

УДК 621.316

**SMART GRID: NEW PROSPECTS OR NEW PROBLEMS? (Part 2)<sup>1</sup>****V. Gurevich***Ph. D., Honorable professor Central Electric Laboratory, Israel Electric Corp.,  
e-mail: vladimir.gurevich@gmx.net*

*In the paper observed modern conception for future electrical grid building in Russia and in West countries and disclosed hazards accompanying transition to Smart Grid.*

*Key words: smart grid, electrical grid, relay protection, reliability, intentional destructive electromagnetic impacts.*

**3. Smart Grid: panacea or the road to hell?**

As it turned out in the previous chapter, Smart Grid is a concept associated with the global reconstruction of the whole power supply system. It is obvious that implementation of such a global program demands enormous investments. Thus it is logical to ask: how, in fact, it will benefit us? What economic returns can we expect from these investments? Unfortunately, none of the numerous publications describing the advantages of Smart Grid, as we found out, gives any business case for the realization of the Smart Grid concept.

Doesn't the existing structure of electrical networks provide a steady electrical supply for consumers? Aren't the microprocessor-based electric power meters more widely applicable beyond this concept? Does the development of modern microprocessor-based automated diagnostics systems suffer from the lack of the Smart Grid? Aren't modern MPDs capable of meeting all current challenges of relays? Certainly, the radical change of network configuration and appearance of numerous power sources in a network can change functions and algorithms of relay protection dramatically. However, how can national-wide electrical network structures which have developed for decades change so fundamentally in rather practical than theoretical ways? And what for? As for a large number of small power generating sources (wind generators, solar batteries) which the Smart Grid apologists expect to be included in the future general electrical network, such developments are doubtful. As we saw in many European countries (Italy, Netherlands, Germany, Spain, etc.) wind generators or solar batteries were not used (as power network entities) as single network power units (except of the individual devices powering separate facilities). The common practice is to combine them in

the large power units occupying huge areas (see Fig. 1) and connected to grids. For example, the capacity of the Thanet wind generator located at southeast coast of Kent county in Great Britain and consisting of 100 wind turbines (the planned number is 340) is 300 MW.

Available microprocessor-based automatic operation systems successfully manage such large power installations and synchronize them with the networks without any "Smart Grid". Besides, as we know, the wind-power industry is not all that profitable. According to the experts of the British Energy Research Centre, the energy produced at the coastal wind power stations is approximately 90% more expensive than the energy produced from traditional fuel sources and 50% more expensive than the energy produced from nuclear fuel.

On the other hand, if we consider the Smart Grid concept as a fundamental reconstruction of electrical grids resulting in the significant sophistication of their structures and operations, we should be aware of the predictability of such modes and the ability to determine who should calculate relay protection set points and how for such complicated networks. Another point is to what extent the set points will be able to reflect the actual grid emergency modes. We expect that both due to the complexity of the network and a high number of cross-coupled active components, it will be a real challenge to find the reason a failure occurred, even using the self-diagnostics devices. It will require modeling of network operation modes along with considerable research. Compared to the existing grids we assume that such networks will be much more difficult to operate and require far more skilled staff. The "one-and-all" computing process covered by the Smart Grid concept is already in full play both in industry and energetics.

Часть 1 статьи опубликована в № 1 2011 г.



Fig. 4. Modern Solar (Photo-Electric) and Wind Generator Stations

The absolutely outrageous willingness to integrate all kinds of power equipment with the computer network and all-round and to move from the old reliable analogue electronics to digital microprocessor-based units very often results in catastrophic consequences [24].

Relay protection is another issue. Within the Smart Grid the following are the expected developments:

- Concentrating more functions within single microprocessor module;
- Combining relay protection with power equipment monitoring and diagnostics functions;
- Applying fuzzy logic algorithms, proactive functions, artificial intellect, neuron nets, etc.

