Riabchinska V.
Scientific supervisor: Olishevskiy I.H.
(*Dnipro University of Technology, Dnipro, Ukraine*)

METHODS OF PROVIDING CYBER PROTECTION AT ENTERPRISES

Continuous cyber attacks affect industrial enterprises around the world, even those with a developed cybersecurity system. The damage caused by such attacks is growing exponentially, forcing companies to take new cybersecurity measures.

Extensive information about the existence of threats and lack of reliable information about the details of cyberattacks, many companies hide the facts of losses from them, understanding the scale of threats and lack of understanding of what to do, a wide range of solutions with conflicting descriptions of opportunities. decision - how to protect the industrial network.

One of the effective methods of counteracting industrial cyber threats is specialized vulnerability control systems developed for industrial automation systems. In addition to traditional requirements for connection monitoring, anomaly detection, and signature database vulnerabilities, such systems must work with specialized industry protocols.

The last "border" of protection against attacks from the IT network of the enterprise and the lower segment of the perimeter are specialized means of detecting / preventing cyber threats of ASC TP networks. This is an important tool, as a targeted attack may well pass through firewalls and reach a critical object in the lower segments of the industrial network.

A special mention should be made of the Distributed Deception Platform (DDP), which allows you to deploy a network of counterfeit and particularly attractive to attackers lures that are virtually indistinguishable from real ones.

Using false information available in traps, such as passwords, network environment, bookmarks, user files, and system configurations, is almost 99% likely to detect malicious intrusion. The technology network deploys simulations of PLCs, SCADA servers and other network assets, as well as the ability to highlight the real device that is the most attractive trap. Traps are actually penetration sensors.

In the course of writing this article, 4 main areas for building information security of the enterprise were identified (Table 1)

Table 1

1.	Basic security of network perimeter and remote access	With the increase in the number of devices connected to the IT infrastructure and the mass transition to remote work, the boundaries of the network perimeter of enterprises have expanded and blurred, so it needs more attention.
2.	Organization of effective access control systems	Identifying users is a must for any secure system, regardless of location, device type, or application. You can organize effective access control systems with the help of: -Build an SSO system (Simplify the authentication process) -Implementation of multi-factor authentication systems (For more effective protection of accounts)
3.	Risk reduction and loss minimization	Adherence to the principles of "zero trust", micro-segmentation and minimum access rights to systems and interfaces. Employees should have as many rights as they minimally need for their

		productive work.
4.	Cybersecurity system event monitoring	Control of all events by means of monitoring systems or external SOC (security operation center). So you can detect the actions of cybercriminals in advance and protect critical data of the enterprise.

Over the past few years, market uncertainty and changing consumer behavior have led to increased cybercrime and fraud, while remote labor is changing the perimeter of the network, opening up new avenues for hackers to access private and confidential data. The network infrastructure of most organizations was built according to the 80/20 rule, ie 80% of employees were in the office and 20% worked remotely. The pandemic turned this 80/20 rule upside down. When all the workforce is removed, this has created many new security vulnerabilities for IT teams. There are four things to think about: the perimeter, the VPN, the physical security of the computer, and, of course, the human element.

References

1. Guidelines on cybersecurity from experts [Electronic resource]. - Access mode: http: //www.isaca.org.ua/ index.php / press-center / news / 191-translation-of-guidelines-on-cybersecurity

2. Buryachok VL Information and cybersecurity: sociotechnical aspect: textbook / [V.L. Buryachok, VB Толубко, В.О. Хорошко, С.В. Tolyup]; for the head ed. Dr. Tech. Sciences, Professor VB Tolubka. - К .: ДУТ, 2015. - 288 с.

3. Klymenko V. Internal threats to information security of the organization / V. Klymenko // Bulletin of the NBU. - 2008. - № 5. - P. 62-63.

4. On Amendments to the Law of Ukraine “On Fundamentals of National Security of Ukraine”: Draft Law of Ukraine on Cyber Security of Ukraine of March 7, 2013 № 2483. - Access mode: // www.w1.c1.rada.gov.ua/ pls / zweb2 / webproc4_1? pf3511 = 45998