



## Project Proposal

**Title of the project proposal:** Analysis of immunity of technical systems and devices to ultrashort ultra-wideband electromagnetic pulses (UWB EMP) and development of methods for protection against their effects

**Significance of the project:** Widespread computerization and digitization, saturation of equipment of all kinds and purposes with electronics, as well as the dynamic evolution of generations of cellular (mobile) communications from the second (2G) and third (3G) generations to the fourth (4G LTE), and then to the planned fifth (5G) and the sixth (6G) generations - these are inevitable processes due to the highest efficiency of radio electronic technique and systems in all spheres of human activity - both in everyday life and in industry, utilities, trade, healthcare, education, transport, etc., and also, certainly in the areas of public administration, law enforcement, protection from emergencies and defense.

However, with all the attractiveness of the increasingly widespread use of computer systems for information collecting, storing and processing, of technological process control systems, of systems for public wireless information services and all other systems using electronics, wired and wireless information technologies, it is necessary to take into account their significantly higher susceptibility to the external electromagnetic influences - unintentional and deliberate.

It is especially necessary to reckon with the extremely high dependence of state and local government processes, law enforcement systems, systems of protection against emergencies, etc., on the quality and reliability of the operation of critical objects and control systems - computers and their networks, databases, automated control systems utilities, transportation and other critical systems and facilities. With the implementation of the concepts and technologies of "Smart City", "Smart Home", "Unmanned Transport", "Electronic Health Care" and other information services of modern society, implying an ever-deepening automation of all industrial, technological and management processes, the failure of these systems can have catastrophic consequences and lead to huge losses.

The technological base of modern critical computer systems for information collecting, storing and processing, of controlling technological processes and wireless information services, is the use of micro- and nano electronics. A decrease in the size of the electronic elements while maintaining the size of the connecting elements and an increase in its capacity, leads to an increase in its susceptibility to external electromagnetic influences. Extremely rapid growth in the spatial density of electromagnetic radiation sources (up to 1-10 devices per square meter in 5G/6G systems), data rates over radio channels (up to 1-10 Gbps in 5G/6G systems) and wireless area traffic capacity (up to 1-10 Mbit/m<sup>2</sup> in 5G/6G systems) leads to an extremely significant complication of the electromagnetic environment (EME), an increase in the levels and broadbandness of external electromagnetic exposures, which negatively affects the reliability of the operation of complex information systems.

One of the most dangerous reasons for disrupting the operation of these systems can be their defeat by powerful ultra-wideband electromagnetic pulses (UWB EMP), which are increasingly used in terrorist electromagnetic attacks and in local hybrid military operations within the framework of various coercive actions.

The UWB EMP peculiarities are their extremely high pulse power (intensity) of the electromagnetic field (EMF) at its low average power, as well as the location of the main part of their frequency spectrum in the microwave range, which makes it possible to create compact devices for generating ultra-powerful UWB EMPs capable of ensuring the defeat of unprotected infrastructure objects, individual computers, computer networks and databases, for example, secretly from a car, from a distance of up to 100-200 m.

In modern world, the presence of ever-increasing threats of electromagnetic terrorism and hybrid actions of coercion (aimed at destroying state and local infrastructure in order to disrupt state and local governance) urgently requires the adoption of effective measures to counter these threats.

### **Some test results:**

Analysis and experimental research of the susceptibility of various technical means and objects to the impact of UWB EMP, carried out at BSUIR in 2017-2020, confirmed the high danger of UWB EMP impact on radio electronic means for various purposes. In particular, it was found that

- even at relatively low exposure levels (1 ... 5 kV/m), interference caused by UWB EMP leads to a loss of information data rates in communication channels, which can lead to significant failures in the operation of complex control and monitoring systems;
- for unprotected electronic devices and public equipment (personal computers, laptops, tablets, video cameras, etc.), even low exposure levels can lead to the failure of these devices;
- at levels of UWB EMP exposure above 5 kV/m, the received information is lost and / or distorted for a long time, which often significantly exceeds the time of UWB EMP exposure. This can cause irreversible processes in complex robotic systems controlled by automation, and lead not only to a malfunction in its operation, but also to the failure of executive mechanisms;
- in cases of UWB EMP exposure with a high pulse amplitude (20 kV/m and higher) equipment fails due to irreversible processes in electronic devices and components (thermal breakdown of semiconductor elements such as microcircuits / chips, transistors, diodes) even in protected avionics devices and systems of industrial use;

the impact of UWB EMP on the control systems of complex technological processes with a high probability can lead to their failure, as well as lead to catastrophic consequences.

