

3. IBM Security. *IBM X-Force threat intelligence index 2024*.
<https://www.ibm.com/reports/threat-intelligence>

4. Wang, H., Yang, Y., & Yang, W. (2018). Big data management and analytics: A survey. *IEEE Transactions on Knowledge and Data Engineering*, 30(6), 1000-1019.
<https://doi.org/10.1109/TKDE.2018.2800984>.

Ярич І.Я.,

методист, викладач,

Державний навчальний заклад «Вище професійне училище №34 м.Стрий»

КІБЕРБЕЗПЕКОВА СТРАТЕГІЯ ПІДПРИЄМСТВА В УМОВАХ ВОЄННОГО ЧАСУ ТА ПОВОЄННОГО ВІДНОВЛЕННЯ УКРАЇНИ

У контексті воєнної агресії росії проти України та масштабного переходу на цифрові інфраструктури, питання кібербезпеки набуло особливої актуальності. Підприємства стають мішенню кібератак, що мають на меті дестабілізацію, викрадення даних, знищення інфраструктури. У післявоєнний період, коли почнеться активне економічне відновлення, ризики залишатимуться високими. Ефективне забезпечення кібербезпеки на підприємствах потребує комплексного вирішення та вимагає скоординованих дій на національному, регіональному і міжнародному рівнях [3].

Ключовими аспектами кібербезпеки підприємств є захист критичної інфраструктури, резервне копіювання і відновлення даних, навчання персоналу, впровадження сучасних технологій захисту, співпраця з державними і міжнародними організаціями. Повоєнне відновлення України потребуватиме комплексного підходу до кібербезпеки, щоб забезпечити стабільність економіки та захистити підприємства від нових викликів [2].

Заходами кібербезпеки, які можуть бути застосовані підприємствами для захисту своїх даних та мінімізації ризиків кібератак є:

- фішинг-атаки та їх запобігання: навчання персоналу розпізнаванню фішингових листів та підозрілих посилань, що допоможе уникнути витоку конфіденційної інформації;

- програми-вимагачі: використання сучасного антивірусного програмного забезпечення та регулярне резервне копіювання даних, що допоможе захиститися від атак, які блокують доступ до інформації та вимагають викуп;
- двофакторна автентифікація: впровадження додаткового рівня захисту для входу в корпоративну систему значно знижує ризик несанкціонованого доступу;
- моніторинг загроз: використання спеціалізованих систем для виявлення аномальної активності в мережі, що дозволяє оперативно реагувати на потенційні загрози;
- шифрування даних: застосування сучасних методів шифрування гарантує, що навіть у разі витоку інформації вона залишиться недоступною для злоумисників.

Впровадження заходів кібербезпеки на підприємстві потребує комплексного підходу, що включає оцінку ризиків, політику безпеки, навчання персоналу, використання сучасних технологій, резервне копіювання, співпрацю з експертами [4].

Ефективна кібербезпекова стратегія підприємства повинна бути всебічною та інтегрованою у всі аспекти його діяльності [1]:

- починається з детальної оцінки ризиків, що дозволяє виявити наявні кіберзагрози та найбільш вразливі місця в інфраструктурі підприємства, цей процес забезпечує ідентифікацію критично важливих активів таких, як дані конфіденційності, ключові інформаційні системи та комунікаційні канали, які потребують найвищого рівня захисту;
- розроблення та впровадження чіткої політики та процедур, які регулюють усі аспекти кібербезпеки на підприємстві: правила щодо доступу до інформаційних ресурсів, використання мобільних пристроїв, створення та управління паролями, встановлення процедур реагування на інциденти, політики безпеки мають бути зрозумілими для всього персоналу та регулярно оновлюватися відповідно до змін у технологічному середовищі;
- використання сучасних технологічних рішень для захисту від кібератак: антивірусні програми, фаєрволі, системи виявлення та запобігання вторгненню,

шифрування даних, регулярне оновлення програмного забезпечення і системи безпеки є критичними місцями для захисту від нових загроз;

- регулярне навчання персоналу щодо обізнаності кіберзагроз та правильній їх поведінці в разі виявлення деяких небезпек, людський фактор є найслабшою ланкою в системі кібербезпеки, тому навчання має стати невіддільною частиною корпоративної культури підприємства.

Цілями кібербезпекової стратегії підприємства є безперервність роботи, захист критичної інформації, швидке виявлення і реагування на інциденти, відновлення ІТ-інфраструктури після атак, навчання персоналу з питань кібергігієни, дотримання законодавства України та міжнародних норм [5].

Підходи до впровадження кібербезпекової стратегії підприємства в умовах обмежених ресурсів включають партнерство з державою та міжнародними організаціями (наприклад, НБУ, USAID, НАТО), використання хмарних сервісів з високим рівнем безпеки, open-source рішення щодо підтримки кібербезпеки, спільні ініціативи на рівні галузі (CERT-UA, ISAC).

Специфіка впровадження кібербезпекової стратегії підприємства для повоєнного періоду включає інтеграцію кібербезпеки в проекти відбудови (Smart Cities, e-Government), розробку національних стандартів з кібербезпеки підприємств, стимулювання локального виробництва безпечного ПЗ, створення кадрів з підтримки ІТ-освіти та сертифікації (CISSP, CEN, CISM).

Ефективна кібербезпекова стратегія повинна бути багаторівневою, включати оцінку ризиків, розробку політики і процедур, впровадження технологічних рішень та навчання персоналу. Це дозволить захистити підприємство від кіберзагроз та мінімізувати деякі ризики для бізнесу. Кібербезпека повинна стати ключовим компонентом стратегічного планування кожного підприємства в Україні, яке має адаптуватися до гібридних загроз, виходячи з досвіду війни. Гнучкість, адаптивність та партнерство – основа кіберстійкості в повоєнний період.

Список використаних джерел

1. Дія. Бізнес. (2024). *Що таке кібербезпека для бізнесу?*
https://business.diia.gov.ua/entrepreneur-handbook/item/scho_take_kiberbezpeka_dlya_biznesu
2. Національний інститут стратегічних досліджень. (2022). *Концепція стратегії повоєнного відновлення та розвитку України.*
<https://niss.gov.ua/sites/default/files/2022-05/stratvidnovlennya-koncept-v2.pdf>
3. Кузьменко, О., Маклюк, О., & Чернишова, О. (2022). Кібербезпека бізнесу під час війни. *Економіка та суспільство*, (44).
<https://doi.org/10.32782/2524-0072/2022-44-21>
4. Мінфін. (2025). *Кібербезпека бізнесу під час війни.*
<https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny>
5. Westelecom. (2024). *Основи кібербезпеки для бізнесу.*
<https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa>

Чаркіна Т. Ю.,
д.е.н., професор,
Очкасов О.Б.,
к.т.н, доцент,
Залеський О. В.,
здобувач третього (наукового) рівня вищої освіти,
Український державний університет науки і технологій, м. Дніпро

НАПРЯМКИ РОЗВИТКУ ПЕРСОНАЛУ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

Зараз цифровізація стала основною рушійною силою трансформацій у різних сферах економіки, і транспортна галузь не стала винятком. Світові тенденції вказують на стрімке впровадження цифрових технологій у всі рівні транспортного процесу — від логістики та управління рухом до обслуговування клієнтів і управління персоналом. Ці зміни зумовлюють