использован как самостоятельный вид оружия! С этого момента и начинается история электромагнитного оружия. Ныне, интенсивные исследования в области электромагнитного оружия проводятся в России, США, Англии, Германии, и Китае, Индии и др. В США, например, такие исследования проводятся самыми большими компаниями военного-промышленного комплекса, таких как TWR, Raytheon, Lockheed Martin, Los Alamos National Laboratory, Air Force Research Laboratory on Kirtland Air Force Base, New Mexico, а также многими гражданскими организациями и университетами. В Германии работы в этой области возглавляет Rheinmetall Weapons and Munitions уже в течение многих лет. В России этим направлением занимается целый комплекс научных организаций, входящих в состав Объединенного Института Высоких Температур РАН и некоторые другие [1]. Как это ни покажется странным, но первыми мировому сообществу о своих исследованиях в области электромагнитного оружия сообщили в 1994 году именно российские ученые А. Прищипенко, В. Кисилев и С. Кадимов в своем докладе "Радиочастотное оружие на будущем поле боя" на международной конференции во Франции [2]. Этот доклад произвел в то время настоящий фурор и привел к тому, что в последствие эти вопросы стали обсуждаться в открытой печати. В дальнейшем в открытой печати появились и другие сообщения о достижениях российских ученых в этой области [3, 4, 5]. Сегодня вопросы электромагнитного терроризма уже открыто обсуждаются на зарубежных и российских научных конференциях [6], а через Интернет можно не только приобрести Е-бомбу, но и найти ее подробное описание, рис. 2 (см. <http://daily.sec.ru/dailyplshow.cfm?rid=45&pid=6276> - на русском языке). Вызывает особую настороженность тот факт, что такие описания сегодня можно найти и на многих арабских Интернет сайтах.

Еще более опасным представляется тот факт, что для создания мощного направленного пучка электронов, сжигающего все электронные и электрические цепи на своем пути, сегодня уже не нужны устройства взрывного типа.

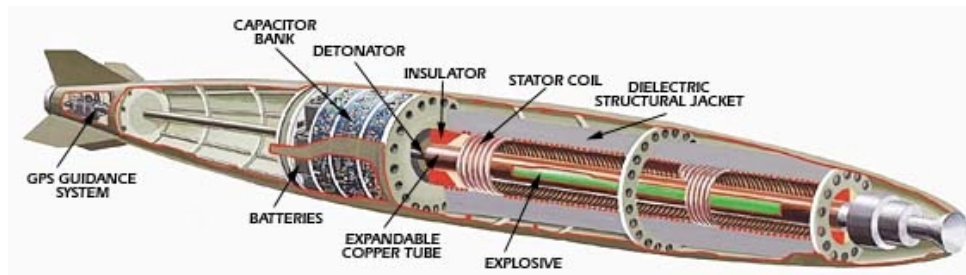


Рис. 1. Конструкция Е-бомбы (<http://www.lizmichael.com/ebomb.htm>)

Оказывается современная электронная аппаратура может генерировать направленные пучки энергии, соизмеримые по мощности со взрывом Е-бомбы. Еще более ужасным представляется тот факт, что многие виды такого секретного ранее оборудования стали свободно продаваться всем желающим [7]. Например, на Интернет сайте (http://www.hcei.tsc.ru/ssi/techn/tech3_ru.shtml) новосибирского Института Сильноточной Электроники РАН указаны все необходимые реквизиты для заказа компактных генераторов мощных направленных волновых пучков сверхширокополосного электромагнитного излучения мощностью до 1 ГВт, рис. 2. Не нужно обладать особой фантазией, чтобы представить себе такой генератор, установленный на



Рис. 2. Компактные генераторы мощных направленных волновых пучков сверхширокополосного электромагнитного излучения мощностью до 1 ГВт.

автомобиле и способный на расстоянии 500 – 1000 м за доли секунды сжечь всю электронную аппаратуру на электростанции, подстанции, главном диспетчерском пульте.

Старые, списанные радиолокаторы, оказывается, представляют не меньшую опасность и также могут быть использованы для направленного воздействия на электронную аппаратуру. Да что там радиолокаторы, если вывести из строя телевизор соседу по дому может каждый желающий, с помощью переделанной микроволновой печи. Такие, с позволения сказать "рецепты", с чертежами и подробными описаниями также можно найти сегодня в Интернете. По данным журнала "Popular Mechanics" вполне боеспособное электромагнитное оружие может быть построено сегодня даже любителем при затратах всего около 400 долларов.

