DOI: https://doi.org/10.36059/978-966-397-336-4-51

КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА ФІНАНСОВІЙ БЕЗПЕЦІ ДЕРЖАВИ ТА СУБ'ЄКТІВ ПІДПРИЄМНИЦТВА В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

Яструбецька Леся Сергіївна
доктор економічних наук,
професор кафедри фінансів, грошового обігу і кредиту
Львівського національного університету імені Івана Франка
Кузін Галина Ігорівна
здобувач першого (бакалаврського) рівня вищої освіти
Львівського національного університету імені Івана Франка

Вступ. Складність геополітичних процесів та стрімкі темпи цифровізації економіки зумовлюють виникнення й поширення конфліктів нового типу – гібридних. Загрози, спричинені ними, є проблемою як для національної безпеки окремих держав й суб'єктів господарювання, так і для глобальної безпеки в цілому, оскільки деструктивні наслідки їх впливу охоплюють усі сфери життєдіяльності суспільства – політичні, соціальні, інформаційні, технологічні, економічні тощо.

Серед гібридних інструментів особливу небезпеку становлять інформаційні, оскільки швидкість їх еволюції становить суттєві труднощі для розроблення своєчасних й адекватних заходів реагування. Відтак, ці гібридні важелі впливу потребують ретельного аналізу з метою оновлення теоретико-методичних й прикладних засад їхнього попередження, нейтралізації та протидії.

Питаннями цифровізації економіки, в тому числі вивченням таких супутніх негативних наслідків, як кіберзлочинність, а також оцінкою її впливу на фінансову безпеку суб'єктів господарювання займались такі вітчизняні і зарубіжні науковці, як З. Варналій, С. Вітер, А. Мехед, І. Світлишин, О. Підхомний, Г. П'ятницька та інші. Однак, чимало аспектів цієї складної проблематики ще потребують поглибленого аналізу, уточнення й доповнення.

Метою дослідження є обґрунтування необхідності формування системи кібер-захисту в інформаційному просторі в контексті зміцнення фінансової безпеки суб'єктів господарювання та держави й визначення ефективних заходів щодо запобігання кібератакам у підприємницькій діяльності.

Результати. Цифрова трансформація створює нові можливості для здійснення фінансово-господарської діяльності суб'єктів господарювання та генерує додаткові важелі управління підприємствами, однак, своєю чергою, може зумовлювати також появу викликів і загроз їхньому подальшому розвитку у формі кібератак, вчинюваних зловмисниками.

Кібератаки – це комп'ютерні або мережеві атаки, спрямовані на інформаційні системи, інфраструктуру або ресурси підприємства з метою завдання шкоди, крадіжки конфіденційної інформації, перешкоджання нормальному функціонуванню або отримання фінансової вигоди [3]. Відтак, в сучасних умовах винятково важливого значення набуває кібер-безпека, оскільки на сьогодні практично неможливо уявити жоден об'єкт технологічної інфраструктури, який не був би оснащений різними програмними комплексами, багато з яких мають вихід у мережу Інтернет, що несе значні ризики для їхнього функціонування в зв'язку з наявністю таких характеристик [2]:

– інформаційна відкритість, яка спричиняє вразливість щодо шкідливих впливів і кібератак й може погіршити конкурентоспроможність підприємств, оскільки їх конфіденційну інформацію може бути використано недобросовісними конкурентами;

– наявність ризиків збою програмного забезпечення (повна або часткова втрата даних у разі помилок у програмному забезпеченні, втрата інформації унаслідок зараження системи комп'ютерними вірусами тощо), які можуть стати причиною неналежного функціонування виробничих ліній й унеможливити виконання зобов'язань перед контрагентами;

– зловмисність дій сторонніх осіб (несанкціоноване копіювання, знищення, підроблення або блокування інформації, порушення роботи комп'ютерної системи, спричинення витоку даних);

– необхідність підвищення вимог до кваліфікації персоналу, що зумовлюється причинами технологічного ускладнення виробничих процесів.

Кібератаки, вчинювані зловмисниками у корпоративному секторі, набули значних масштабів і темпів здійснення й призводять до значних фінансових, репутаційних й правових наслідків для суб'єктів господарювання. Водночас, об'єктами агресивних дій на сьогодні є також державні установи. Зокрема, в 2017 році було вчинено низку кібератак вірусами WannaCry та Petya.A (згодом – NotPetya) на світові сервери та комп'ютерні системи окремих країн і підприємств. Найбільш уразливими виявились українські суб'єкти підприємництва й державні установи, серед яких – уряд України, національна пошта, метрополітен Києва, Чорнобильська АЕС, міжнародний аеропорт «Бориспіль», а також низка інших комерційних структур, ЗМІ, банків [4].

