УДК 004
DOI: 10.31733/17-03-2023-554-555

Egor NICULIN
Laboratory of Information Security
(Academy of Economic Studies,
Chisinau, Moldova)
Scientific adviser: **S.A. Ohrimenco,**
DSc, Professor

CATEGORISATION OF CURRENT IT-CHALLENGES AND THREATS

The development of the modern economy is highly dependent on information technology (IT**)**. At the same time, the increasing use of the same information technology has given rise to a number of problems and threats that could well cause significant damage to businesses and individuals.

Among the most significant threats of this kind facing the modern economy are:

- Cybercrime - such as online fraud or cyber extortion;

- Cyberattacks - all kinds of hacking, development and introduction of malware and ransomware into networks;

- Data breaches - resulting in the loss or theft of confidential information. In particular, financial data, intellectual property (patent data and other trade secrets) and other private information.

- Disruptive attacks - Distributed denial of service (DDoS) attacks - can cause significant disruption to various complexes that support economic, financial or production activities;

- Supply chain attacks - in which attackers disrupt the software or hardware used in products or services. Both directly harm processes and indirectly undermine trust in technology;

- Human error. Despite numerous technical security measures, human error remains a significant threat to the security and stability of systems. And errors can be as simple as getting caught up in phishing scams or using vulnerable passwords, as well as systemic, resulting in ineffective security measures for businesses and organisations [1,3,5].

Thus, it is clear that through the widespread use of information technology and related systems already widely available today, individuals, groups and state agencies can exert concrete influence on economies, finances, politics at various levels and the personal security of citizens. Generally, these influences will be aimed at gaining different types of benefits and competitive advantages. This includes the economy.

These kinds of influences can take many forms, including:

- Industrial espionage. State- or corporate-sponsored actors or groups (including decentralised ones) may use attacks of various kinds or cyberspace to steal sensitive information from businesses, organisations and government agencies in the sponsoring state. The goal may be to give domestic companies a global or regional advantage in certain regions and destinations.

- Market manipulation. As in the previous example, individual professionals or groups sponsored by governments or corporations may use cyberattacks to manipulate financial markets or steal sensitive financial information to gain advantage.

- Infrastructure attacks. Also under the patronage of government agencies or individual corporations, certain actors can use cyberattacks to disrupt the critical infrastructure of rival corporations or states. Attacks could target power grids, transportation systems, communications structures, and more. The target of such an attack would be direct economic damage;

- Disinformation campaigns: Dissemination of false information directly about an opponent or critical to its functioning or even existence issues, events or actions. The aim is to achieve a strategic advantage. Including through undermining the trust of citizens, consumers or partners, fraught with significant complications for the opponent, both at the corporate and interstate levels [4,6].

The obvious conclusion is that an individual, society, state or corporation is vulnerable to modern cyber threats. And the number of these challenges, threats and other factors that can undermine information and, consequently, economic security will only increase over time.

These kinds of threats to information security can have serious consequences at various levels. Both for the individual and at the corporate level. And even government systems are seen

as vulnerable in this aspect [7].

The natural countermeasures are seen as investments in security technology, the development of robust cyber security policies and procedures, and the education and training of counter-cyber specialists. [8-10].

In addition, there is a clear need to develop a Single Universal Catalogue of Current IT Challenges and Threats. In addition to the description of threats and methodology of negative impacts, the Universal Catalogue should contain:

Continuously updated databases with examples of actual cybercrime; Detailed descriptions of goals achieved or not achieved by perpetrators; Methods used to disrupt and neutralise threats and subsequent investigations; Recommendations to minimise the chances of disruption to current security protocols and methodologies [11].

Such a catalogue could be the subject of several self-developing international projects running in parallel.

1. Chris Bronk (2016). Cyber Threat. The Rise of Information Geopolitics in U.S. National Security. Praeger Security International. ISBN: 978-1-4408-3498-1.

2. Jason Andress (2019). FOUNDATIONS OF INFORMATION SECURITY A Straightforward Introduction. No starch press. ISBN-10: 1-7185-0004-1 ISBN-13: 978-1-7185-0004-4.

Nurlan Karimov (2019). The European Union Cyber Security and Protection of Human Rights. DOI:10.13140/RG.2.2.26425.31841

4. Bernd W. Wirtz (2019). Digital Business Models. Concepts, Models, and the Alphabet Case Study. Springer. ISBN: 978-3-030-13004-6.

5. N. MACDONNELL ULSCH (2014). Cyber Threat! How to Manage the Growing Risk of Cyber Attacks. John Wiley & Sons, Inc. ISBN 978-1-118-935969-5.

6. Elizaveta Gaufman (2016). Security Threats and Public Perception. Digital Russia and the Ukraine Crisis. Springer. ISBN: 978-3-319-43201-4.

7. Andrew Whiting (2020). Construction Cybersecurity. Manchester University Press. ISBN: 978-1-5261-2332-.

8. Paul Rosenzweig (2013). Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare. The Great Courses. ISBN: 9781470381844.

9. https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637967/EPRS_BRI(2019)637967_EN.pdf

10. https://www.collegenp.com/technology/the-future-is-now-how-technology-is-changing-the-world/

11. https://www.law.kuleuven.be/citip/blog/should-companies-give-confidential-access-to-their-trade-secrets-part-1/

УДК 004+351.86
DOI: 10.31733/17-03-2023-555-557

Наталія ТОЛОШНА
науковий співробітник
наукової лабораторії соціологічних
та кримінально-правових досліджень
Дніпропетровського державного
університету внутрішніх справ

ВПЛИВ ІНФОРМАЦІЙНОГО ПРОСТОРУ НА НАЦІОНАЛЬНУ БЕЗПЕКУ В УМОВАХ ВОЄННОГО СТАНУ

Сьогодні як ніколи для України та її громадян потреба в безпеці стала базовою. «Посприяло» цьому повномасштабне вторгнення російської федерації та, як наслідок, реальні та потенційні загрози обстрілів, ракетних атак, наступу ворожих військ, щоденні кровопролитні бої, в яких українські захисники стримують та відбивають натиск держави-терориста.

У таких умовах держава, виконуючи свої безпосередні обов'язки перед громадянами, стоїть на захисті національної безпеки.

Відповідно до термінології закону України «Про національну безпеку України», національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Національні інтереси України, у свою чергу, – життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний