КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.23.310317
УДК 65.011.56:004

**Фролов Ігор Михайлович**
Приватний вищий навчальний заклад «Європейський університет»
ORCID ID: 0009-0004-1163-8787
*ihor.frolov@e-u.edu.ua*

**Колодінська Яніна Олексіївна**
Приватний вищий навчальний заклад «Європейський університет»
ORCID ID: 0000-0002-3330-7565
*yanina.kolodinska@e-u.edu.ua*

# МЕНЕДЖМЕНТ КІБЕРБЕЗПЕКИ ІТ-ПРОДУКТІВ

**Анотація.** У статті розглянуто актуальні питання менеджменту кібербезпеки ІТ-продуктів. Зокрема, увагу приділено видам кіберзагроз та методам підвищення рівня безпеки підприємства й ІТ-продуктів. Відзначено важливість дослідження цієї тематики у зв'язку з розвитком ІТ-галузі в Україні та ролі ІТ-сфери для вітчизняної економіки в умовах повномасштабної російської агресії. Проаналізовано сучасні тенденції недоброякісного використання інформаційних технологій у гібридній війні, що обумовлюють необхідність дослідження інструментів здійснення кіберзлочинів, ключових груп зловмисників та інформації, яка є постійною ціллю для кібератак. У роботі проведено аналіз сучасних методів кібератак та їх наслідків на якість ІТ-продукту і діяльність підприємства. На основі отриманих результатів розроблено рекомендації щодо формування ефективної системи кіберзахисту. Зокрема, визначено ключові напрями забезпечення кіберзахисту підприємства, спрямовані на посилення захисту та підвищення конкурентоспроможності вітчизняних розробників ІТ-продуктів на міжнародному та внутрішньому ринках. Наголошено на актуальності тематики дослідження в умовах перерозподілу бюджетних коштів на критично важливі сектори економіки, що вимагає від менеджменту виробників ІТ-продуктів пошуку вітчизняних та міжнародних інвестицій. У цьому контексті забезпечення надійними методами й інструментами кіберзахисту розглядається як один з ключових факторів конкурентоспроможності сучасних розробників ІТ-продуктів. Загалом, стаття містить комплексний підхід до дослідження проблематики менеджменту кібербезпеки ІТ-продуктів, що є особливо актуальним в умовах гібридної війни та зростаючої залежності економіки від ІТ-сфери. Отримані результати можуть бути використані для створення та удосконалення існуючої політики забезпечення кіберзахисту на підприємстві й ІТ-продуктах.

**Ключові слова:** кібербезпека; ІТ-продукт; кібератаки; кіберзлочин; система менеджменту кібербезпеки.

## ВСТУП

**Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями.** В умовах повномасштабного вторгнення росії на територію України перед вітчизняними підприємствами постало питання готовності до атак ворога на території кіберпростору як повноцінному фронті під час кібервійни. Зокрема менеджмент вітчизняних виробників ІТ-продукції був вимушений зіткнутися з потребою удосконалення існуючої системи кіберзахисту або ж розробляти нову відповідно до актуальних викликів та загроз в інформаційному просторі.

В наслідок перерозподілу бюджетних коштів на критично важливі сектори економіки перед менеджментом багатьох виробників ІТ-продуктів постало питання пошуку вітчизняних та міжнародних інвестицій, вирішення якого вимагає посилювати

зусилля та шукати засоби для перемоги у конкурентній боротьбі з-поміж підприємств на міжнародному та вітчизняному ринку. Сучасні тенденції розвитку ІТ-продуктів потребують забезпечення надійними методами й інструментами кіберзахисту як одного з ключових акторів конкурентоспроможності сучасних розробників ІТ-продуктів. Визначення ключових напрямів забезпечення кіберзахисту підприємства спрямоване на посилення захисту і підвищення конкурентних позицій українських ІТ-продуктів на вітчизняному та міжнародному ринку.

