Volodymyr Mishchenko, Doctor of Economics, Professor
Institute for Economics and Forecasting of the NAS of Ukraine
Kyiv, Ukraine
Svitlana Naumenkova, Doctor of Economics, Professor
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
DOI: https://doi.org/10.30525/978-9934-26-222-7-30

DIRECTIONS OF COUNTERING CYBER THREATS AND REDUCING THE LEVEL OF CYBER RISKS

НАПРЯМИ ПРОТИДІЇ КІБЕРЗАГРОЗАМ ТА ЗНИЖЕННЯ РІВНЯ КІБЕРРИЗИКІВ

Процеси цифровізації економіки на основі впровадження сучасних ІК-технологій, хмарних сервісів, Інтернету речей, накопичення та оброблення значних обсягів інформації,

віддаленого обслуговування та роботи, мобільних онлайн операцій, е-комерції тощо сприяли появі нових інформаційних загроз і ризиків. І хоча більшість компанії роблять значні інвестиції в сучасні технології та обладнання з метою захисту від кіберзагроз, масштаби та суми втрат у результаті їх реалізації постійно зростають [1, с. 59; 2, с. 198; 3, с. 32].

Переважна більшість компаній та органів державної влади у всіх країнах світу вже зіткнулися з впливом кібератак і вразливості ІТ-систем на свою діяльність. Центр стратегічних та міжнародних досліджень США щомісяця реєструє в середньому десять значних кібератак. Кількість атак програм-вимагачів, починаючи з 2019 р., щорічно зростає вдвічі, а кількість фішингових атак лише за січень-лютий 2020 р. збільшилась у п'ять разів [4]. При цьому варто зазначити, що якщо в минулому кібератаки здійснювали окремі особи, то сьогодні набуває поширення кіберхакінг – діяльність організованих груп зловмисників.

Головними наслідками реалізації кіберзагроз є збитки або втрати в результаті порушення або припинення діяльності компаній, порушення або припинення роботи інформаційно-комунікаційних систем, програмного забезпечення та обладнання, пошкодження, викрадення або розголошення інформації та персональних даних, фінансові втрати тощо [5, с. 26].

З метою зменшення потенційного впливу кіберзагроз на свою діяльність компанії повинні розробляти ефективні захисні стратегії, використовуючи максимально широкий спектр методів та інструментів. Головними напрямами посилення кібербезпеки компаній, на наш погляд, є:

1) вдосконалення доступу до даних та інформаційних платформ;

2) автоматизація процесів, застосування штучного інтелекту, машинного навчання та аналітики великих даних;

3) підвищення рівня кваліфікації працівників і залучення спеціалістів у галузі кібербезпеки;

4) посилення механізмів регулювання впровадження та використання нових ІК-технологій;

5) розвиток системи кіберстрахування [6, с. 27; 7, с. 192].

Сучасний етап цифровізації економіки та різноманітних сфер життєдіяльності людини пов'язаний зі стрімким збільшенням обсягів інформації. У 2020 р. щосекунди кожна людина створювала близько 1,7 мегабайти інформації [4]. Використання віддалених і гібридних форм роботи та поширення цифрових технологій потребують швидкого й надійного доступу до великих масивів даних. Масштаби та інтенсивність обміну й використання інформації стрімко зростають. З'явився новий клас провайдерів, які завдяки використанню хмарних технологій спеціалізуються на збиранні, зберіганні, обробленні, систематизації, аналізі та управлінні даними, які використовуються широким колом споживачів.

Таке збільшення обсягів даних і розширення можливостей доступу до них посилює ймовірність незаконного заволодіння ними, що стає головним джерелом кібератак зловмисників. При цьому варто зазначити, що технічні, технологічні та людські можливості більшості компаній ще відстають від методів і технологій здійснення кібератак, а тому управління кіберризиками часто не відповідає сучасним вимогам цифрових трансформацій [8, с. 7].

З метою забезпечення надійного захисту даних і зниження рівня кіберризиків, пов'язаних з розширенням доступу до даних, стратегічним напрямом діяльності компаній повинно стати використання принципу «нульової довіри» та технологій поведінкової аналітики.

