DOI: https://doi.org/10.32782/PPSS.2023.1.82

ВИКЛИКИ ТА ЗАГРОЗИ В ГЛОБАЛЬНОМУ КІБЕРПРОСТОРІ: ЗАХОДИ З ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ У СУЧАСНОМУ СВІТІ

Ростислав Романович АТАМАНЮК,

курсант 3-го курсу Навчально-наукового інституту права та підготовки фахівців для підрозділів Національної поліції Дніпропетровського державного університету внутрішніх справ
https://orcid.org/0009-0000-4653-7960

Науковий керівник: *Копилов Е. В., викладач кафедри оперативно-розшукової діяльності Дніпропетровського державного університету внутрішніх справ*

CHALLENGES AND THREATS IN THE GLOBAL CYBERSPACE: MEASURES TO ENHANCE CYBERSECURITY IN THE MODERN WORLD

The text examines current cybersecurity issues in the modern world, focusing on the rise of cyber threats and identifying their general and specific aspects. Among the primary threats highlighted are cyber-attacks, cyber espionage, and cyber terrorism, which can lead to significant consequences for economic activities, infrastructure, and national security. It is noted that the increasing volume of personal information in the global cyberspace poses a threat of misuse. To effectively counter these threats, the author recommends a comprehensive approach to cybersecurity. This includes the necessity of a systematic and continuous approach to protection, regular updates of software and hardware, the use of strong passwords and two-factor authentication, conducting regular security audits, and protection against phishing and internal threats. Emphasis is also placed on the importance of collaboration, information exchange, and education as effective means to combat cyber threats. Overall, the text underscores that ensuring cybersecurity requires not only technical measures but also cultural changes, collaboration, and education to guarantee reliable protection in a world where cyber threats continually grow in complexity and scale.

Глобальний кіберпростір став суттєвою складовою сучасного світу, а разом з цим зростають і загрози, пов'язані з кібербезпекою. Ці загрози включають в себе кібератаки, кібершпигунство, кібертероризм, а також інші види зловмисних дій в мережі. З метою захисту сучасного світу від кіберзагроз та викликів, необхідно вживати комплекс заходів з підвищення кібербезпеки.

Однією з найпоширеніших загроз є кібератаки. Кіберзлочинці можуть атакувати комп'ютерні системи, мережі та додатки з різних мотивів, включаючи фінансову вигоду, розвідку та знищення даних. Кібератаки можуть мати серйозні наслідки для господарської діяльності, інфраструктури та національної безпеки.

Країни і злочинці використовують кібершпигунство для отримання конфіденційної інформації з різних сфер, включаючи політику, економіку та обо-

рону. Це може становити загрозу для національної безпеки і веде до появи кібершпигунських скандалів та конфліктів між країнами.

Кібертерористи використовують кібератаки для сприяння своїм ідеологічним чи політичним цілям. Ця загроза може призвести до руйнування інфраструктури, втрати життів та загрози глобальній безпеці.

Збільшення кількості особистої інформації, яка зберігається в глобальному кіберпросторі, створює загрозу зловживанням цією інформацією. Втрата особистих даних може призвести до крадіжок і шахрайства [1].

Підвищення кібербезпеки у сучасному світі вельми важливе завдання, оскільки глобальний кіберпростір стає все більш вразливим на кіберзагрози. Ось кілька заходів, які призначені для підвищення кібербезпеки:

Захист від кіберзагроз вимагає системного та постійного підходу. Організації повинні бути готовими до атак, стежити за новими загрозами та адаптуватися до них, щоб забезпечити надійну кібербезпеку.

В сучасному світі, де глобальний кіберпростір відіграє значущу роль в нашому житті, підвищення кібербезпеки є істотною складовою забезпечення інформаційної безпеки, економічного розвитку та національної безпеки. Загрози в цій сфері стають все більш вибагливими та розповсюдженими, тож ефективні заходи для їх запобігання та усунення стають критично важливими. Забезпечення кібербезпеки вимагає не лише технічних заходів, але й культурних змін, співпраці та освіти. Тільки за таких умов можна гарантувати надійний захист у світі, де кіберзагрози постійно зростають у складності та масштабі. Надійна кібербезпека є необхідною для забезпечення стабільності, приватності та безпеки в цій важливій сфері нашого життя.

1) Регулярне оновлення програмного забезпечення та апаратури. Забезпечення, що всі операційні системи, програми і апаратні засоби оновлюються до останніх версій, є важливим для закриття вразливостей, які можуть бути використані зловмисниками.

2) Міцні паролі та двофакторна аутентифікація. Вимагати від користувачів створювати міцні паролі та включайте двофакторну аутентифікацію для доступу до важливих систем і облікових записів.

3) Регулярні аудити безпеки. Проводити періодичні аудити безпеки для виявлення вразливостей та вирішення їх.

4) Захист від фішингу. Навчити персонал розпізнавати спроби фішингу та надайте їм інструменти для захисту від них.

5) Співпраця та обмін інформацією. Співпрацювати з іншими організаціями та урядовими структурами для обміну інформацією про кіберзагрози і обрані методи захисту.

6) Захист від внутрішніх загроз. Звернути увагу на захист від можливих внутрішніх загроз, таких як недобросовісні співробітники або витоки інформації.

7) Школа та навчання. Навчання персоналу та користувачів кібербезпеці є критично важливим для запобігання атакам та загрозам.

8) Використання сучасних технологій. Використання інноваційних технологій, таких як штучний інтелект, для виявлення та запобігання кіберзагрозам.

9) Захист критичної інфраструктури. Забезпечення надійного захисту критичних об'єктів, таких як енергетика, транспорт та комунікації.

10) Постійна оцінка та оновлення стратегій кібербезпеки. Кіберзагрози постійно змінюються, тому важливо постійно переглядати та оновлювати свої стратегії та заходи з підвищення кібербезпеки [2].

Список використаних джерел:

1. Коженівський Т. В. Кіберзлочинність як загроза сучасній безпеці. *Протидія кіберзагрозам та торгівлі людьми* : матер. наук.-практ. конф. (26 листоп. 2019 р., м. Харків). Харків : ХНУВС, 2019. С. 89-92.

2. Столбовий В. М., Кисленко Д. П. Заходи з підвищення кібербезпеки на державному та корпоративному рівнях в умовах діджеталізації суспільства. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична.* Випуск 37/2023. С. 175-183.

3. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки. *Міжнародні відносити.* 2018, №18-19.