**DOI:** https://doi.org/10.30837/EK.2023.032

**Ткаченко А.Г.,**
*здобувач,*
*Харківський національний університет радіоелектроніки*
*ORCID: https://orcid.org/0000-0002-6714-7731*
**Шапошник Б.В.**
*здобувач,*
*Харківський національний університет радіоелектроніки*
*ORCID: https://orcid.org/0000-0001-5439-906X*

# КІБЕРСТІЙКІСТЬ ДЛЯ ПІДВИЩЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

В епоху, позначену зростанням цифровізації, економічна безпека підприємств залежить від їх здатності протистояти кіберзагрозам і відновлюватися після них. Кіберстійкість стала критично важливою концепцією для захисту бізнесу від потенційно руйнівних наслідків кібератак.

Так, у звіті компанії Cisco [1] наголошується, що:

– 86 % організацій принаймні один користувач намагався підключитися до фішингового сайту;

– 70 % організацій мали користувачів, які отримували шкідливу рекламу в браузері;

– 50 % організацій зіткнулися з діяльністю, пов’язаною з програмами-вимагачами;

Глобальна кіберзлочинність щодня завдає компаніям 16,4 мільярдів збитків, а атака програм-вимагачів відбувається кожні одинадцять секунд [2].

Європейське агентство з кібербезпеки ENISA проаналізувало основні загрози у кіберпросторі, які включають: програми-вимагачі, зловмисне програмне

забезпечення, засоби соціальної інженерії (пропаганда, дезінформація), загрози для даних, відмова в обслуговуванні, маніпулювання інформацією та втручання, атаки на ланцюг поставок [3]

Проте управління ризиками є складним, безперервним, повторюваним процесом для всіх організацій. Сьогодні багатьом компаніям потрібна допомога у створенні суворого підходу до управління кіберризиками.

Успішна кібератака може порушити роботу підприємства, призвести до простою та втрати продуктивності. Це може мати каскадний вплив на ланцюг поставок і відносини з клієнтами. А через те, що у глобалізованій економіці підприємства взаємопов'язані. Порушення в одній організації може негативно вплинути на інші в екосистемі, ще більше підкреслюючи важливість кіберстійкості [4].

Підприємства, які стають жертвами кібератак, часто зазнають значних фінансових втрат. Вони можуть включати прямі витрати, такі як витрати на пом'якшення порушення, юридичні витрати та штрафи регуляторів. Крім того, існують непрямі витрати, пов'язані зі збитком репутації та втраченими можливостями для бізнесу.

Кіберстійкість означає здатність організації готуватися до кіберінцидентів, реагувати на них і відновлюватися після них, продовжуючи ефективну роботу. Вона охоплює проактивний підхід до кіберзагроз, наголошуючи не лише на запобіганні, але й здатності адаптуватися та відновлюватися, коли заходи безпеки не дають результатів.

Стратегія кіберстійкості життєво важлива для безперервності бізнесу. Це може надати переваги, крім підвищення рівня безпеки підприємства та зниження ризику впливу на його критичну інфраструктуру. Кіберстійкість також допомагає зменшити фінансові втрати та репутаційну шкоду. І якщо організація отримує сертифікат кіберстійкості, вона може викликати довіру у своїх клієнтів і клієнтів.

Крім того, кіберстійка компанія може оптимізувати цінність, яку вона створює для своїх клієнтів, збільшуючи свою конкурентну перевагу завдяки ефективній та ефективній діяльності. Кіберстійкість надає організаціям конкурентну перевагу перед компаніями, які її не мають [4].

Європейський Союз зробив значні кроки для підвищення кіберстійкості на регіональному рівні, визнаючи транскордонний характер кіберзагроз. Це включає імплементацію Директиви NIS, яка зобов'язує постачальників критичної інфраструктури забезпечувати мінімальний рівень кібербезпеки. У вересні 2022 року Європейський Союз прийняв Акт з Кіберстійкості (Cyber Resilience Act) [5]. Цей Регламент встановлює:

а) правила розміщення на ринку продуктів із цифровими елементами для забезпечення кібербезпеки таких продуктів;

б) основні вимоги до проектування, розробки та виробництва продуктів із цифровими елементами, а також зобов'язання суб'єктів господарювання щодо цих продуктів щодо кібербезпеки;

в) основні вимоги до процесів обробки вразливостей, які впроваджують виробники для забезпечення кібербезпеки продуктів із цифровими елементами протягом усього життєвого циклу, а також зобов'язання суб'єктів господарювання щодо цих процесів;

г) правила ринкового нагляду та забезпечення виконання вищезазначених правил і вимог.

