229. CYBER RESILIENCE IN CRITICAL INFORMATION INFRASTRUCTURE

Artsiomchyk V.S.
Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus
Shaputsko A.V. – Lecturer, Master of Arts (Philology)

This paper examines how approaches to protecting critical information infrastructure have been shifting from purely preventive methods toward a resilience-based model. It argues that achieving complete security is not realistic and highlights the need to build systems that can keep operating even when cyber incidents occur.

Critical infrastructure means things like power stations, water supply systems, hospitals, and transport networks. These are not just normal services – they are the things that keep a country running. If a power grid goes down, hospitals lose electricity, traffic systems stop working, and people can get hurt. Because of this, protecting these systems is a very serious topic, and both the government and private companies have to work together on it [1, 2].

For many years, the main idea in cybersecurity was to build a strong border around the network. Companies used firewalls and antivirus programs to try to stop hackers from getting in. This worked okay for a while, but the problem is that attackers became much smarter. Now they can steal employee passwords, use software bugs that nobody knew about, and move around inside a network without anyone noticing. The old way of just blocking the entrance is simply not good enough anymore [1].

Because of this, a new idea called cyber resilience has become popular. The main point is that you cannot stop every single attack, so you have to be ready for when something goes wrong. Instead of only trying to keep hackers out, organizations now focus on making sure their systems can still work even during an attack. For example, if one part of the system breaks, it should automatically switch to a backup so that the most important things keep running. This idea is called graceful degradation [2].

Industrial systems like factories and power plants have their own special problems. The computers that control machines are often very old and were not built with security in mind. You also cannot just turn them off to update them, because that would stop production. One solution is deep packet inspection, which means checking all the data going through the network in real time to find anything suspicious, without touching the machines themselves [1].

Another important method is called zero trust. The basic idea is that you should never automatically trust anyone, even if they are already inside the company network. Every time someone wants to access something, the system checks who they are, what device they are using, and whether it makes sense for them to be there. This is much safer than the old approach where anyone inside the network could move around freely [2].

The human side of security is just as important as the technical side. Many successful attacks happen not because the software was weak, but because an employee clicked on a bad link in an email. This is called phishing, and it is still one of the most common attack methods. Companies need to regularly train their staff to recognize these threats. It is also important to make sure that employees only have access to the things they actually need for their job, so that if one account is hacked, the damage is limited [1, 2]. Beyond training, organizations should also establish clear reporting procedures so that employees know exactly what to do when they notice something suspicious.

New technologies like artificial intelligence are also starting to help with cybersecurity. AI systems can look at huge amounts of data very quickly and spot unusual behavior that a human might miss. At the same time, more and more devices like cameras and sensors are being connected to networks in critical infrastructure, and many of them have very weak built-in security. This means organizations need to keep track of every device on their network and make sure everything is updated regularly.

In conclusion, the most important thing to understand is that perfect security does not exist. Every system can be attacked at some point, so the real question is how fast you can detect the problem and recover from it. Organizations that combine good technology, trained employees, and clear response plans will always be in a better position than those who just hope nothing bad happens. For IT students, learning about these topics is becoming one of the most useful skills you can have.

References:

1. Kaspersky ICS CERT Threat Report // Kaspersky ICS CERT. – URL: https://ics-cert.kaspersky.com (date of access: 10.03.2026).

2. ENISA Guidelines for Critical Information Infrastructure Protection // European Union Agency for Cybersecurity (ENISA). – URL: https://www.enisa.europa.eu (date of access: 10.03.2026).