"Расползанию" такого рода аппаратуры способствуют не в последнюю очередь широкое применение новых технологий в армии и в полиции. Такие "игрушки", как ручной излучатель, рис. 3, способен не только остановить автомобиль преступника, сжигая в нем всю бортовую электронику и систему зажигания, но полностью разрушить электронные системы контроля и управления на энергетических объектах, в системах охраны, связи и т.п., попади он в руки преступнику или террористу.

Зависимость нашей цивилизации от электроники, компьютеров, микропроцессоров стала столь сильной, что беспечность в сфере защиты этих систем от преднамеренного воздействия на них направленного электромагнитного излучения граничит с преступлением и может обернуться непредсказуемыми последствиями. Следует отметить, что еще несколько лет назад средства массовой информации очень неохотно публиковали статьи на эту тему, опасаясь привлечь внимание террористов и криминальных элементов. Однако, после последней крупнейшей аварии в энергосистеме США террористы сами обратили внимание на зависимость

современной Западной цивилизации от электроэнергетики в ряде своих высказываний и угроз. После этого последовал шквал статей в "Нью-Йорк Таймс" и других публичных изданиях посвященных вопросу незащищенности важнейших систем жизнеобеспечения общества от электромагнитного терроризма.



Рис. 3. Ручной генератор мощного направленного электромагнитного излучения частотой 95 ГГц разработанный компанией Raytheon.

В работе [8] прямо указывается, что электроэнергетические системы являются сегодня важнейшей целью террористических атак.

В США проблемой устойчивости электроэнергетических систем к электромагнитному терроризму уже озаботились и начали искать пути защиты. В феврале 1998 года состоялись даже специальные слушания в Конгрессе по этому вопросу. Этими вопросами сейчас занимается такая авторитетная в области электроэнергетики организация, как КЕМА, аппаратуру и испытательные стенды предоставляет Sandia National Laboratories. Этими организациями проводятся эксперименты по исследованию устойчивости систем релейной защиты, систем передачи данных и др. к искусственно сгенерированным электромагнитным импульсам большой мощности. В докладе Ю. Парфенова и В. Форгова из Объединенного института высоких температур РАН представленном на международном конгрессе в Цюрихе в 2001 году, посвященном преднамеренным электромагнитным воздействиям, также сообщалось о практических экспериментах в этой области, выполненных в России. Оборудование для проведения таких исследований имеется во многих организациях, причем, в последнее время оно предлагается в аренду всем желающим. Например, подробную информацию об одном из таких испытательных стендов можно найти на Интернет сайте Истринского филиала ВЭИ им. Ленина.

Воздействие мощного электромагнитного излучения или импульса на электронную аппаратуру приводит к появлению в ее цепях очень высоких напряжений (киловольты) и протеканию больших токов, вызывающих взрывообразное термическое разрушение электронных компонентов или электрической пробой тончайших диэлектрических пленок и электронных переходов внутри полупроводниковых элементов. Провода высоковольтных электрических сетей представляют собой огромные антенны, обсорбирующие высокочастотное излучение и обеспечивающие его транспортировку через системы трансформации непосредственно к электронным и микропроцессорным реле защиты, а от них к системам передачи данных и т.д. В этой ситуации экранирование проводов, идущих от трансформаторов тока и напряжения к реле ничего не дает так как помеха проходит внутри экранированного кабеля. Размещение высокочувствительной аппаратуры в стандартных металлических шкафах также малоэффективно, так как высокочастотное излучение способно проникать даже сквозь небольшие вырезы и даже щели в таких шкафах. Низковольтная распределительная сеть 220 В также является по-сути огромной антенной, принимающей и доставляющей разрушительное излучение через цепи питания электронной аппаратуры. Телефонные линии, часто используемые в качестве каналов передачи данных в электроэнергетике – еще один канал для электромагнитной интервенции.