**Аналіз досліджень та публікацій.** Дослідження системи кіберзахисту на підприємствах усіх галузей економіки України є актуальною темою наукових досліджень. Питанню забезпечення підприємств у кіберпросторі присвячено роботи багатьох вітчизняних вчених. Зокрема вчені досліджують місце менеджменту кібербезпеки у сучасній управлінській науці та практиці [2], [6], [7], методи протидії кібератакам [4] – [6], а також ризики та можливості кібербезпеки у сучасних економічних моделях [5] – [7]. В умовах повномасштабної війни набуває актуальності дослідження проблематики інтеграції цифрових технологій у військові доктрини [3].

Враховуючи сучасні тенденції розвитку ринку вітчизняних ІТ-продуктів, виникає потреба дослідження методів забезпечення ефективної системи протидії атакам зловмисників та захист українських підприємств у кіберпросторі.

**Мета дослідження** полягає в формуванні пропозицій для удосконалення систем кіберзахисту підприємств України відповідно до сучасних методів здійснення кіберзлочинів та новітніх інструментів злоякісного впливу зловмисників на персонал підприємств та користувачів вітчизняних ІТ-продуктів.

## ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

ІТ-сектор України, зокрема підприємства з розробки та впровадження ІТ-продуктів відіграють важливу роль в умовах війни, забезпечуючи валютні надходження у вітчизняну економіку, створюючи нові робочі місця, а також сприяючи технологічному розвитку завдяки розробці та впровадженню інновацій. Залучення іноземних інвестицій забезпечують економічне та інноваційне зростання, а також створюють нові шляхи для міжнародної співпраці й інтеграції [10], [11]. Українські фахівці розробляють ІТ-продукти для забезпечення військових, управлінських, освітніх та громадських потреб [1]. Саме тому актуальності набуває розробка систем кіберзахисту від ворожих атак задля збереження конфіденційної інформації споживачів та розробників даних ІТ-продуктів та уникнення позапланових витрат на відшкодування наслідків від скоєних кіберзлочинів.

Забезпечення належного рівня безпеки є обов’язковим завданням менеджменту будь-якого підприємства чи організації. Розвинена система безпеки необхідна для ефективного функціонування розробника ІТ-продуктів. Наявність кіберзахисту є запорукою привабливості підприємства для інвесторів, клієнтів та працівників, що посилює конкурентні позиції ІТ-продуктів компанії на ринку [2]. Водночас наявність прогалин в системі захисту кіберпростору може стати причиною втрати конфіденційної інформації наявних контрагентів, виникнення зайвих джерел фінансових і кадрових втрат, а також призвести до витіснення підприємства з ринку.

Для розробки ефективної системи кіберзахисту менеджмент повинен чітко визначити сторони зацікавлені у здійснені кібератак, інформацію на заволодіння якою

будуть спрямовані зусилля зловмисників, наслідки від здійснення успішних кібератак, та найбільш розповсюджені методи кіберзлочинів [9].

Кібератаки на підприємство або на ІТ-продукт можуть здійснювати різні зацікавлені сторони, визначення яких допоможе оцінити рівень кіберзагроз на основі мотивації потенційних зловмисників та розробити ефективну стратегію протидії та уникнення загроз у кіберпросторі. До потенційних учасників кіберзлочину можна віднести наступні категорії [3], [4]:

- держави відповідно до своїх геополітичних, економічних та військових мотивів. Завдяки наявності значних ресурсів здатні тривалий час здійснювати кібератаки для отримання розвідданих або здійснення диверсій;
- приватні організації або компанії, які здійснюють кібератаки на замовлення спонсоруючого їх уряду, підприємства чи організації для досягнення необхідних цілей;
- кібертерористи, діяльність яких в основному спрямована проти цивільного населення для поширення терору чи переслідування політичних цілей шляхом атак на інформаційні мережі для викрадення конфіденційних даних;
- кіберзлочинці. До цієї категорії належать особи або злочинні угрупування метою яких є отримання прибутку від викупу або продажу викраденої конфіденційної інформації про ІТ-продукт, працівників, партнерів або клієнтів підприємства;
- кіберактивісти, які використовують кібератаки для поширення пропаганди або нанесення шкоди підприємству чи ІТ-продукту відповідно до своєї мети;
- недобросовісні конкуренти, які бажають викрасти результати розробок або іншу конфіденційну інформацію;
- інсайдери. До цієї категорії належать особи всередині підприємства які випадково або навмисно зловживають своїм доступом до інформації та ресурсів;
- автоматизовані програми (боти та віруси), які можуть використовувати для поширення спаму, DDoS-атак, викрадення даних та маніпулювання соціальними мережами та інших цілей кіберзлочинців;
- системи штучного інтелекту також можуть використовуватися для автоматизації кібератак та інших зловмисних дій.