As shown [25–28] the reliability of MPDs lower than the reliability of electromechanical relays even today. However, it doesn't mean that it is necessary to slow down the transition from EM relays to MPDs. Rather it sets a serious challenge to be resolved. Some lines of attack on the problem have been proposed by the author [29–32]. In a few words they can be combined as follows:

- Do not flood the MPD with the functions beyond relay protection such as monitoring of electric equipment;
- Limit the number of functions in a single microprocessor terminal; optimize this number not only by relaying cost, but also by its reliability;
- Refuse the fuzzy logic algorithms providing relay protection unpredictability;
- Simplify the program interface as far as possible based on some unified MPD software platform;
- Leading manufacturers of computer-based test equipment for MPD should develop a set of programs fully compatible with the unified MPD software platform and allowing complete automation of MPD testing to minimize human errors;
- Develop new MPD design principles based on universal interchangeable functional modules such as PCs; create the market of universal functional MPD modules;
- Carry out special research and development efforts for ensuring required functionality of relay protection under malicious destructive electromagnetic impacts, for example, by improving MPD sustainability against such actions or by providing a redundant emergency set of electromechanical RPs.

As you can see, the above principles are opposite to the trends of the Smart Grid concept. What does this mean? It means that implementation of the con-

cept will lead to a critical decline in the reliability of relay protection.

The feasibility of replacing all conventional current and voltage transformers with digital output optoelectronic devices (according to the Smart Grid) is also not assured both from economical and technical points, as we discussed previously [33].

In a word, the advantages of the comprehensive implementation of the Smart Grid concept are not that obvious as its apologists declare. At the very least, no one has proved its economic feasibility yet. On the other hand, the separate projects with proven economic efficiency are actively realized without any connection to the global concept of the Smart Grid.

It looks even more doubtful when considering some of the not so pleasant facts which passionate supporters of the Smart Grid usually never mention.

This is about the vulnerability of the Smart Grid against hacker attacks. In fact, if all elements of the Smart Grid are to be controlled by commands through the networks with TCP/IP protocols, there is an enormous potential danger of external intervention to the power system operation. Many experts emphasize this hazard [34 - 55] devoting international conferences [56] to it. Only apologists of the Smart Grid "do not notice" these problems. What do we hear from apologists of the Smart Grid? Nothing, we hear only the usual reservations about the necessity to isolate the internal network of the Smart Grid from the external Web, about access passwords and other trivial safety measures. We all understand that all these measures can limit access for normal people, but not for experienced hackers cracking even the very well protected networks of the Ministries of Defense and banks.

However, hackers are not the major concerns since the armies of many countries of the world have special divisions consisting of skilled professionals trained for cyber wars, that is, for cracking and sabotaging the protected computer networks of the enemy. It is safe to say that computer networks of the Smart Grid will be the target number one for such divisions. "Welcome to the Twenty First century war," says Richard Clark, former adviser of former US president George Bush for cyber safety, "Imagine the bursting of electric generators, the derailing of trains, the crashing of planes, the blowing up of gas pipelines, the arms systems suddenly ceasing to work, and armies not knowing where to move". It is not an episode from the next Hollywood blockbuster, it is a summary of consequences of such a new type of

battle as cyber war by skilled American experts [57]. The current Head of Cyber command of the Pentagon and the Chief of National Security Agency (NSA), General Alexander at hearings of Military Service Committee of House of the USA has declared that the effect of the cyber weapon is comparable to the effect of a mass destruction weapon. Additionally, one of the former employees of NSA, Charles Miller, has even calculated that the arrangement of the cyber structure capable of successfully attacking and completely paralyzing the USA costs only 98 million dollars [57]. "We consider it as one of the basic directions for the future and expect a double growth of the market totaling billions of dollars," emphasized Stephen Hokins, vice-president of intelligence and information systems division of Raytheon. It is worth the effort as the cyber budget reached 8 billion USD this year, and in 2014 this amount will grow to 12 billion USD. While the annual budget increase expected for other directions will come to 3 - 4%, in the short term this rate for cyber safety will grow at least 8% annually. The leading role in this new type of war will belong to military men, and naturally they will receive the lion's share of the cyber budget: more than 50% out of 8 billion dollars in 2010 will be given to the Pentagon. "According to the experts, the cyber weapon is developing with great speed. Many countries - including the USA, Russia, China, Israel, Great Britain, Pakistan, India, Northern and South Korea - have developed sophisticated cyber weapons which can get into computer networks and are capable of destroying them," write Shivon Gorman and Stephen Fidler, authors of the article [58]. Some representatives of the American intelligence and analytics are afraid that the cyber weapon can fall into the hands of terrorists. "The question is when will "al Qaeda" get it?" says James Lewis, the expert in cyber safety of the CSIS [58].