В такой ситуации, конечно, трудно найти универсальное средство, способное обеспечить стопроцентную защиту. Однако, имеется достаточно много средств, обеспечивающих существенное ослабление воздействия мощного высокочастотного излучения на электронную аппаратуру [9]. Во-первых, в области специальных средств связи уже давно используются специальные устройства, предотвращающие излучение высокочастотных сигналов с компьютеров и средств связи в эфир и в питающие сети с целью предотвращения утечки важной информации. В этих же системах связи для полной гальванического отделения от сетей питания 220 В используется агрегат мотор-генератор с диэлектрическим валом, соединяющим мотор с генератором. Такого же рода технические решения могут быть использованы и для защиты электронной аппаратуры от проникновения в нее высокочастотных излучений извне. На рынке электроэнергетического оборудования в последние годы появились оптические трансформаторы тока и напряжения [10], выпускаемые на все классы напряжений, например, трансформаторы Канадской фирмы NxtPhase (www.nxtphase.com), которые в совокупности с оптоволоконными линиями вместо электрических проводов способны существенно ослабить влияние мощных электромагнитных излучений. В настоящее время на

Западе бурно развивается целая индустрия направленная на производство силовых высокочастотных фильтров разных размеров и мощностей, промышленных элементов защиты от перенапряжений и комбинированных устройств, сочетающих в себе высокоэффективные фильтры с быстродействующими разрядниками. Выпускаются специальные металлические шкафы, обеспечивающие полную защиту от высокочастотных излучений, выпускаются также и специальные электропроводные резиновые прокладки и электропроводные смазки для повышения степени защищенности обычных металлических шкафов.

Наряду со специальными мерами, которые необходимо предпринять для обеспечения надлежащей безопасности в электроэнергетике, существуют и давно известные и тривиальные методы, например такие, как уменьшение импеданса цепей заземления, особенно на высоких частотах; более взвешенный и осторожный подход к вопросу о замене старых электромеханических реле защиты новыми микропроцессорными.

Учитывая значительную степень опасности с одной стороны и легкодоступность специального оборудования для электромагнитных террористических атак – с другой стороны, в спецслужбах многих стран созданы специальные подразделения для противодействия таким атакам. В США это проблемой занимается целый ряд правительственных организаций, включая специальный отдел в ФБР. После кибер атаки из Ирана, предпринятой в 2003 году на Электрическую Компанию Израиля [7] было создано специальное подразделение в Израильской службе внутренней безопасности SHABAK. Аналогичное подразделение было создано и в Научно-техническом центре "Атлас" при ФСБ России [6]. Однако, по нашему мнению, пришло время создать при Министерстве энергетики общероссийский координационный центр, который бы занялся глубоким изучением специфических проблем электромагнитного терроризма конкретно в электроэнергетике, привлекая к сотрудничеству российских специалистов в области электромагнитного оружия, испытаниями оборудования, организацией производства специальных защитных средств, разработкой технических требований и специальных рекомендаций для электростанций и подстанций. Учитывая темпы развития техники электромагнитного оружия и его доступность, такой центр должен быть создан незамедлительно, времени ни "раскачку" уже не осталось.

ЛИТЕРАТУРА

1. Gurevich V. Electromagnetic Terrorism: New Hazards. – Electrical Engineering and Electromechanics, N 4, 2005.
2. A. B. Prishchepenko, V. V. Kiseljov, and I. S. Kudimov, "Radio frequency weapon at the future battlefield", Electromagnetic environment and consequences, Proceedings of the EUROEM94, Bordeaux, France, May 30-June 3, 1994, part 1, p. 266-271.
3. Кадуков А.Е., Разумов А.В. Основы технического и оперативно-тактического применения электромагнитного оружия. Петербургский журнал электроники, вып. 2, 2000.
4. Россия выставляет на рынок оружие будущего. Газета "Независимое военное обозрение" N 39 (261), 19 – 25 октября 2001.
5. Прищипенко А. Новый вызов террористов – электромагнитный. Газета "Независимое военное обозрение", 05.11. 2004.
6. Богданов В. Н., Жуковский М. И., Сафронов Н. Б. Электромагнитный терроризм – состояние проблемы. Доклад представлен Научно-техническим центром "Атлас" ФСБ России. Материалы конференции "Информационная безопасность регионов России – 2005", С. Петербург, 14 -16 июня 2005 г.
7. Gurevich V. The Hazards of Electromagnetic Terrorism. – Public Utilities Fortnightly, June 2005.
8. Douglas J., Grid Security in the 21 Century. – EPRI Journal, Summer 2005, pp. 27-33.
9. Рябов Ю. Г. Общие положения по сохранению живучести и обеспечению защиты радиоэлектронных средств от воздействия электромагнитного оружия и электронного терроризма – "Специальная техника" N 3, 2002.
10. Design Options Using Optical Current and Voltage Transducers in a High Voltage Substation. IEEE PES Substation Committee Annual Meeting, May 1, 2000.