Важливо зазначити, що різні категорії кіберзлочинців можуть об’єднуватись один з одним для досягнення власних цілей, що дозволяє їм розширити перелік потенційних інструментів для кібератак.

Необхідно розуміти які конфіденційні дані є цікавими для кіберзлочинців задля створення ефективної системи їх захисту. Зусилля зловмисників у кіберпросторі можуть бути спрямовані на заволодіння такою інформацією про підприємство або ІТ-продукт, як [2], [6]:

- інформація про ІТ-продукт: код, інформація користувачів, конфіденційна документація та інтелектуальна власність підприємства;
- інформація про розробника ІТ-продукту: фінансові дані, конфіденційна інформація співробітників, документація компанії, дані клієнтської бази.

Викрадення конфіденційної інформації внаслідок кібератак може призвести до негативних наслідків для підприємства та ІТ-продукту. До таких наслідків відносять [2], [5]:

- втрата конфіденційної інформації про ІТ-продукт, його розробників та споживачів;
- технічне відставання від конкурентів внаслідок втрати потенційних зусиль на розробку та впровадження інновацій на користь пошуку засобів усунення наслідків спричинених кібератаками;
- втрата користувачів ІТ-продукту через небезпеку втрати приватності та загальну ненадійність ІТ-продукту;
- втрата кваліфікованих кадрів через незабезпечення належних умов праці в інформаційному просторі;
- додаткові часові витрати на здійснення професійної діяльності внаслідок перерв у роботі підприємства викликаних технічними збоями;
- додаткові фінансові витрати на відшкодування наслідків кібератак спричинених користувачам, розробникам та інвесторам ІТ-продукту;
- втрата іміджу надійного та безпечного підприємства серед учасників ринку;
- втрата потенційних інвесторів які не бажають витрачати кошти на розвиток небезпечного ІТ-продукту;
- втрата конкурентних позицій на ринку внаслідок перерахованих вище наслідків.

Усвідомлення усіх можливих наслідків нехтування розробкою ефективної системи кіберзахисту допоможе менеджменту підприємства та розробникам ІТ-продуктів зосередити необхідні зусилля на усуненні недоліків у комплексі протидії зловмисникам в інформаційному просторі.

Важливою складовою комплексу ефективної протидії кіберзагрозам є визначення можливих методів та інструментів кібератак на ІТ-продукт, його розробників та користувачів [8]. Сучасний розвиток засобів здійснення злочинних дій в інформаційному середовищі характеризується великим розмаїттям інструментів здійснення атак, масштабами та специфікою проведення, мірою автоматизації та спрямованістю кінцевого результату кіберзлочину.

До найбільш розповсюджених методів кібератак на підприємства з розробки та впровадження ІТ-продуктів відносяться [2],[4] – [7]:

- фішингові атаки, які спрямовані на отримання конфіденційної інформації розробників і користувачів шляхом надсилання вірусовмісних повідомлень через соціальні мережі або ІТ-продукт. Наслідками такої кібератаки може стати втрата паролів, передача третій стороні доступу до номерів та PINкодів платіжно-розрахункових карт, розповсюдження історії та закладок браузера;
- застосування автоматизованих ботів для аналізу наявних вразливостей системи або ІТ-продукту, підбираючи паролі та розміщуючи у системи шкідливе програмне забезпечення;
- DDoS-атаки які полягають у створенні великих обсягів фальшивого трафіку до комп’ютерної системи підприємства або напряму на ІТ-продукт для перевищення можливого обсягу трафіку з метою позбавлення доступу до продукту звичайних користувачів;
- шкідливе програмне забезпечення, створене для проведення кібератак або заподіяння шкоди комп’ютерним системам. Зазвичай воно здатне поширюватись і заражати додаткові комп’ютерні системи;
- використання програм-вимагачів для шифрування даних на комп’ютері жертви з метою отримання викупу за розшифровку даних. Користувачів та

розробників IT-продукту можуть поставити перед вибором: заплатити викуп або прийняти ризик видалення важливих даних;
- перехоплення даних користувачів через фейкові веб-сайти або інструменти IT-продукту;
- соціальна інженерія спрямована на співробітників, щоб через психологічні маніпуляції змусити їх розкрити конфіденційну інформацію про підприємство, IT-продукт та користувачів;
- кібератаки проведені недобросовісними співробітниками зсередини організації через зловживання доступом з метою корпоративного шпигунства чи здійснення диверсій.

Розглянута інформація повинна допомогти менеджменту IT-компаній в розробці ефективної системи кіберзахисту підприємства та створених IT-продуктів. Серед складових системи менеджменту кібербезпеки варто виділити наступні [2], [4] – [7]:

- дослідження та аналіз ризиків кібербезпеки підприємства шляхом створення відповідного відділу на підприємстві та використання методології OCTAVE або методики ISO 27005;
- розробка нормативної документації з вимогами та засобами підтримки сформованої політики кібербезпеки яка б включала правила поведінки у кіберпросторі, визначала відповідальних осіб за підтримку належного рівня кіберзахисту підприємства та IT-продуктів та порядок дій при виникненні загрози кібератаки;
- використання інноваційних та перевірених методів шифрування даних, VPN, аутентифікації та моніторингу стану кібербезпеки на підприємстві для зменшення кількості можливих варіантів доступу зловмисників до конфіденційної інформації компанії;
- використання системи корпоративних облікових записів, ліцензійного програмного забезпечення та надійних паролів для запобігання найбільш розповсюджених методів здійснення кіберзлочинів;
- застосування антивірусних програм для діагностики корпоративного обладнання на наявність шкідливого програмного забезпечення та перевірки вкладених електронних ділових листів, а також для виявлення та видалення вірусів;
- використання брандмауера для контролю трафіку, блокування вірусовмісних сайтів та обмеження відправлення службових даних на пристрої, що не належать до корпоративної власності;
- ігнорування підозрілих повідомлень та аналіз змісту листів які шахраї видають за розпорядження керівництва;
- створення резервних копій даних з метою забезпечення безпечного зберігання важливої інформації;
- інвестиції в освіту та належні умови праці співробітників як один з головних факторів забезпечення кібербезпеки підприємства. В умовах постійного удосконалення методів протидії кібератакам людський фактор залишається вразливою частиною найефективнішої системи кіберзахисту будь-якого підприємства. Недостатня обізнаність персоналу та ненормовані умови праці, внаслідок яких допускаються помилки у використанні інформаційних систем, стають причинами ефективності існуючих методів кібератак на підприємство та IT-продукти. Тому важливо розвивати корпоративну культуру підприємства, орієнтуючись на потреби та методи захисту кіберпростору.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Розглянуті у статті питання розвитку менеджменту кібербезпеки IT-продуктів набувають актуальності в умовах повномасштабної війни росії проти України як важливого напряму в економіці сьогодення. Сучасні тенденції розвитку IT-продуктів потребують забезпечення надійними методами й інструментами кіберзахисту як одного з ключових факторів конкурентоспроможності українських розробок. Авторами зазначено, що ефективна система кіберзахисту повинна ґрунтуватися на чіткому розумінні зацікавлених сторін у здійсненні кібератак, потенційних наслідків від них, а також методів та інструментів, які можуть використовувати зловмисники.