### **Proposed contents of cooperation:**

Taking into account the above, BSUIR offers the following scientific and technical cooperation in this area:

- joint testing of technical systems and devices for immunity to UWB EMP,
- creation of a database on the immunity of technical means and their elements to UWB EMP,
- research of the physical phenomena that determine the nature of the impact of UWB EMP on radio-electronic equipment,
- development of physical and mathematical models to describe the impact of the UWB EMP on radio-electronic equipment; justification of measures to minimize the results of this impact,
- joint development of methods for protecting radio electronic equipment from the impact of UWB EMP and other types of electromagnetic exposure (CW, HPEM, E1 HEMP, E3 HEMP).

### **Experience and capabilities of BSUIR in this area:**

BSUIR has a metrologically certified mobile complex for testing the equipment immunity to UWB EMP. The complex consists of a radiating antenna, generators of high-voltage pulses, and a field level meter (Fig. 1).

A highly qualified research team has been created in BSUIR. The team has an extensive experience

- in development of practical methods and executing experimental measurements of UWB EMP impact on various technical devices and systems in laboratory and field conditions,
- in theoretical research and mathematical modeling of UWB EMP impact on the means of shielding (protection), including the assessment of the effectiveness of these means.



**Fig. 1. Mobile complex for testing of equipment immunity to UWB EMP**

Nominal amplitude of the pulse at the beginning of the working area on the radiation axis	not less than 50 kV/m
Dimensions of the irradiation zone (with a nominal pulse amplitude and with an inhomogeneity of 3 dB) near the beginning of the working area	1 × 1 m
Duration of the pulse front between levels from 0.1 to 0.9 of the amplitude on the radiation axis	150 ps ± 30 %
Pulse duration at the level of 0.5 of the amplitude on the radiation axis	250 ps ± 30 %
UWB EMP emission mode	pulse train
Pulse repetition frequency, continuously adjustable	from 100 to 1000 Hz
Duration of pulse train, discretely adjustable	0,1; 0,2; 0,5; 1,0 s ± 10 %
Duration of pulse train, continuously adjustable	from 10 s to 5 min
Power supply	220 V / 50 Hz

**Table 1. Parameters of mobile complex for testing of equipment immunity to UWB EMP**

	<p>Testing the control system of 1.9 TDH diesel engine in the open test area.</p>
	<p>Testing the radar "Groza-M-154" in the laboratory.</p>
	<p>Testing the industrial computer "IPC-610-SYS41-2" in the laboratory.</p>

**Table 2. Examples of testing the equipment immunity to UWB EMP**

### **Description of BSUIR:**

Since 2002 BSUIR is appointed by Decision of Belarus Government as a Key Organization in Republic of Belarus for solving problems of Interference Protection and Electromagnetic Compatibility (EMC) of Radio Electronic Equipment.

The World Priority of BSUIR in development of advanced technologies for system-level design of EMC and electromagnetic protection is confirmed

- by presentations of these technologies on leading international symposiums and exhibitions in USA, Canada, China, Japan, Russia, Germany, Great Britain, Belgium, France, Switzerland, Spain, Italy, Poland, India, etc.;

- by scientific publications in leading IEEE and EU editions,

- by exporting of Hi-Tech products and services on area of EMC/protection in 10 countries,

- by the great experience of experts of BSUIR EMC R&D Laboratory in solving of complicated EMC/protection problems for Belarus Government and different Belarus and foreign customers, and

- by the wide international scientific and technical cooperation with experts from Canada, USA, China, Israel, Italy, Great Britain, Sweden and other countries.

**EMC R&D Laboratory of BSUIR would be happy to cooperate with you in the proposed area as well as in other EMC-related areas!**

### **BSUIR Technique for EMC/EMP/EME/EMS system analysis & design:**



### **Contacts:**

Belarusian State University of Informatics and Radioelectronics (BSUIR)

EMC R&D Laboratory, tel.: (+37517) 2938994, 2938438, [www.emc.bsuir.by](http://www.emc.bsuir.by), [emc@bsuir.by](mailto:emc@bsuir.by)

BSUIR, 6, P. Brovka Str., Minsk, 220013, Republic of Belarus