інтелектуального виявлення загроз, та адаптивних систем захисту.

Підвищення кваліфікації персоналу та підготовка експертів у галузі кібербезпеки: Необхідно проводити навчальні курси, тренінги та семінари для працівників правоохоронних та військових організацій з питань кіберзахисту. Це допоможе підготувати кваліфікованих фахівців, які зможуть вчасно реагувати на кіберзагрози.

Створення спеціалізованих центрів кібербезпеки: Важливо створити центри, які будуть відповідальні за моніторинг та аналіз кіберзагроз, а також за реагування на інциденти кібербезпеки в умовах воєнного стану.

Міжнародне співробітництво в галузі кібербезпеки: Україна повинна активно співпрацювати з іншими країнами та міжнародними організаціями у сфері обміну інформацією та досвідом щодо кіберзахисту під час воєнного конфлікту.

Забезпечення резервування та відновлення інформаційних систем: Важливо розробити та впровадити плани резервування та відновлення інформаційних систем, що дозволить відновити роботу критичних інформаційних ресурсів у найкоротший термін після кібератаки або інциденту.

Проведення свідомості та просвітницьких заходів: Важливо надавати інформацію громадськості про потенційні кіберзагрози та методи їх запобігання. Це допоможе залучити громадян до заходів кібербезпеки та створить атмосферу зростаючої уваги до цих питань у суспільстві.

Загалом, розвиток кіберзахисту під час воєнного стану в Україні вимагає комплексного підходу, спрямованого на створення надійного інформаційного простору та ефективну відповідь на кіберзагрози з метою захисту національних інтересів та забезпечення безпеки громадян і держави.

1. Синиціна Ю.П. Інформаційна безпека умовах військовий стану. Сучасні пріоритети розвитку України: економічна та інформаційна безпека: зб. матеріалів Всеукр. наук.-практ. конф. Дніпро: ДДУВС, 2023. С. 103–108.

2. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект. Підручник. Львів: «Магнолія 2006», 2018. 320 с.

3. Безуглий Д., Інформаційна безпека України: огляд останніх тенден- цій. Фізико-математична освіта, вип. № 2(16), 2018. С. 13–17 с.

УДК 004.738.5:351.862.4
DOI: 10.31733/15-03-2024/2/369-370

Egor NIKULIN
Olga PECHKOVSKAYA
students of group TI-222

Lucia GUZHUMAN
PhD, Associate Professor

Serghei OHRIMENCO
DsC, Professor

(Laboratory of Information Security,
Academy of Economic Studies,
Chisinau, Moldova)

NEW CHALLENGES OF CYBER SECURITY

The report examines new cyber security challenges in an ever-changing threat landscape. These include, most notably, an increased number of software abuses (e.g., crypto-ransomware) targeting mobile applications and communications and developed using artificial intelligence and machine learning tools [1],[2],[3].

A separate and poorly researched group of security threats is represented by situations when supercomputers will be used on the defending and attacking sides. Currently, such scenarios have been analysed only at the theoretical level, but their implementation is already possible in the confrontation in cyberspace between individual countries and their groups. The uniqueness of the situation lies in the following [4]:

- the power of supercomputers can be used both to build defence systems using artificial intelligence and to develop means of overcoming defence systems;

- cybercriminals have taken a swing at supercomputers and there have been cases of supercomputers being compromised due to cryptominer infections.

These phenomena give rise to hidden and unknown threats that pose a serious danger in connection with the development of ultra-high performance peta and exascale computing systems. The essence of hidden threats is as follows [5]:

– supercomputers use a high-performance element base of supercomputers, there is a huge number of components, which increases the probability of technical bookmarks and makes it more difficult to combat them;

– supercomputers have the highest performance, a large number of simultaneously running processes, which makes it difficult to track what is happening in them processes running simultaneously, making it difficult to monitor their events for intrusion detection;

– the information processed using supercomputers is related to national security issues and the solution of the most important scientific and technical tasks, management of critical infrastructures, etc., which is a serious motivation for organising cyberattacks;

– supercomputer users are highly qualified and there are usually many of them, which increases the risk of internal attacks;

– those interested in attacking supercomputing resources are highly skilled, usually representing organised communities, state-sponsored organisations and individual criminals;

– the attacking supercomputer can quickly assess the state of the attacked object, find vulnerabilities, plan and conduct a mass attack, quickly adapt to the results of the attack and conduct a series of subsequent attacks. This scenario can be realised in automatic mode under the control of the attacking party.

Due to changes in the threat landscape, new tasks to be initially solved should be identified. We consider it necessary to highlight the following, relying on a number of works [6-8]:

1. It is necessary to develop a set of models that can be used to determine the impact of new platforms on the creation and operation of computing systems in terms of protection against unauthorised access as a major cybersecurity threat.

2. New platforms depend on and require higher power consumption. For this, robust mechanisms must be developed to ensure secure power supply to critical processes. Otherwise, a deliberate attack or inadvertent failure in the energy supply loop will result in the loss of huge amounts of critical data needed to solve a large number of analytical problems.

3. The qualification requirements for cybersecurity users and administrators increase significantly, as the volume of data processed increases, specialised software is used, and additional training is required to work with it.

4. Supercomputers and their associations (supercomputer centres) are becoming a strategically important link in government administration. Such centres process and store categorised information with different classification codes. This requires a radical overhaul of security policy.

The above list of tasks does not exhaust the solution to all existing problems, but it makes us take a fresh look at current cybersecurity challenges.

1. Omar Santos, Samer Salam, Hazim Dahir (2024). The AI Revolution in Networking, Cybersecurity, and Emerging Technologies. Pearson Education, Inc. ISBN-13: 978-0-13-829369-7

2. Malini Rao (2023). AI/ML in Cybersecurity. Your Go to Guide to Understand AI/ML in Cybersecurity. Independently Published. ISBN-13 978-2854456370

3. Georgios I. Zekos (2023). Artificial Intelligence and Competition. Economic and Legal Perspectives in the Digital Age. Springer. ISBN 978-3-031-48083-6 https://doi.org/10.1007/978-3-031-48083-6

4. Molyakov A. New-age Supercomputers: Hi-Speed Networks and Information Security //Journal of Electrical and Electronic Engineering. 2019. Т. 7. №. 3. С. 82-86.

5. Molyakov A. S. New Multilevel Architecture of Secured Supercomputers //Current Trends in Computer Sciences & Applications. 2019. Т. 1. №. 3. С. 57-59.

6. Ben Buchanan (2020). The Hacker and The State. Cyber Attacks and the New Normal of Geopolitics. Harvard University Press. ISBN 978-0-674-24601-0

7. Ted Lee (2022). Strategic Hacker. FeelzON. ISBN 979-11-977833-1-9

8. Eric Cole (2013). Advanced Persistent Threat Understanding the Danger and How to Protect Your Organization. Elsevier, Inc.