One of the directions of the new type of war is the creation of a special virus that seizes computer networks and resembles the Win32/Stuxnet virus which defeated protected computer networks of the nuclear power program of Iran in September 2010. Win32/Stuxnet poses a threat to the industrial enterprises. During start up this malicious program employs the previously unknown vulnerability of USB-stick LNK-files. Execution of the malicious code results from the vulnerability of the Windows Shell related to the display of dedicated LNK-files. The new distribution method may open the door to other vicious programs which will use the same route since the vulnerability still exists [59]. Win32/Stuxnet can also bypass HIPS (Host Intrusion Prevention System) protecting the systems from external impacts as this malicious program contains files with legal signatures. Now this virus makes several thousands attacks per day on the computers with Siemens installations [60]. According to experts the attacks are directed to sophisticated systems such as automatic programs operating whole plants, and municipal infrastructure units, including public water supplies. The [60] publishes comments of analysts who consider

the attacks to Siemens devices as the first occurrence of mass "industrial sabotage". The complex analysis performed by experts of Symantec showed that Stuxnet is an extremely dangerous and complex threat to the safety of the computer systems and is focused on the infection of industrial equipment monitoring systems which are also widely used at electric power stations. By changing the programmable logic controllers (PLC) code the virus attempts to reprogram the industrial control systems (ICS) in order to take over the control without operators being aware. The complexity of the virus and its extremely high selectivity testify that this malicious program was created by a group of the highly skilled experts possessing the huge budget and integration capabilities rather than by some self-taught hacker [57]. After analysis of the code of a worm, the experts of Kaspersky's Laboratory concluded that the Stuxnet "was not intended for espionage on the infected systems, it was developed for sabotage". "Stuxnet does not steal money, confidential information or send spam," Evgenie Kaspersky confirms, "this thread is created to control productions, and literally to take over the operation of the production capacities. Quite recently we have struggled with cyber criminals and Internet hooligans, but now, I am afraid, the time has come of cyber terrorism, the cyber weapon and cyber wars" [57].

Recent developments in the field of deliberate destructive electromagnetic impacts on the electronic equipment represent at least a hazard for the Smart Grid, as described earlier [61].

Background. In 1928 physicist Arthur Compton (USA) theoretically predicted that the adverse factor of nuclear explosion is represented by electromagnetic pulse. The test explosion of the first hydrogen bomb over the Pacific Ocean proved the Compton's effect in 1958. The explosion was followed by such unexpected complications, observed hundreds miles from the explosion point, like street lights in Hawaii went out; failure of radio navigation systems in Australia and faults in radio communication system in many other regions. This was where Compton was recalled. That caused panic: it turned out that a powerful stream of electrons generates such a high electromagnetic pulse that it can cause electric and electronic devices located at great distances out to stop operating. Therefore, it can be used as a separate kind of weapon! Obviously the history of electromagnetic weapons began at that moment [62].

The first theoretical ideas about the nonnuclear shockwave **super-powerful pulse generators** (SPG) were described by Andrei Sakharov, the member of the Soviet Union Academy of Sciences, during his research of nuclear fusion reactions in the early 50s of the last century [63]. In the 60s not only scientists but also politicians of the USSR understood that this source of super-power electromagnetic pulses could be the basis for creating a new type of weapon. This was revealed in addresses of N.S. Khrushchev in the 60s where he referred to some "fantastic weapons". Certainly, it took some time to

create new weapons based on purely theoretical studies. The first report about SPG, as independent weapon generating super-powerful electromagnetic pulses, was officially announced by the Soviet scientist A.B. Prischepenko after successful tests were made on March 2, 1984 at the weapon range of Krasnoarmeisky Research Institute "Geodesiya" in Moscow region (now Federal Research Center "Geodesiya"). Later, A.B. Prischepenko formulated general principles for combat use of electromagnetic weapons. According to published data, this pulse lasts tens or hundreds of microseconds, while the amplitudes of the emerging current reach tens of millions of amperes. Just to compare: the strength of lightning current during a storm discharge usually does not exceed 20 - 30 thousand amperes and very rarely it can reach 100 thousand Amps.

According to [64] in the 80s the Soviet Union has repeatedly conducted experiments with electromagnetic weapons in space, which resulted in the numerous faults of power systems. About twenty years ago the author of this book attended the advance defense of doctoral thesis on the theoretical aspects of the transfer of energy from the space super-high-frequency source to the Earth. In those years, the USSR simultaneously conducted experiments on generating super-power electric discharges (which were the powerful sources of electromagnetic emission). Many American newspapers and magazines of that time reported about unusually powerful electric discharges over the territory of the USSR, which had never been seen before, and at zero storm activity. Some 25 years ago, the author of this book personally saw a picture of a super-long horizontal discharge between two towers above the houses of one village.

In the years of perestroika, Russian scientists A. Prischipenko, V. Kiselev and S. Kadimov informed the world society about a new type of weapon developed in the USSR in commemoration of the new era of relations with Western countries. Their report presented at the International Conference in France [65] was entitled "Radio frequency weapons at future battlefield".

That report created a furor and became public domain. Thereafter, other reports on achievements of Russian scientists in this area appeared in the print [66 - 68]. Today, the issues on electromagnetic war and terrorism are freely discussed in the press, and at foreign and Russian scientific conferences [69, 70].

The first experiments on nuclear explosions in the atmosphere were not forgotten as well. Recent studies have shown that a nuclear explosion set off in near space (at the altitude of 200 - 300 km) would hardly be noticed by the population of the territory over which it was set off.

However, all life support systems (power system, water supply, telecommunications, communi-

cation, etc.) would all be put out of operation within a few moments. For this purpose there are special IEC standards (see e.g. [71]), which detail the methodology for testing the steadiness of electric network equipment to high-altitude electromagnetic pulse (HEMP). Special mobile simulators generating pulses similar to those that are induced in power lines wires under HEMP were designed for such testing.

According to data cited in this document, the overvoltage in dead power lines under HEMP becomes so high that it causes a breakdown of even the linear insulators of 35 kV class and, naturally, of all lower class insulators. If the same pulse penetrates the live power line, even 110 kV insulators are broken-down.

Thus, there is no need to say what happens with all the rest of equipment that has direct, inductive or capacitive couplings with power line wires.

There is no need to have any special imagination to imagine how one can put mobile generators, weighing 300 - 400 kg, Fig. 5, in a light truck or a van with a plastic body in order to affect the electronic equipment of substations and power plants, computer centers, mission control centers, etc. from a certain distance.

Several pulses of such emissive power will be enough to burn out all electronic devices, including the DPRs, of course. According to some reports, it damages even electronics that are switched off at the moment of action. Surely, many countries work on the same issues, including Israel, China, India and Iran. In the U.S., for example, this field is intensively researched by such big corporations as TWR, Raytheon, Lockheed Martin, Los Alamos National Laboratory, Air Force Research Laboratory (Kirtland Air Force Base, New Mexico), as well as by many civic organizations and universities. In Germany, Rheinmetall Weapons and Munitions has been leading in this field for many years. In particular, the Americans have developed generators of powerful electromagnetic pulses working under different principles (fig. 6).

The main channels of destructive force impact on the following electronic equipment: power lines of all voltage classes, control cables and wire communication lines, air. Since DPR is connected to external power lines, branched network of control cables and wires, power line antenna-cables (by VT and CT) and computer network, the destructive effect on them can be both very high and at the same time hidden.

The reticence of electromagnetic attack is increased by the fact that the analysis of damage in the destroyed equipment does not allow identifying the cause of damage, since the same damage can be a result of either intentional (attack) or unintentional (e.g., lightning induction) destructive forces. This circumstance allows an attacker to use this technique repeatedly with success.

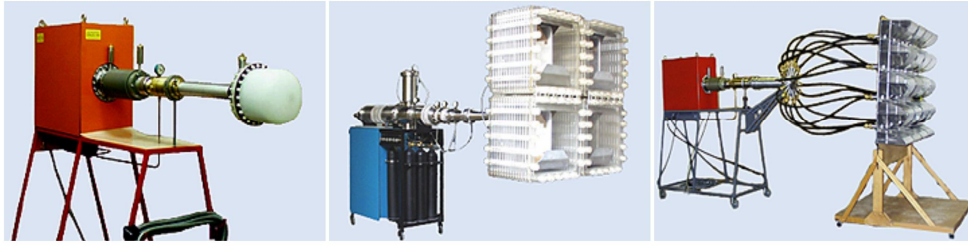


Fig. 5. Super-power ultra-broadband pulse oscillators of directed super-high-frequency electromagnetic emission of IHCE SB RAS with output power up to 1 billion Watts, which is consistent with the capacity of nuclear power plant unit.