Кіберстійкість спрямована на підтримку здатності компанії завжди доставляти товари та послуги. Це може включати можливість відновлювати штатні механізми, а також можливість постійно змінювати або модифікувати механізми при необхідності навіть після виходу з ладу штатних механізмів, наприклад, під час кризи або після порушення безпеки. При застосуванні на практиці кіберстійкість слід розглядати як превентивну міру протидії людським

помилкам і небезпечному (і апаратному) програмному забезпеченню. Таким чином, метою кіберстійкості є захист всього підприємства з урахуванням усіх вразливих компонентів інфраструктури.

Ефективна кіберстійкість має бути стратегією, заснованою на оцінці ризиків для всього підприємства, підходом до співпраці від керівників до всіх в організації, партнерів, учасників ланцюжка постачання та клієнтів. Він повинен проактивно керувати ризиками, загрозами, вразливими місцями та впливом на критичну інформацію та допоміжні активи [6].

Ефективна кіберстійкість також передбачає управління ризиками, розуміння прав власності на дані та управління інцидентами. Оцінка цих характеристик також вимагає досвіду та оцінки.

Крім того, організація також повинна збалансувати кіберризики з доступними можливостями та конкурентними перевагами. Він повинен розглянути, чи економічно ефективна профілактика є життєздатною та чи може натомість вона досягти швидкого виявлення та виправлення з хорошим короткостроковим ефектом для кіберстійкості. Для цього підприємство повинно знайти правильний баланс між трьома видами контролю: превентивним, виявленням і коригуючим. Ці засоби контролю запобігають, виявляють і усувають інциденти, які загрожують кіберстійкості організації [6].

Кіберстійкість – це постійний процес, який вимагає постійного моніторингу та оцінки ризиків.

Так, у роботі [6] пропонується процес підтримки компанією кіберстійкості з таких етапів:

– формування стратегії: Базуючись на цілях організації, стратегічна робота визначає критичні активи, такі як інформація, системи та послуги, які є найбільш важливими для неї та її зацікавлених сторін. Ця робота також включає виявлення вразливостей і ризиків, з якими вони стикаються;

– дизайн кіберзахисту: на етапі проектування системи кіберзахисту та відновлення компанії обирають відповідні та пропорційні засоби контролю, процедури та навчання для системи управління;

– операційне використання системи підтримки кіберстійкості: перевіряє засоби контролю щоб визначити, коли критичні активи перебувають під ризиком через внутрішні, зовнішні, навмисні чи випадкові дії.

– оперативна робота: контролює, виявляє та керує кіберподіями та інцидентами, включаючи постійне контрольне тестування для забезпечення ефективності, ефективності та послідовності.

– еволюція кіберстійкості: еволюційна робота постійно захищає навколишнє середовище, що постійно змінюється. Коли організації оговтуються після інцидентів, вони повинні вчитися на досвіді, змінюючи свої процедури, навчання, дизайн і навіть стратегію.

У роботі [7] автори пропонують таку структуру процесу оцінки ризиків кібербезпеки: ідентифікація усіх активів компанії; визначення пріоритетності/важливості активів; ідентифікація можливих загроз для активів; ідентифікація усіх невизначеностей у зовнішньому середовищі; оцінка вірогідності прояву загроз; проведення оцінки наслідків реалізації загроз та оцінка супровідних збитків/витрат.

На основі аналізу літературних джерел [4, 6-9] пропонується процес підтримки кіберстійкості підприємства, представлений на рисунку 1.

Етап ідентифікації пов’язаний із розвитком глибшого організаційного розуміння основних вразливостей кібербезпеки у ваших мережах, системах, людях і даних, а також ваших можливостей ІКТ.  Функція захисту полягає в розгортанні відповідних заходів кібербезпеки для забезпечення надання послуг. До них належать програми безпеки «першої лінії захисту» для запобігання, обмеження або стримування впливу потенційних загроз.

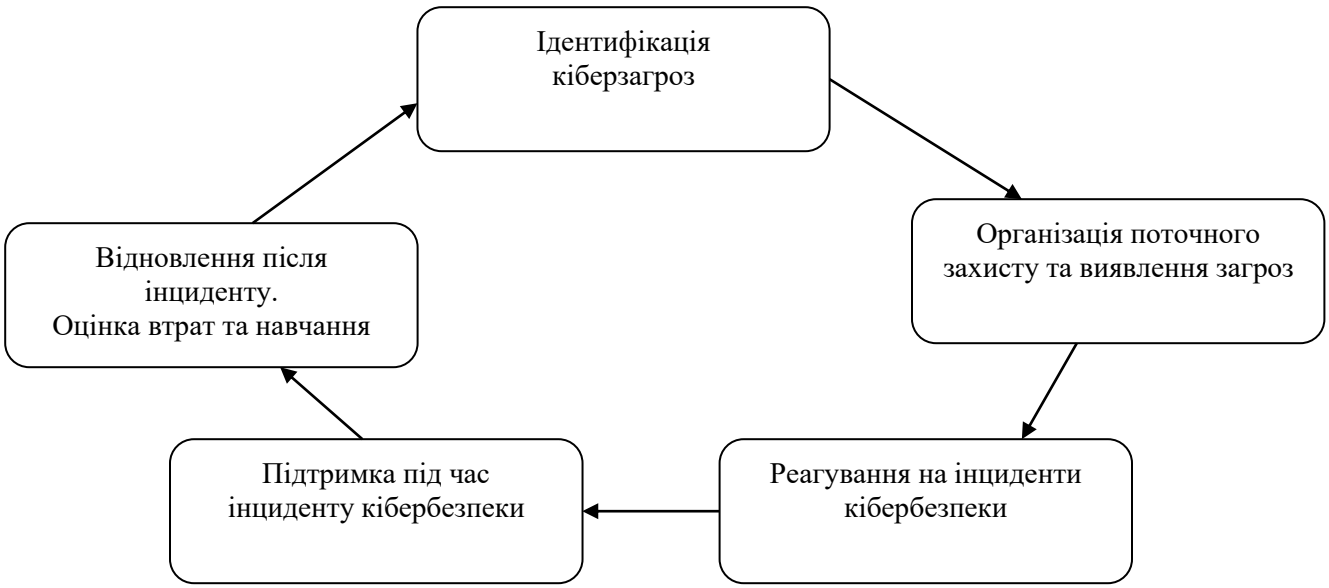


Рисунок 1 – Процес формування та підтримки кіберстійкості для підприємства

*Джерело: запропоновано авторами*

Це може включати:

– керування ідентифікацією та заходи контролю доступу, включаючи фізичний і віддалений доступ;

– заходи безпеки даних для захисту доступності, цілісності та конфіденційності конфіденційної інформації;

– постійне обслуговування, оновлення та підтримка ваших пристроїв і програмного забезпечення.

Для досягнення кіберстійкості підприємствам потрібно створити систему постійного моніторингу зовнішнього та внутрішнього кіберсередовища, а також постійного захисту даних, інфраструктури компанії. Підприємства повинні постійно оцінювати та розуміти свої ризики для кібербезпеки. Це передбачає визначення потенційних загроз, вразливостей і критичних активів, які потребують захисту. Системи безперервного моніторингу та виявлення інцидентів впроваджуються для моніторингу інцидентів у мережі й системах організації за допомогою систем виявлення вторгнень і технологій безпеки та керування

подіями (Intrusion Detection Systems and Security Information and Event Management-SIEM). Вони призначені для виявлення та попередження керівництва про аномалії, включаючи поведінку користувачів і аномальні зміни в інформації в мережах, виміряні порівняно з базовою лінією «нормальної» активності. Забезпечення резервних систем і резервних копій даних може допомогти підтримувати роботу під час і після кіберінциденту.

Працівники часто є першою лінією захисту. Інвестиції в програми навчання та підвищення обізнаності з кібербезпеки можуть допомогти в ранньому виявленні та запобіганні кіберзагрозам.

