Технічні науки

Огірко Ольга Ігорівна
кандидат технічних наук,
доцент кафедри економіки та економічної безпеки
Львівський державний університет внутрішніх справ

Кос Вікторія Романівна
здобувач вищої освіти освітнього ступеня бакалавр
факультету управління та економічної безпеки
Львівського державного університету внутрішніх справ

Чорній Світлана Сергіївна
здобувач вищої освіти освітнього ступеня бакалавр
факультету управління та економічної безпеки
Львівського державного університету внутрішніх справ

ДІАГНОСТИКА СУЧАСНИХ ЗАГРОЗ ТА КІБЕР-РИЗИКІВ ПІДПРИЄМСТВ

Анотація. *У статті досліджено особливості трактування кібербезпеки. Праведно аналіз сучасних загроз та кібер-ризиків, виявлено динаміку росту кібер-злочинів та збитків від них. Розроблено модель управління кібер-ризиками на підприємстві.*

Ключові слова: *кібербезпека, економічні злочини, кібер-злочини, кібер-ризики.*

Поставка проблеми. Використання сучасних технологій дає підприємствам великі можливості в розповсюдженні та передачі інформації, дозволяє виконувати фінансові, банківські операції, операції купівлі-продажу незважаючи на відстані та кордони. З одної сторони використання інформаційних технологій, значно підвищує ефективність процесів, проте

збільшується число комп'ютерних злочинів, які можуть завдати підприємствам як фінансових, так і інформаційних втрат. Тому забезпеченню кібербезпеки приділяється все більше уваги в різних країнах світу.

Аналіз останніх досліджень і публікацій. Кібербезпека є об'єктом дослідження відомих вітчизняних учених, таких як: В. Бурячок, Д. Дубов, О. Ткаченко, С. Мельник, В. Толубко, В. Хорошко та ін.

В. Л. Бурячок, В. Б. Толубко та В. О. Хорошко трактують кібербезпеку як стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, нейтралізація викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [1].

На думку Олександра Ткаченка під кібербезпекою розуміється стан захищеності кіберпростору держави та окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, при якому порушується їхня стабільність чи сталий розвиток, своєчасне виявлення, запобігання та відповідна нейтралізація реальних і потенційних викликів (кібервтручань, кіберзагроз, кіберзлочинів) реальним особистим, корпоративним, інституціальним інтересам [2].

Враховуючи викладене, **метою статті** є дослідження кібербезпеки підприємств, а саме сучасних загроз пов'язаних з використанням сучасних інформаційних технологій та кібер-ризиків.

Виклад основного матеріалу. За законом України «Про основні засади забезпечення кібербезпеки України», кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного

середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [1].

Як одну із складових економічної безпеки підприємств, кібербезпеку можна розглядати, як процес ефективного використання програмно-інформаційного забезпечення в організації управлінні, безпечної передачі інформації для зниження ризиків, пов'язаних з порушенням інтелектуальної власності, та своєчасного виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз інтересам підприємства [1-3].

На сьогодні в Україні одним із найпоширеніших економічних загроз є кіберзлочини, які відбуваються за допомогою комп'ютерних і телекомунікаційних технологій, кількість яких щороку зростає (рис.1).

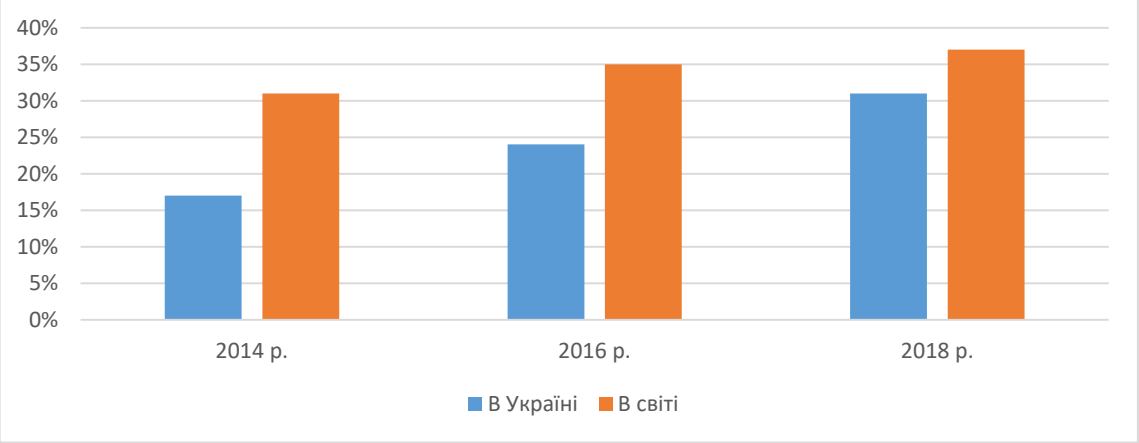

Рис. 1. Кіберзлочинність в Україні та світі

Джерело: сформовано авторами на основі [4; 5].

До таких злочинів відносять розповсюдження комп'ютерних вірусів, шахрайства з платіжними картками, крадіжки грошей з банківських рахунків, викрадення інформації (рис 2).

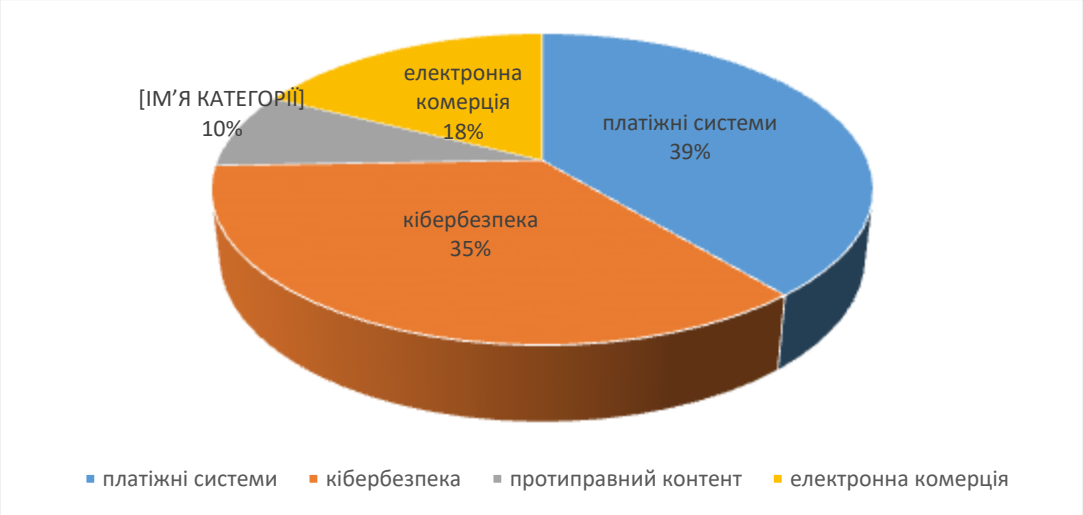

Рис. 2. Викрито кіберзлочинів в Україні у 2019 році

Джерело: сформовано авторами на основі [6].

У 2019 році кіберзлочинами в Україні завдано збитків на суму 28 млн. грн. і тільки 60% відшкодовано [6]. Як бачимо, це реальна загроза, яка може надходити з будь-якої країни світу і виходити за межі конкретної юрисдикції на відміну від багатьох інших традиційних видів економічних загроз підприємствам.

До основних джерел загроз кібербезпеки підприємств відносять такі [1; 2; 7; 9]:

✓ протизаконна діяльність деяких структур у сфері формування, поширення і використання інформації;

✓ порушення встановлених регламентів збору, обробки та передачі інформації;

✓ навмисні дії та ненавмисні помилки користувачів інформаційних систем;

✓ локальних та віддалених атак на ресурси інформаційної системи;

✓ помилки в проектуванні інформаційних систем;

✓ збій в роботі інформаційної системи, викликаних помилками в програмному забезпеченні або технічній несправності.

Дослідити кібербезпеку підприємства допомагає аналізу ризиків. Такий аналіз повинен розпочинатися з заходів щодо обстеження безпеки інформаційної системи з метою визначення того, які ресурси і від яких загроз потрібно захищати, і наскільки ресурси мають потребу в захисті. Виявлення ризиків допоможе організувати роботу фахівців, виходячи з природи і небезпеки загроз. Моніторинг аналізу ризиків є ефективним засобом контролю загроз кібербезпеки підприємств.

Управління ризиками складається з оцінки масштабів ризиків та виробленні ефективних, економічно виправданих заходів для зменшення їх масштабів.

Модель управління кібер-ризиками, які сьогодні виникають на підприємствах показана на рис. 3.