Fig. 6. Left - a super-power mobile high-voltage pulse generator FEBETRON-2020. Output voltage is 2.3 million Volts, the output current is 6000 Amps. In the center - a powerful microwave generator mounted on the car. Right – a transportable powerful microwave generator.

High-frequency sources of high-power emission, operating in the centimeter and millimeter range, have an additional mechanism for the penetration of energy into equipment through so-called "back doors", i.e., even through small holes, openings, windows and cracks in metal housings and through poorly shielded interfaces. Any hole that leads inside the equipment acts as a crack in the microwave cavity, allowing microwave emission to form an extensional standing wave inside the equipment. The components located at opposite assemblies of the standing wave will be exposed to strong electromagnetic fields and overvoltage. Memory elements and modern highly-integrated microprocessors are especially sensitive to this kind of impacts.

Thus, it is clear that it is not that easy to protect ourselves from all these "troubles". And even such well-known noise-resistant technology, like optical fiber, is prone (it may seem strange) to the impact of powerful electromagnetic pulses. First, optical fiber lines are equipped with microelectronic-based and even microprocessor-based terminals designed to convert electric signals into light and vice versa. Second, it is known that light polarization vector in optical fiber can be changed under external magnetic field (strictly speaking, this is a basic principle for magneto-optical current transformers available in the market today).

Due to this, the signals of relay protection systems and communications transmitted by optical fiber, built in a power line wire (a very common technology today) will be subjected to distortions under high pulse currents flowing through the same wires and creating pulsed magnetic fields.

The author was shocked that not only ordinary power energy specialists, but also managers do not

have even minimal knowledge on this topic. Moreover, the author's attempts to raise this topic in articles and on relay protection forums lead to mockery and "pooh-poohing" towards him.

The basic channels for force destructive impacts on electronic equipment are the power supply lines of all voltage classes, control cables, wire communications, computer networks, and the airways. Since within the Smart Grid the microprocessor equipment is connected to the external power grid, distributed control cables, power line antenna-cables (through the voltage and current transformers) as well as to the computer network, the destructive impact may be both very high and hidden. The concealment of an electromagnetic attack significantly rises considering the fact that the analysis of damages to the destroyed equipment does not allow unequivocally identifying the reason of such damage as the same damages can be intentional (attack) or inadvertent (for example, a lightning bolt). This circumstance allows malefactors to use this technology successfully and repeatedly.

Microwave sources of intense radiation in centimeter- and millimeter range provide additional mechanisms for penetration of energy into the equipment "through a back door", such as small apertures, cuts, windows and gaps in metal cases, or through poorly shielded interfaces. Any aperture penetrating into the equipment acts as crack in a microwave cavity allowing microwave radiation to form a spatial standing wave inside the equipment. The components located in opposite nodes of a standing wave will be exposed to a high electromagnetic field and overvoltage. Memory elements and modern microprocessors with very high-scale of internal component integration are especially exposed to such impacts.

So, it becomes clear that the protection against such "misfortunes" is a challenge. And, amazingly, even such known noise-proof technologies as fiber-optics are exposed to powerful electromagnetic impulses. First, fiber-optic lines have terminations consisting of microelectronic components and even microprocessors which are designed for converting an electric signal into light and back. Second, the vector of light polarization in optical fiber can change under the external magnetic field (as a matter of fact, this principle is used in magneto-optical current transformers available on the market). This means that signals of relaying and communications transferred through the optical fiber built in HV power lines (this technology is prevailing today) will be exposed to distortions as high-pulse currents producing pulsed magnet fields flow thorough the lines.

It should be emphasized that some years ago mass media were reluctant to publish articles on this subject being afraid to draw attention of terrorists and criminals. However, after the last largest power interruption in the USA terrorists realized the dependency of a modern Western civilization on electric power industry and declared that in a number of the statements and threats. Subsequent squall of articles in New York Times and other prints was devoted to the vulnerability of critical vital service systems to electromagnetic terrorism. For example, in [75] it is explicitly stated that the electric power systems are the major target for terrorist attacks today. Therefore, the carelessness of management and personnel of electric power system entities acting like an ostrich for many years seems amazing. Isn't it a crime of carelessness to neglect a large number of articles on this subject published in special technical literature, in the press, on the Internet and in books, Fig. 7 [76–80]?