Виділено важливі складові системи кіберзахисту: дослідження та аналіз ризиків, розробка нормативної документації, використання інноваційних методів шифрування, антивірусних програм та брандмауерів, створення резервних копій даних та інвестування в освіту та належні умови праці співробітників.

Отримані результати можуть бути використані при розробці нових методів та алгоритмів захисту інформації від кібератак, вивчення досвіду країн-лідерів у сфері кібербезпеки та адаптації їхніх практик до українських реалій, дослідженні психологічних та соціальних факторів, які впливають на кібербезпеку, а також при підготовці фахівців з кібербезпеки, які володіють знаннями та навичками для протидії сучасним кіберзагрозам.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kompanets, N. I. (2024). The influence of martial law on the transformation of business behavior models of IT enterprises. *Academic visions, (27).* https://doi.org/10.5281/zenodo.11120608
2. Horbachenko, S. (2024). The place of cybersecurity management in modern management science and practice. *Sustainable development of the economy, (1(48),* 144–149. https://doi.org/10.32782/2308-1988/2024-48-19
3. Stanko, A., Mykytyshyn, A., & Blavitskyi, A. (2024). Integration of modern technologies into military doctrines: cyber threats and adaptation to the digital dimension of conflicts. In *Military conflicts and man-made disasters: historical and psychological consequences,* 75–77.
4. Kuzina, V., & Filipov, M. (2024). Modern trends in the development of information technology. In *Modern youth in the world of information technology,* 49–50.
5. Horbachenko, S. A., & Klevtsyevych, N. A. (2024). The role of cybersecurity in the implementation of circular economic models: risk and opportunity analysis. *Visnyk of Kherson National Technical University, (1(88)),* 342–348. https://doi.org/10.35546/kntu2078-4481.2024.1.48
6. Horodianska, L. (2024). Cyber Threats in Small Businesses in the Current Environment. In *New information technologies of business management,* 59–62.
7. Haiduk, O., & Zverev, V. (2024). Analysis of cyber threats in the context of rapid development of information technology. *Cybersecurity: Education, Science, Technique, 3(23),* 225–236. https://doi.org/10.28925/2663-4023.2024.23.225236
8. Lakhno, V. A., Kasatkin, D. Y., Skliarenko, O. V., & Kolodinska, Y. O. (2022). Modeling and Optimization of Discrete Evolutionary Systems of İnformation Security Management in a Random Environment. Machine Learning and Autonomous Systems. *Smart Innovation, Systems and Technologies, 269,* 9–22. https://doi.org/10.1007/978-981-16-7996-4_2
9. Shulha, O., Gudz, I., Kotvytska, N., Koretska, N., Nikolaievskyi, O., Kolodinska, Y., Lytvynenko, L., & Vilianskyi, A. (2023). Management of employees` staff motivation in higher education institutions in Ukraine. *AD ALTA: Journal of Interdisciplinary research, 13(1),* 154–158.
10. Kolodinska, Y. (2024). Network methods of simulation of it project management processes in the conditions of the digital economy. *Herald of Khmelnytskyi National University. Economic Sciences, 326(1),* 289–296. https://doi.org/10.31891/2307-5740-2024-326-45
11. Kolodinska, Y., & Velykoivanenko H. (2023). Innovative entrepreneurship as a factor in the development of the digital economy: current trends and challenges in Ukraine. *Economics and management, 2,* 31–38.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023

**Ihor Frolov**
Private Higher Educational Establishment "European University"
ORCID ID: 0009-0004-1163-8787
*ihor.frolov@e-u.edu.ua*

**Yanina Kolodinska**
Private Higher Educational Establishment "European University"
ORCID ID: 0000-0002-3330-7565
*yanina.kolodinska@e-u.edu.ua*

