УДК 65.012.32:339.9(4-672ЄС)

Цимбалюк Сергій,
к.е.н., доцент кафедри економіки та менеджменту,
Волинський інститут ім. В. Липинського ПрАТ «ВНЗ «МАУП»,
м. Луцьк, Україна
Tsymbaliuks@ukr.net

ЄВРОПЕЙСЬКА ПРАКТИКА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БІЗНЕСУ

Кібербезпека стала критичною проблемою для компаній у всьому світі, оскільки частота та складність кібератак продовжують зростати. Країни Європейського Союзу (ЄС) знаходяться в авангарді боротьби з цією зростаючою загрозою, розробляючи комплексні стратегії та ініціативи для захисту бізнесу від кіберзагроз.

Одним із ключових аспектів підходу ЄС до кібербезпеки для бізнесу є розробка надійної правової та нормативної бази. Країни-члени ЄС запровадили різноманітні директиви та нормативні акти, спрямовані на підвищення рівня кібербезпеки компаній, що працюють у ЄС. Наприклад, Загальний регламент захисту даних (GDPR), який набув чинності в 2018 році, містить положення, пов’язані з безпекою даних і повідомленнями про порушення, накладаючи на підприємства значні зобов’язання щодо захисту персональних даних громадян ЄС. Відтепер, компанії, що обробляють персональні дані осіб, які проживають в ЄС, незалежно від місця реєстрації підприємства, зобов’язані дотримуватися суворих правил GDPR. Це стосується як персональних даних клієнтів, так і даних їх кінцевих замовників та працівників.

Основними змінами, які GDPR вносять у сферу кібербезпеки бізнесу, є [1]:

- гармонізація нормативної в області захисту персональних даних на території всього ЄС, що базується на веденні компаній транснаціональної діяльності.
- адаптація законодавства до сучасних технологічних реалій, що забезпечує більш ефективний захист даних в умовах швидкого розвитку цифрових технологій.
- посилення прав громадян на захист їхніх персональних даних, що змушує бізнес вдосконалювати системи кібербезпеки для забезпечення конфіденційності інформації.
- збільшення відповідальності та обов'язків компаній у сфері обробки та зберігання персональних даних, що вимагає від підприємств впровадження більш жорстких заходів безпеки.
- вимоги до документування процесів обробки даних та контролю за їх відповідністю регламенту, що забезпечує більшу прозорість і можливість перевірки дотримання норм GDPR.
- запровадження принципу прозорості у використанні персональних даних, зобов'язуючі компанії чітко інформують осіб про цілі, методи обробки та суб'єкти, які мають доступ до своїх даних.

Зусилля ЄС зосереджені на створенні єдиної політики безпеки в кіберпросторі, що призвело до розробки та публікації оновленої Стратегії кібербезпеки ЄС 16 грудня 2020 року [2]. Основні цілі цієї стратегії включають зміцнення захисту критично важливих інфраструктур та ефективну відповідь на масштабні кібератаки ззовні. Важливим аспектом є підвищення загальної кібербезпеки, а також забезпечення доступу до безпечних цифрових послуг та інструментів для всіх громадян та бізнес-структур у ЄС. Особлива увага приділяється захисту електронних мереж, фінансових установ, транспортних систем, медичних закладів та державних органів від будь-яких кіберзагроз і ризиків. В цьому контексті Єврокомісія запропонувала створити мережу центрів кібербезпеки по всій ЄС, які використовуючи передові технології, включаючи штучний інтелект, допоможуть створити ефективний захисний бар'єр проти кібератак.

Запропонована система має на меті раннє виявлення кібератак та розробку стратегій для їх запобігання, виявлення та нейтралізації.

З 16 січня 2023 року вступила в силу Директива про мережеву та інформаційну безпеку NIS 2 (the security of network and information systems)[3], спрямована на покращення стану кібербезпеки у ЄС. Вона визначає рамки управління кіберкризами, встановлює вищий рівень стандартів безпеки та однакових вимог до звітування у всіх секторах, які підпадають під її дію. Директива вимагає від компаній впровадження конкретних заходів інформаційної безпеки і надання докладних звітів про будь-які інциденти. Неспроможність компаній дотримуватися цих положень може призвести до високих штрафів, особливо у великих організаціях, де максимальний штраф може сягати мінімум 7 мільйонів євро або 1,4% від загального річного обороту. Держави-члени мають право накладати різні санкції на організації, що порушують умови Директиви NIS 2, включаючи призупинення або анулювання ліцензій та дозволів. Недотримання цих вимог також може призвести до репутаційних втрат, зниження довіри клієнтів, партнерів та інвесторів.

Для підвищення кібербезпеки бізнесу країни ЄС здійснюють активну політику просування державно-приватного партнерства. Співпраця між урядовими установами, галузевими організаціями та приватними підприємствами відіграла важливу роль у обміні інформацією про загрози, найкращими практиками та ресурсами для захисту від кібератак. Агентство ЄС з кібербезпеки (ENISA) відіграє суттєву роль у сприянні співпраці між державами-членами ЄС, пропонуючи вказівки та підтримку підприємствам для покращення їхніх можливостей у сфері кібербезпеки [4]. Крім того, такі ініціативи, як Європейська організація з кібербезпеки (ECSO), об’єднують зацікавлених сторін галузі для стимулювання інновацій та інвестицій у технології та рішення кібербезпеки.