Fig. 7. Some books devoted to deliberate destructive electromagnetic impacts published in Russia

The author has been simply shocked by a total ignorance of this problem not only by "shop floor" power engineers, but also by executives. Moreover, attempts to discuss this subject in articles

and on forums on relay protection lead only to sneers and scornful snorting.

Both the concept of the Smart Grid providing the widest application of microprocessor devices in all elements of electric power systems and the tendency toward increasing the density of elements in microchips (accompanied by a decrease in their sustainability to external electromagnetic impacts) combined with advancements in the field of remote destructive means form a very dangerous vector. And the "ostrich" policy of unwillingness to know and realize potential hazards has never led to good...

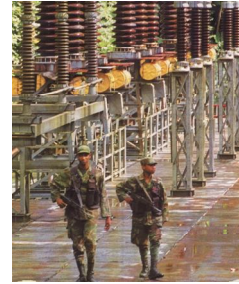


Fig. 8. Is the Smart Grid our future?

All these are the realities of today while full practical implementation of the concept of the Smart Grid is still very far away. But what will happen if this concept is developed and implemented? Even today it is safe to say that full implementation of the Smart Grid concept will boost the vulnerability of electric power systems and decrease their sustainability. If before it was a question of MPD problems [81], the concept of the Smart Grid will give a boost to these problems making them more global and dangerous, Fig. 8.

#### So what the Smart Grid really is?

In our opinion, the Smart Grid is a global publicity campaign juicy for hundreds of manufacturers, research centers and universities. The purpose of it is to promote numerous products, technologies and researches compulsorily "attached" to the popular term of "Smart Grid" and "wheelde" enormous investments out of the state budgets [82] to develop and manufacture products and systems under the devastatingly extended term of "Smart Grid". As for apologists of the Smart Grid, it seems like their financial interests prevail over the sensible doubts and fears concerning the dangers resulted from the full implementation of the concept. Neglecting these hazards can lead to global international catastrophes.

Moreover, the normal growth of technology will not be slowed down if the concept isn't implemented. It will only be sounder, more rational and more careful.

#### References

24. Gurevich, V.I. Price for «the progress» // Components and Technologies. – 2009. – N 8. – P. 112–118.
25. Gurevich, V. Reliability of Microprocessor-Based Relay Protection Devices: Myths and Reality // Engineer IT. Part I. – 2008. – N 5. – P. 55–59; Part II: 2008. – N 7. – P. 56–60.