# CYBERSECURITY MANAGEMENT OF IT PRODUCTS

**Abstract.** The article delves into the pressing issues of cybersecurity management for IT products. Particular attention is paid to the types of cyber threats and methods for enhancing the security of enterprises and IT products. The importance of researching this topic in the context of the development of the IT industry in Ukraine and the role of the IT sphere for the domestic economy in the conditions of full-scale russian aggression is emphasized. Modern trends of malicious use of information technologies in hybrid warfare are analyzed, which necessitates the study of tools for committing cybercrimes, key groups of attackers, and information that is a constant target for cyberattacks. The paper analyzes modern methods of cyberattacks and their consequences on the quality of the IT product and the activities of the enterprise. Based on the obtained results, recommendations for the formation of an effective cybersecurity system are developed. In particular, the key directions of cybersecurity for the enterprise are defined, aimed at strengthening protection and increasing the competitiveness of domestic IT product developers in the international and domestic markets. The relevance of the research topic in the context of the redistribution of budget funds to critically important sectors of the economy is emphasized, which requires the management of IT product manufacturers to search for domestic and international investments. In this context, ensuring reliable methods and tools of cybersecurity is considered as one of the key factors of competitiveness of modern IT product developers. Overall, the article presents a comprehensive approach to the study of cybersecurity management of IT products, which is especially relevant in the conditions of hybrid warfare and the growing dependence of the economy on the IT sphere. The results obtained can be used to create and improve the existing cybersecurity policy for the enterprise and IT products.

**Keywords:** cybersecurity; IT product; cyberattacks; cybercrime; cybersecurity management system.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kompanets, N. I. (2024). The influence of martial law on the transformation of business behavior models of IT enterprises. *Academic visions, (27).* https://doi.org/10.5281/zenodo.11120608
2. Horbachenko, S. (2024). The place of cybersecurity management in modern management science and practice. *Sustainable development of the economy, (1(48),* 144–149. https://doi.org/10.32782/2308-1988/2024-48-19
3. Stanko, A., Mykytyshyn, A., & Blavitskyi, A. (2024). Integration of modern technologies into military doctrines: cyber threats and adaptation to the digital dimension of conflicts. In *Military conflicts and man-made disasters: historical and psychological consequences,* 75–77.
4. Kuzina, V., & Filipov, M. (2024). Modern trends in the development of information technology. In *Modern youth in the world of information technology*, 49–50.
5. Horbachenko, S. A., & Klevtsyevych, N. A. (2024). The role of cybersecurity in the implementation of circular economic models: risk and opportunity analysis. *Visnyk of Kherson National Technical University, (1(88))*, 342–348. https://doi.org/10.35546/kntu2078-4481.2024.1.48
6. Horodianska, L. (2024). Cyber Threats in Small Businesses in the Current Environment. In *New information technologies of business management*, 59–62.

7. Haiduk, O., & Zverev, V. (2024). Analysis of cyber threats in the context of rapid development of information technology. *Cybersecurity: Education, Science, Technique, 3(23),* 225–236. https://doi.org/10.28925/2663-4023.2024.23.225236
8. Lakhno, V. A., Kasatkin, D. Y., Skliarenko, O. V., & Kolodinska, Y. O. (2022). Modeling and Optimization of Discrete Evolutionary Systems of İnformation Security Management in a Random Environment. Machine Learning and Autonomous Systems. *Smart Innovation, Systems and Technologies, 269,* 9–22. https://doi.org/10.1007/978-981-16-7996-4_2
9. Shulha, O., Gudz, I., Kotvytska, N., Koretska, N., Nikolaievskyi, O., Kolodinska, Y., Lytvynenko, L., & Vilianskyi, A. (2023). Management of employees` staff motivation in higher education institutions in Ukraine. *AD ALTA: Journal of Interdisciplinary research, 13(1),* 154–158.
10. Kolodinska, Y. (2024). Network methods of simulation of it project management processes in the conditions of the digital economy. *Herald of Khmelnytskyi National University. Economic Sciences, 326(1),* 289–296. https://doi.org/10.31891/2307-5740-2024-326-45
11. Kolodinska, Y., & Velykoivanenko H. (2023). Innovative entrepreneurship as a factor in the development of the digital economy: current trends and challenges in Ukraine. *Economics and management, 2,* 31–38.