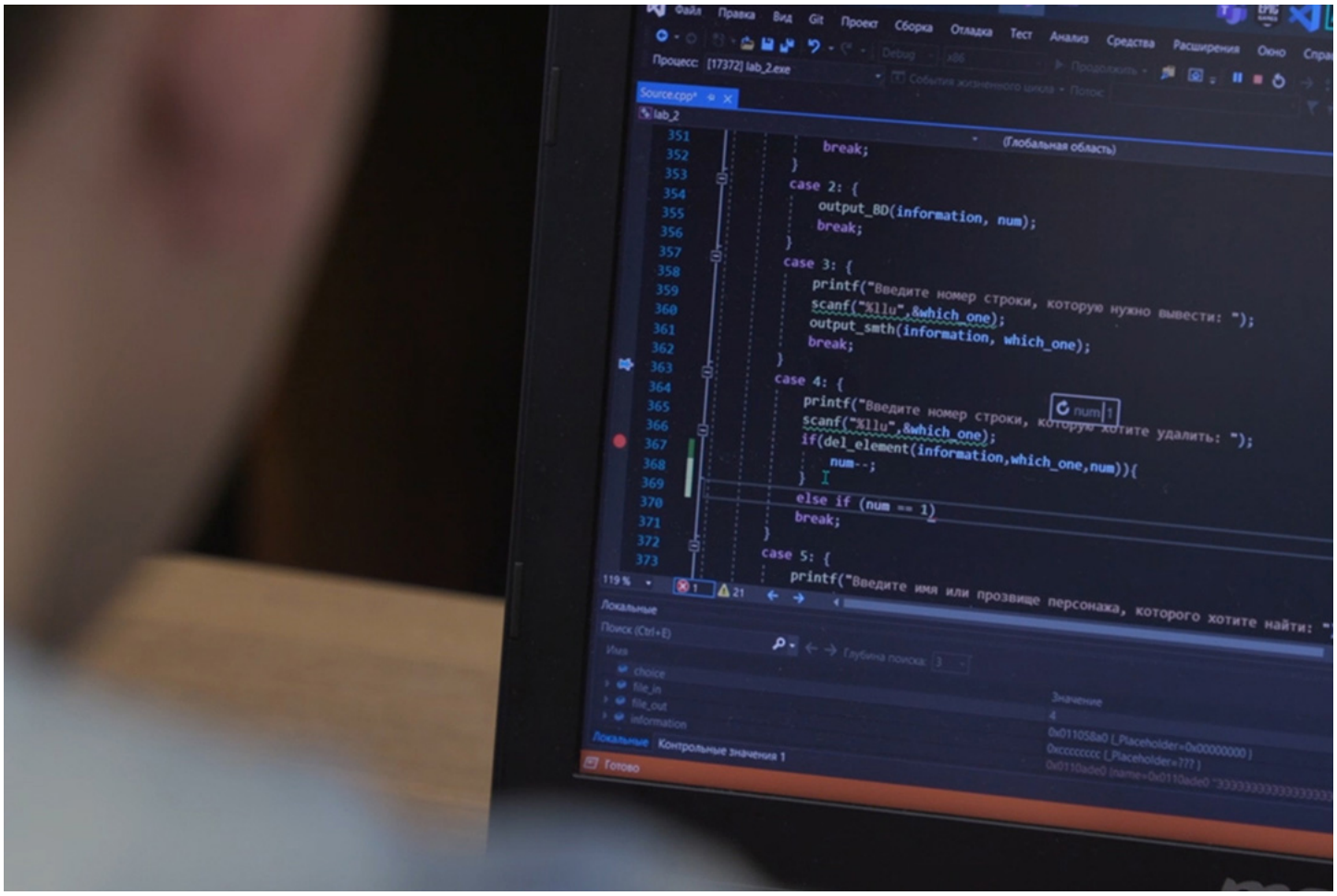
Scientists will protect the “Smart City” from cyber threats



St. Petersburg, like other cities in the Russian Federation, is actively participating in the establishment of the “Smart City” program, which will provide new services for residents of the megalopolis, increasing the safety of citizens. Digital services are essential for such a system.

Due to the Internet of Things (IoT) systems, the environment can adapt to the needs of humanity on its own accord. Cybersecurity threats are especially dangerous for such infrastructure.

Specialists from Peter the Great St. Petersburg Polytechnic University (SPbPU) developed the methodology for assessing cyber risks in intelligent systems of a Smart City. The developed methodology was tested on the “smart crossroads” test bench (a component of the smart transport system of a Smart City). The results were published in the scientific journal "Machines" of the MDPI Publishing House.

Scientists note that the new goal for cybercriminals is to disrupt the functioning of large enterprises and urban infrastructure, as well as is to intercept the control over them. The attackers using wireless links can remotely invade into the target subnet or device (a group of devices), intercept traffic, launch denial of service attacks, and take control of IoT devices to create botnets.

> “Currently, traditional cyber risk analysis strategies can’t be directly applied in the construction and assessment of digital infrastructures in a Smart City, because the new network infrastructure is heterogeneous and dynamic. The goal of our project is to ensure the level of the information assets security considering the specifics of modern cyber threats,” notes researcher Vasily Krundyshev, Institute of Cybersecurity and Data Protection SPbPU.

Researchers of St. Petersburg Polytechnic University developed a methodology for analyzing cybersecurity risks, which includes the stages of identifying asset types, identifying threats, calculating risks, and analyzing the resulting risk values. The proposed methodology is based on a quantitative approach, at the same time it is easily and quickly computable, which is especially important for the functioning of modern dynamic infrastructures. Experimental studies using a set of developed simulation models of typical digital infrastructures of a Smart City (Internet of Things, smart building, smart crossroads) demonstrated the superiority of the approach proposed by the authors over existing analogs.

In the near future, it is planned to arrange the automatic calculation of cybersecurity risks in a Smart City based on the developed methodology.

The reported study was funded by Russian Foundation For Basic Research according to the research project № 19-37-90001.