26. Gurevich, V.I. Reliability of Microprocessor-Based Protective Devices – Revisited // Journal of ELECTRICAL ENGINEERING. – 2009. – Vol. 60, N 5.
27. Gurevich, V.I. Problems with Evaluation of the Reliability of Relay Protection // Electrotechn. Complexes and Control Systems. – 2010. – N 3. – P. 56–59.
28. Gurevich, V.I. How to Rebuild Relaying? // Energize. – 2010. – N 4. – P. 36–39.
29. Gurevich, V.I. The New Concept of Digital Protective Relays Design // Serbian Journal of Electr. Engineering. – 2010. – Vol. 7, N 1. – P. 143–151.
30. Gurevich, V. Sophistication of Relay Protection: Good Intentions or the Road to Hell? // Energize. – 2010. – Jan/Feb. – P. 44–46.
31. Gurevich, V.I. The New Concept of Digital Protective Relays Design // Serbian Journal of Electr. Engineering. – 2010. – Vol. 7, N 1. – P. 143–151.
32. Gurevich, V. The New Way in Digital Protective Relays Designing // Electrotechn. Complexes and Control Systems. – 2010. – N 1. – P. 34–37.
33. Gurevich, V.I. Optical-Electronic Instrumental Transformers: Panacea or the Partial Solution for the Partial Problems // Electric Power's News. – 2010. – N 2. – P. 24–28.
34. Robertson, J. Security experts offer caution on Smart Grid // Associated Press. – 2009. – July 31.
35. Krebs, B. «Smart Grid» raises security concerns // The Washington Post. – 2009. – July 28.
36. Slocum, Z. Report: Smart-grid hackers could cause blackouts // Cnet. News. – 2009. – March 21. – URL: [http://news.cnet.com/8301-1009\\_3-10201651-83.html](http://news.cnet.com/8301-1009_3-10201651-83.html).
37. Baldor, L.C. New threat: Hackers look to take over power plants // Associated Press. – 2010. – April 8.
38. Nakashima, E. Defense official discloses cyberattack // The Washington Post. – 2010. – August 25.
39. Gorman, S. U.S. Plans Cyber Shield for Utilities, Companies // The Wall Street Journal. – 2010. – July 8.
40. Lemos, R. Hacking the Smart Grid // Technology Review. – 2010. – April 05.
41. Mills, E. Experts warn of catastrophe from cyberattacks // InSecurity Complex. – 2010. – February 23.
42. Aitoro, J.R. Energy set to form new group to protect electric grid from cyberattacks // NextGov. – 2010. – May 01.
43. Barret, L. U.S. Reviewing Cyber Threat to Power Grid // Internet News. – 2009. – September 15. – URL: <http://www.internetnews.com/security/article.php/3839241>.
44. Hamilton, T. Smart grid saves power, but can it thwart hackers? // TheStar.com. – 2009. – August 03. – URL: <http://www.thestar.com/printArticle/675453>.
45. Gross, G. Lawmakers: Electric utilities ignore cyber warnings // Computerworld. – 2009. – July 21.
46. [http://www.computerworld.com/s/article/print/9135753/Lawmakers\\_Electric\\_utilities\\_ignore\\_cyber\\_warnings](http://www.computerworld.com/s/article/print/9135753/Lawmakers_Electric_utilities_ignore_cyber_warnings).
47. Gorman, S. Electricity Industry to Scan Grid for Spies // Wall street Journal. – 2009. – June 18.
48. Miller, S.C. Our infrastructure in their crosshairs // The News & Observer. – 2009. – May 12.
49. Smart Grid offers savings, vulnerabilities // HS Daily Wire. – 2009. – April 30.
50. Critics: Cybersecurity standards for grid do not go far enough HS // Daily Wire. – 2009. – May 01.
51. Sarwate, A. Hot or Not: SCADA security is hot // SC Magazine US. – 2009. – April 23.
52. Mills, E. Just how vulnerable is the electrical grid? // CNET. News. – 2009. – April 10.
53. Meserve, J. «Smart Grid» may be vulnerable to hackers // CNN. Com. – URL: <http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html>.
54. Madrigal, A. Report: A Smart Grid Is a Hackable Grid // The Atlantic. com. – 2010. – October 7. – URL: <http://www.theatlantic.com/technology/archive/2010/10/report-a-smart-grid-is-a-hackable-grid/64231/>.
55. Half of critical infrastructure providers have experienced perceived politically motivated cyber attack // Transmission & Distribution World. – 2010. – October 6.
56. Preventing Catastrophic Impacts from Adverse Cyber-Physical Events // CISW-SG 2010 Smart Grid Survivability Workshop. – Arlington, Virginia USA. – 2010. – October 13-14.
57. Scherbakov, V. Cyberspace – real war // Voенно-promyshlennyi curier. – 13.10.2010. – N 40 (356).
58. Gorman, S., Fidler, S. Cyber Attacks Test Pentagon, Allies and Foes // Wall Street Journal. – 2010. – September 25.
59. Kriakvina, Y. ESET warns about attack of worm Win32/Stuxnet. 19.07.2010. – URL: <http://www.ixbt.com/news/soft/index.shtml?13/54/55>.
60. Computer systems of Siemens became the target for the first global attempt of industrial sabotage. London, July, 22nd, PRIME-TASS. – URL: <http://www.prime-tass.ru/news/0 / % 7BA89148AF-A72E-49C4-86BC-5D6D8598E340%7D.uif>
61. Gurevich, V.I. Problems of Electromagnetic Impacts on Digital Protective Relays // Components and Technologies. – 2010. – N 2. – P. 60–64 ; N 3. – P. 91–96 ; N 4. – P. 46–51.