Відтак, перед органами державної влади, суб'єктами господарювання та кожним громадянином українського суспільства, зокрема, постає необхідність дотримання правил інформаційної безпеки з метою убезпечення від можливих кібер-загроз.

В контексті зміцнення інформаційної безпеки на рівні підприємств можна виокремити низку таких заходів протидії кібер-ризикам (див. рис. 1).

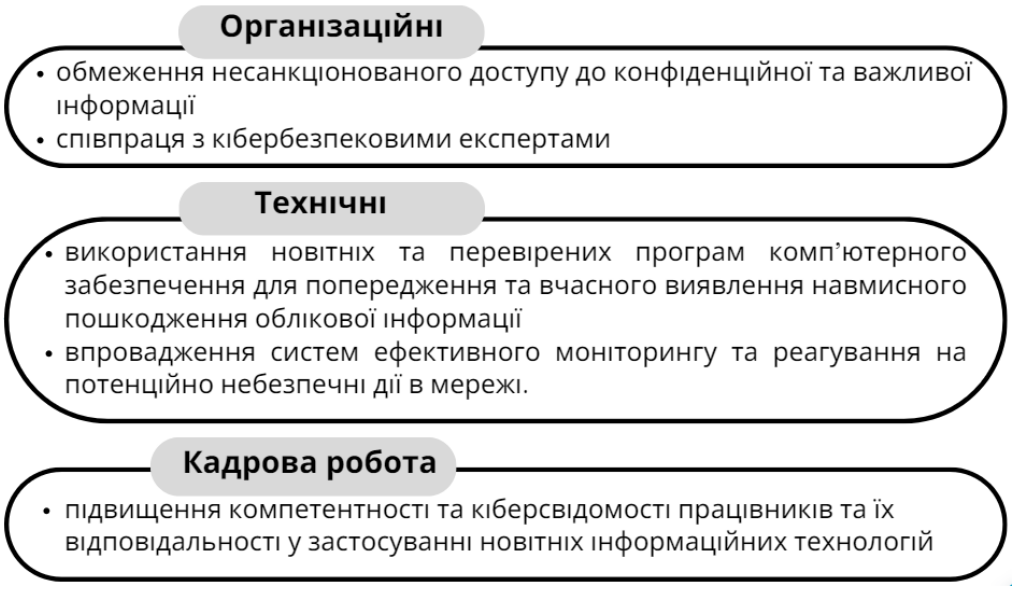

Рис. 1. Заходи протидії кібер-ризикам на підприємстві

Джерело: сформовано на основі [1; 2]

Застосування пропонованих заходів організаційного характеру дасть змогу власникам та керівництву суб'єктів підприємництва значно знизити ризик кібератак й забезпечити захист конфіденційної інформації від недобросовісних дій інших учасників ринку. Крім цього, важливе значення в боротьбі з кіберзлочинністю має державна політика у цій сфері, зокрема розроблення й прийняття законодавчих ініціатив щодо зміцнення інформаційної безпеки держави і ділових одиниць та підвищення ефективності роботи уповноважених органів державної влади щодо захисту інформаційно-технічної інфраструктури країни й фінансово-економічних процесів суб'єктів господарювання від кібернетичних загроз.

Висновки. Формування ефективної політики інформаційної безпеки на національному рівні та стратегій інформаційного захисту на рівні індивідуальних підприємств, а також міжнародне співробітництво в галузі кібер-безпеки сприятимуть протидії загрозам нового типу та нівелюванню їх деструктивного впливу на фінансову безпеку окремих суб'єктів підприємництва та держави загалом.

Список використаних джерел:

1. Вітер С.А., Світлишин І.І. Захист облікової інформації та кібербезпека підприємства. *Економіка та суспільство.* 2017. № 11. С. 497–502. URL: https://economyandsociety.in.ua/journals/11_ukr/80.pdf (дата звернення: 15.11.2023).

2. Мехед А.М., Варналій З.С. Фінансова безпека підприємств в умовах цифрової економіки. *Вісник університету банківської справи.* 2021. № 3 (42). С. 55–61.

3. Найпопулярніші види кібератак у 2021 році. URL: https://10guards.com/ua/articles/the-most-common-types-of-cyber-attacks-in-2021/ (дата звернення: 12.11.2023).

4. Рік після атаки вірусу Petya: що змінилось в кібер-безпеці України. URL: https://www.radiosvoboda.org/a/29336511.html (дата звернення: 20.11.2023).