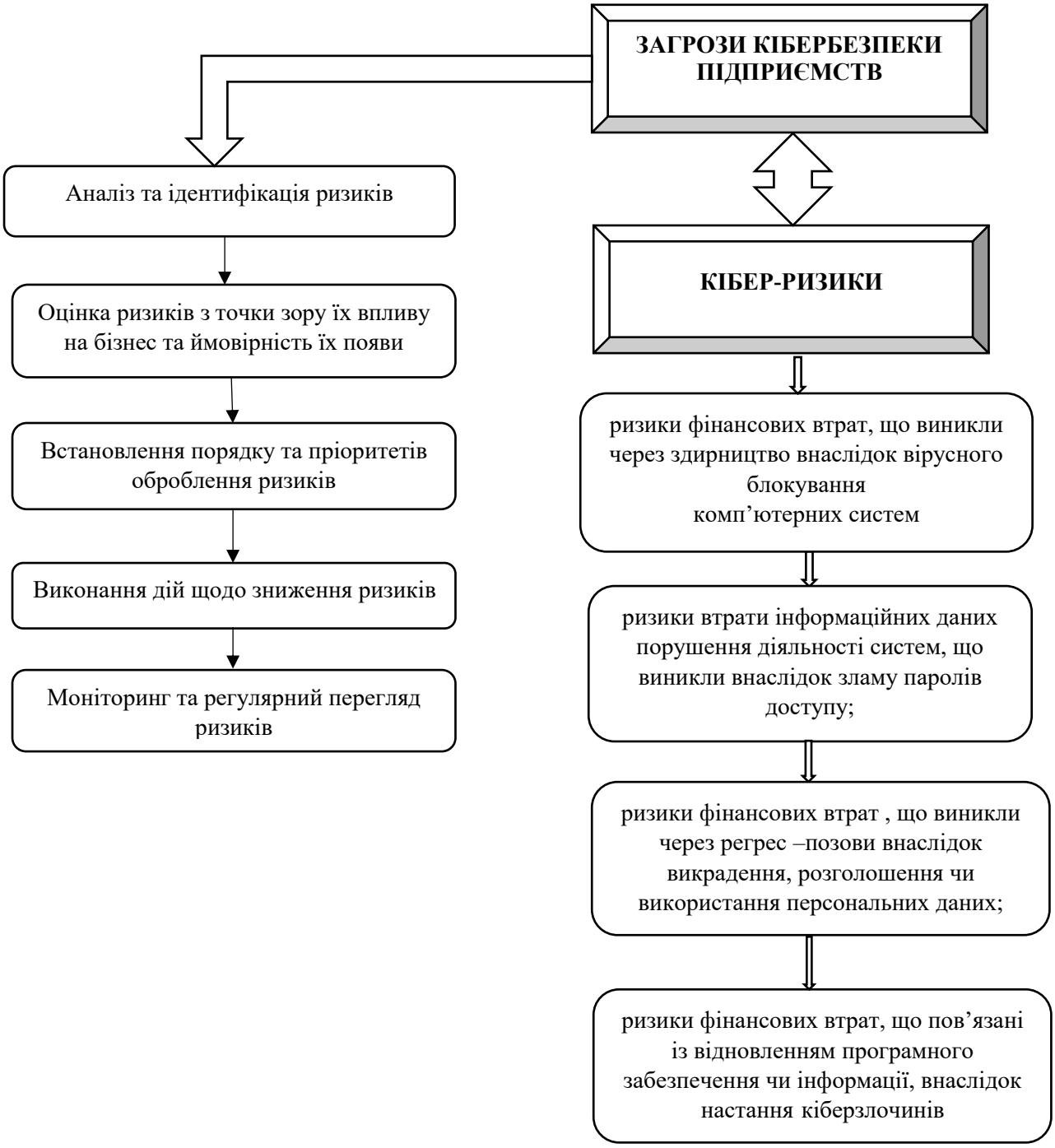

Рис. 3. Модель управління кібер-ризиками підприємства

Джерело: сформовано авторами на основі [7; 8]

Висновки. Сьогодні коли кожна організація починає більше використовувати новітні інформаційні технології, кібербезпека стає однією з основних складових економічної безпеки. Діагностика кібер-ризиків допоможе підприємствам організувати роботу фахівців, виходячи з природи і небезпеки загроз. Кібербезпека потребує постійної підтримки та аналізу її

ефективності, це забезпечить економічну безпеку підприємства та держави в цілому.

Література

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник Київ: ДУТ, 2015. 288 с.
2. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології // Цифрова платформа: інформаційні технології в соціокультурній сфері. 2018. №1 С. 75-83.
3. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 17.03.19).
4. Всесвітнє дослідження економічних злочинів та шахрайства 2018: Результати опитування українських організацій. URL: https://www.pwc.com/ua/uk/survey/2018/economic-crime-survey.htm (дата звернення: 22.06.2020).
5. Україна Всесвітній огляд економічних злочинів. Кіберзлочини в центрі уваги. URL: https://www.pwc.com/ua/uk/press-room/assets/gecs_ukraine_ua.pdf (дата звернення: 22.06.2020).
6. ЗВІТ Голови Національної поліції України про результати роботи відомства у 2019 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf.
7. Бурячок В. Л., Богуш В. М. Рекомендації щодо розробки та запровадження профілю навчання "Кібернетична безпека" в Україні // Безпека інформації. 2014. Т. 20, № 2. С. 126–131.

8. Братюк В. П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні // Актуальні проблеми економіки. 2015. № 9 (171). С. 421–427.
9. Ротова Т. А. Шевченко Ю. Страхування як фінансовий інструмент захисту від кібер-ризиків // Безпека соціально-економічних процесів в кіберпросторі: матеріали Всеукр. наук.-практ. конф. (Київ, 27 берез. 2019 р.). Київ : Київ. нац. торг.-екон. ун-т, 2019. С. 177-178.