62. Gurevich, V.I. Electromagnetic terrorism – The New Reality of The 21<sup>st</sup> Century // The World of Technics and Technologies. – 2005. – N 12. – P. 14–15.
63. Sakharov, A.D. Magnetic explosion generators // The Advances in Physical Sciences. – 1966. Issue. 4. – Vol. 83, 84.
64. The Shocking History of Soviet Russia's Electromagnetic (EM) War Attacks on the United States. – URL: <http://www.bayside.org/news8/sovietelectromagneticattacksonunitedstates.htm>.
65. Prishchepenko, A.B., Kiseljov, V.V. and Kudimov, I.S. Radio frequency weapon at the future battle-field // Electromagnetic environment and consequences, Proceedings of the EUROEM94, Bordeaux, France, May 30 – June 3, 1994. – Part 1. – P. 266–271.
66. Kadukov, A.E., Razumov, A.V. The Basics of Technical and Prestrategic Application of Electromagnetic weapon // The Journal of Electronics of St.-Petersburg. – 2000. – issue 2.
67. Russia Markets the Weapon of Future // Independent Military Review. – 2001. – N 39 (261), October 19–25.
68. Prishchepenko, A.A. New Challenge of Terrorists – Electromagnetic // Independent Military Review. – 2004. – November 5.
69. Bogdanov, V.N., Zhukovskiy, M.I., Safronov, N.B. The Electromagnetic Terrorism – the State of the Problem : presented by the Scientific and Technical center «Atlas» of FSS of Russia // Proceedings of the Conference «Informational Safety of Regions in Russia – 2005», St.-Petersburg, June 14–16, 2005.
70. Daamen, D. Avant-garde Terrorism: Intentional Electro Magnetic Interference. On Methods and Their Possible Impact // Report. Spring. – 2002.
71. IEC/TR 61000-1-3 Electromagnetic compatibility (EMC) – Part 1–3: General – The effects of high-altitude EPM (HEMP) on civil equipment and systems.
72. Explosion Generators of Powerful Electric Current Impulses / Edited by V.E. Fortov. — M. : Science, 2002.
73. Mesyats, G.A. Generation of Powerful Nanosecond Impulses. — M. : Sov. radio, 1973 ; Trimble S. Boeing, Raytheon win work on high power microwave missile // Flight International. – 24.09.2010.
74. Trimble, S. Boeing, Raytheon win work on high power microwave missile // Flight International. – 24.09.2010.
75. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. – URL: [http://www.empcommission.org/docs/empc\\_exec\\_rpt.pdf](http://www.empcommission.org/docs/empc_exec_rpt.pdf).
76. Prishchepenko, A.B. The Explosions and Waves. Explosion sources of Electromagnetic Radiation of Radio Frequency Range // Course Book for 170103 Department Means of Defeat and Ammunition.
77. Prishchepenko, A.B. The weapon of Unique Possibilities // Independent Military Review. – 1998. – N 26. – July 17–23.
78. Gannota, A. The object of defeat – electronics // Independent military review. – 2001. – N 13.
79. Electromagnetic Terrorism at the Edge of Centuries / edited by T.R. Gazizova. – Tomsk : Tomsk State University, 2002.
80. Radio-Electronic Struggle: Forced Defeat of Radio-Electronic Systems / V.D. Dobrykin, A.I. Kupriyanov, V.G. Ponomaryov, L.N. Shustov. – M. : Vuzovskaya Kniga, 2007.
81. Problems of the Digital Protective Relays (<http://digital-relay-problems.tripod.com/>).
82. Sonenklar, C. Obama admin tabs \$3 billion for Smart Grid. – URL: <http://www.heatingoil.com/blog/obama-admin-tabs-3-billion-for-smart-grid-1028/>.

**«ИНТЕЛЛЕКТУАЛЬНЫЕ СЕТИ»: НОВЫЕ ПЕРСПЕКТИВЫ  
ИЛИ НОВЫЕ ПРОБЛЕМЫ? (Часть 2)**

**В.И. Гуревич**

*В статье рассматривается современная концепция построения будущих электрических сетей в России и на Западе и вскрываются опасности, сопровождающие переход к так называемым «интеллектуальным сетям».*

*Ключевые слова: интеллектуальная сеть, электрическая сеть, релейная защита, надежность, преднамеренные деструктивные электромагнитные воздействия.*