Наявність чітко визначеного плану реагування на інциденти має вирішальне значення. У ньому описано кроки, яких необхідно вжити у випадку порушення, щоб мінімізувати шкоду та час відновлення. Залежно від типу кібератаки, чим раніше компанія почне реагувати, тим менше наслідків матиме атака та вищі шанси на успішне відновлення. Швидка реакція допоможе організації продовжити роботу та повернутися до звичайного бізнесу якомога швидше та ефективніше після кібератаки чи серйозного збою.

Проте для такого швидкого реагування дуже важливий добре задокументований, відпрацьований і перевірений план реагування на інциденти.

Не менш важливою є також підтримка даних, інфраструктури та бізнес-процесів під час кібератаки. В оперативному режимі фіксуються аномалії у потоках даних, мінімізується обмін інформацією із зовнішнім середовищем, блокується робота підозрілих програм.

Останній етап спрямований на відновлення даних і послуг після кібератаки або збою до стану, що передував інциденту. В ідеалі організація матиме низку вже існуючих і перевірених планів відновлення, які є чіткими та детальними для ефективного реагування. Ці плани відновлення зазвичай включають: план

аварійного відновлення IT, план забезпечення безперервності бізнесу, план антикризового управління, план зв'язку та комунікацій.

Після завершення відновлення слід запланувати аналіз ефективності дій компанії до, під час та після інциденту кібербезпеки. Дії, отримані на основі отриманих уроків, будуть використані для подальшого вдосконалення засобів керування кібербезпекою.

У час, коли кіберзагрози є реальною та суттєвою загрозою, підприємства та організації повинні використовувати цифрові технології для зміцнення свого захисту. Цифрові інструменти, такі як сканери вразливостей і програмне забезпечення для оцінки ризиків, допомагають виявляти та пом’якшувати потенційні недоліки в системі кібербезпеки організації. В цьому дослідженні вивчаються перспективи використання цифрових технологій для підтримки кіберстійкості у таких напрямках: для виявлення загроз, для оптимізації реагування на загрози, для захисту конфіденційних даних та зниження ризиків втрати важливих даних.

Ефективне виявлення загроз є наріжним каменем кібервідмовостійкості. Різноманітні цифрові інструменти, такі як системи виявлення вторгнень (IDS) і платформи безпеки та управління подіями (SIEM), забезпечують моніторинг і оповіщення в реальному часі. Алгоритми машинного навчання та штучний інтелект все частіше використовуються для підвищення точності виявлення загроз [6].

Цифрові інструменти оптимізують реагування на інциденти та процеси відновлення. Інструменти автоматизації можуть швидко ізолювати скомпрометовані системи, локалізувати порушення та ініціювати процедури відновлення. Крім того, інструменти цифрової криміналістики допомагають у аналізі після інциденту, допомагаючи організаціям зрозуміти масштаби порушення та зменшити майбутні ризики.

Зі зростанням віддаленої роботи інструменти безпечного зв’язку та співпраці мають вирішальне значення для підтримки кіберстійкості. Наскрізне шифрування, захищені платформи для відеоконференцій і зашифровані програми обміну повідомленнями гарантують захист конфіденційних даних під час віддаленої взаємодії.

Дані є основною мішенню для кіберзлочинців. Надійні рішення для резервного копіювання та відновлення даних, як локальні, так і хмарні, незамінні для забезпечення доступності даних навіть після кіберінциденту. Цифрові інструменти спрощують процеси резервного копіювання та відновлення даних.

Основним аспектом кіберстійкості є навчання співробітників кіберзагрозам і найкращим практикам. Цифрові інструменти, зокрема платформи електронного навчання та гейміфіковані навчальні модулі, роблять навчання з питань кібербезпеки доступним і цікавим.

Спільні зусилля щодо обміну інформацією про загрози стали найважливішими для організацій. Цифрові платформи сприяють обміну інформацією про нові загрози та вразливості, надаючи можливість організаціям проактивно захищатися від потенційних атак.

На основі аналізу літературних джерел [1, 3, 4, 6-9] у роботі систематизовано цифрові інструменти для підтримки кіберстійкості підприємства та протидії кіберзагрозам (таблиця 1).