Європейська організація з кібербезпеки (ECSO) представляє собою міжсекторальну організацію в Європі, що допомагає культивувати спільноти у сфері кібербезпеки та сприяє створенню

європейської інфраструктури кібербезпеки. Вона інтегрує зусилля як державного, так і приватного секторів у галузі кібербезпеки Європи, включаючи великі корпорації, малі та середні підприємства, стартапи, науково-дослідні інститути, вищі навчальні заклади, користувачів і постачальників критично важливих послуг, а також об'єднання і асоціації. ECSO співпрацює з муніципальними, регіональними та національними урядовими структурами членів Європейського Союзу та країнами Європейської асоціації вільної торгівлі (ЄАВТ) [5; 6-8].

ЄС приймає заходи для швидкого реагування на сучасні виклики та загрози в інформаційному просторі, впроваджуючи на національному рівні принципи управління ризиками, при цьому наголошуючи на цифрових правах та свободах громадян як на найвищій цінності.

Крім регуляторних заходів і спільних зусиль, країни ЄС віддають пріоритет обізнаності з кібербезпеки та розвитку навичок для бізнесу. Визнаючи людський фактор як значну вразливість у кібербезпеці, багато держав-членів ЄС запровадили інформаційні кампанії, навчальні програми та освітні ініціативи, щоб озброїти бізнес знаннями та навичками для зменшення кіберризиків. Пропагуючи культуру обізнаності та гігієни щодо кібербезпеки, компанії можуть краще розуміти мінливий ландшафт загроз і вживати проактивних заходів для захисту своїх цифрових активів і операцій [9; 10].

Іншим помітним аспектом досвіду ЄС у сфері кібербезпеки для бізнесу є зосередженість на стійкості та реагуванні на інциденти. Країни ЄС підкреслили необхідність для компаній розробляти плани реагування на інциденти, проводити регулярні оцінки кібербезпеки та впроваджувати заходи стійкості для забезпечення безперервності бізнесу в разі кібератаки. Створення Груп реагування на інциденти комп'ютерної безпеки (CSIRT) і національних центрів кібербезпеки надає підприємствам доступ до досвіду, підтримки та координації у

реагуванні на інциденти кібербезпеки, тим самим підвищуючи їх готовність і можливості реагування.

Крім того, ЄС був активним у просуванні міжнародного співробітництва та стандартизації кібербезпеки для бізнесу. Взаємодіючи з глобальними партнерами та міжнародними організаціями, країни ЄС працюють над гармонізацією стандартів кібербезпеки, просуванням транскордонного обміну інформацією та просуванням розвитку норм кібербезпеки та найкращих практик на міжнародному рівні. Приєднавшись до глобальних зусиль, компанії, які працюють у країнах ЄС, можуть отримати вигоду від більш згуртованого та послідовного підходу до кібербезпеки, особливо в контексті все більш взаємопов'язаної та взаємозалежної цифрової екосистеми.

Варто зазначити, що досвід країн ЄС у сфері кібербезпеки для бізнесу демонструє комплексний та багатогранний підхід до вирішення кіберзагроз, що розвиваються, з якими стикається бізнес. Завдяки поєднанню нормативно-правової бази, співробітництва між державним і приватним секторами, підвищення обізнаності та навичок, стійкості та реагування на інциденти, а також міжнародної участі, країни ЄС створили міцну основу для бізнесу, щоб посилити свої можливості та стійкість до кібербезпеки. Оскільки компанії продовжують орієнтуватися в складному та динамічному ландшафті кібербезпеки, досвід країн ЄС пропонує цінну інформацію та стратегії, які можуть слугувати еталоном для вдосконалення практики кібербезпеки в усьому світі.

Список використаних джерел:

1. Загальний регламент захисту даних (GDPR). 2021. URL: https://www.globallogic.com/ua/gdpr/

2. New EU Cybersecuritu Strategy. URL: https://ec.europa.eu/commission/presscorner/detail/ en/IP_20_2391

3. Директива кібербезпеки NIS 2. 2023. URL: https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua

4. ENISA. 2023. URL: https://www.enisa.europa.eu/about-enisa/regulatory-framework

5. ECSO is a proud partner of the European Institutions. 2023. URL: https://ecs-org.eu/

6. Павліха Н. В., Войчук М. В. Концептуальні засади безпеки сталого просторового розвитку: теоретико-методологічний аспект. *Міжнародна економічна безпека України: теорія, методологія, практика.* Колективна практика / за наук. ред. Кравчука П.Я. – Луцьк: ІВВ Луцького НТУ, 2020. 212 с. С. 161-183.

7. Павліха Н. В., Коляда О.М. Особливості впливу зони вільної торгівлі між Україною та ЄС на основні компоненти економічної безпеки України Розділ у монографії. Європейська інтеграція: досвід Польщі та України / Луцьк Люблін: „Drukarnia Kolor Lublin", 2013. С.453- 459.

8. Цимбалюк І. О. Інформаційна безпека підприємства: сучасні реалії та загрози. Теорія та практика менеджменту безпеки: матеріали Міжнар. наук.-практ. конф. (18 травня 2017 р.) / Відп. ред. проф. Л. М. Черчик. Луцьк, 2017. С. 118-119.

9. Інноваційні форми єврорегіонального співробітництва: концептуальні засади та механізми активізації [Текст] : монографія / Наталія Володимирівна Павліха, Ірина Олександрівна Цимбалюк, Ольга Антонівна Корнелюк, Юлія Віталіївна Петришина. Луцьк : ВНУ імені ЛесіУкраїнки, 2022. 214 с.

10. Кузнєцов О. М. Європейський досвід посилення спроможностей у сфері забезпечення кібербезпеки в сучасних умовах. *Інформація і право*. 2021. № 1(36). С. 106-113.

11. Павліха Н., Науменко Н., Корнелюк О. Розвиток та регулювання штучного інтелекту в Україні у воєнний та повоєнний періоди: сучасні тенденції та перспективи. *Цифрова економіка та економічна безпека*, 2023. № 8 (08). С. 105-111.