Таким чином, у все більш оцифрованому та взаємопов’язаному світі підприємства повинні віддавати пріоритет кіберстійкості як фундаментальному компоненту своєї стратегії економічної безпеки. Вартість кібератак і потенціал збою в роботі є значними. Таким чином, проактивний, адаптивний і стійкий підхід до кібербезпеки є важливим для захисту економічних інтересів сучасного бізнесу.

У цифровому світі кіберстійкість є не розкішшю, а необхідністю. Цифрові інструменти пропонують низку можливостей для підвищення здатності організації

протистояти кіберзагрозам. Ці інструменти дають організаціям змогу виявляти інциденти, реагувати на них і відновлюватися після них, одночасно зміцнюючи свою економічну безпеку.

Таблиця 1 – Цифрові інструменти для підтримки кіберстійкості підприємства та протидії кіберзагрозам

| Цифрові технологій | Напрям використання для підтримки кіберстійкості |
|---|---|
| Аналіз великих даних | Контент-аналіз відкритих публікацій та соціальних мереж для протидії розповсюдженню дезінформації<br>Аналіз незвичної поведінки контрагентів та конкурентів |
| Штучний інтелект, машинне навчання | Виявлення багатоканальних атак для інформаційної безпеки<br>Динамічне виявлення онлайн-фішингових електронних листів нульового дня<br>Створення бази знань щодо реакцій на кіберзагрози |
| Інтернет речей (IoT) | Апаратура для кіберзахисту (вважається більш надійним, ніж програмний захист)<br>Збір та керування даними датчиків, контроль та моніторинг виробничої інфраструктури<br>Медіа-спостереження із забезпеченням конфіденційності користувачів, безпеки медіа-ресурсів та вимог до пам’яті вузла-датчика |
| Криптологія | Ідентифікація користувачів<br>Захист даних та інформації |
| Нейроні мережі та пошук даних (Data mining) | Виявлення та класифікація кібератак<br>Ідентифікація користувачів |
| Хмарні обчислення | Покращуюсь використання IoT<br>Скорочення часу реакції у випадку гібридної атаки |
| Smart-контракти з використанням технології Blockchain | Мінімізація ризику, що стосується третіх осіб – розумний контракт реалізується автоматично при настанні події, незалежно від дій контрагентів. |

*Джерело: сформовано авторами*

Цифрові технології, від штучного інтелекту та машинного навчання до надійних заходів кібербезпеки та аналізу великих даних, стали головними захисниками від цих багатогранних загроз. Щоб процвітати в епоху цифрових технологій, підприємства та установи повинні використовувати ці інструменти як невід’ємні компоненти своїх стратегій кіберстійкості.

## Перелік джерел посилання

1. Cisco Company. Cyber security threat trends: phishing, crypto top of list. URL: https://learn-cloudsecurity.cisco.com/umbrella-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list (дата звернення 20.10.2023).

2. World Economic Forum For the public sector, cyber resilience has never been more important. URL: https://www.weforum.org/agenda/2022/07/how-do-you-safeguard-a-city-from-cyber-attacks/ (дата звернення 20.10.2023).

3. European Cyber Security Agency (ENISA) Threat landscape 2023. October 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

4. How and why digital transformation needs cyber resilience URL: https://www.i-scoop.eu/digital-transformation/digital-transformation-cyber-resilience/ (дата звернення 20.10.2023).

5. European Council European Cyber-Resilience Act. URL: https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Articles_ (Proposal_15.9.2022).html (дата звернення 24.10.2023).

6. IBM Company What is Cyber Resilience? URL: https://www.ibm.com/topics/cyber-resilience (дата звернення 26.10.2023)

7. Knowles M. Cybersecurity Risk Management: Frameworks, Plans, & Best Practices URL: https://hyperproof.io/resource/cybersecurity-risk-management-process/ (дата звернення 28.10.2023).

8. Hausken K. Cyber resilience in firms, organizations and societies. *Internet of Things*. 2020. Volume 11. https://doi.org/10.1016/j.iot.2020.100204.

9. Achieving Cyber Resilience: A New Framework URL: https://inconsult.com.au/publication/achieving-cyber-resilience/ (дата звернення 28.10.2023).