Принципово важливим аспектом реалізації принципу «нульової довіри» є переорієнтація систем кіберзахисту та управління ризиками із захисту фізичних об'єктів і мереж на механізми захисту активів і ресурсів компаній та їх клієнтів [9, с. 28]. Використання технологій поведінкової аналітики сприяє організації безпечної роботи працівників компаній на основі відслідковування запитів на доступ до інформації, контролю за аномальною поведінкою користувачів або активністю роботи

пристроїв, а також забезпеченню належного рівня аутентифікації та авторизації.

З метою забезпечення ефективного управління кіберризиками компанії повинні запровадити ризик-орієнтований підхід до автоматизації та автоматичного реагування на кібератаки шляхом використання технологій машинного навчання, штучного інтелекту та аналітики великих даних. Така автоматизація повинна враховувати потенційну мінливість моделей і видів кібератак та максимально повно використовувати захисні можливості й контрзаходи з боку центрів управління безпекою, управління ідентифікацією та доступом, машинну автоматизацію робочих процесів, технології автоматичного виявлення й виправлення невідповідностей у системах та своєчасне оновлення програмного забезпечення.

Залежно від характеру, складності та частоти кібератак компанії можуть реагувати на них шляхом використання технічних (створення стійких репозиторіїв даних, забезпечення автоматизованої реакції на шкідливе шифрування та розширену аутентифікацію) або організаційних (проведення навчань, розроблення сценаріїв можливих кіберзагроз) заходів.

Контроль з боку регуляторних органів за розробленням, впровадженням і використанням ІК-технологій повинен ґрунтуватися, перш за все, на впровадженні можливостей забезпечення кібербезпеки в технологічні можливості програмного забезпечення на всіх етапах його проєктування та створення за такими напрямами: 1) створення безпечного програмного забезпечення на основі тісної взаємодії фахівців у галузі технологічної безпеки та ризиків з розробниками такого забезпечення; 2) максимально повне використання переваг хмарних сервісів (платформа як послуга, інфраструктура як послуга); 3) стандартизація та кодифікація контрольно-інженерних процесів; 4) специфікація програмного забезпечення та деталізація його структурних складових (компоненти з відкритим вихідним кодом, компоненти у кодовій базі, інструменти сканування коду, галузеві стандарти та вимоги).

Важливим напрямом управління кіберризиками є їх страхування. За даними компанії IndustryARC, ринок кіберстрахування в 2021 р. склав близько 10 млрд. дол. США, а в 2026 р. досягне 22,4 млрд. дол. й надалі буде зростати високими темпами [4]. Сьогодні спектр видів страхового покриття внаслідок реалізації кібератак є доволі широким і може включати: збитки (неодержані доходи), що виникли в результаті припинення або переривів у роботі; збитки, пов'язані з порушеннями бази даних (знищення, викрадення, розголошення інформації) та функціонуванням телекомунікаційних мереж; компенсацію витрат компаній на врегулювання наслідків кіберінциденту (витрати на експертизу, відновлення репутації, програмного забезпечення); збитки в результаті віртуального вимагання та інші [10, с. 18]. При цьому варто зазначити, що страхові компанії своєчасно реагують на зміни в ІТ-сфері, враховують унікальні потреби клієнтів, персоналізують пропозиції для різних сегментів ринку та постійно вдосконалюють перелік форм і видів страхового покриття збитків від реалізації кіберзагроз.

Література:

1. Науменкова С.В., Міщенко С.В. Інституційний розвиток фінансового сектору України. *Фінанси України*. 2008. № 7. С. 53–71.
2. Mishchenko S., Naumenkova S., Mishchenko V., Dorofeiev D. Innovation risk management in financial institutions. *Investment Management and Financial Innovations*. 2021. Vol. 18. Is. 1. P. 190–202.
3. Міщенко С. Економіко-статистичний аналіз факторів монетизації економіки. *Вісник НБУ*. 2012. № 1. С. 31–33.
4. Boehm J. et al. Cybersecurity trends: Looking over the horizon. McKinsey & Company. March 10, 2022. URL: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity-trends-looking-over-the-horizon (дата звернення: 28.05.2022).
5. Мищенко С.В. Новые тенденции в монетарной политике и регулировании финансовых систем. *Финансы и кредит*. 2013. № 40. С. 23–29.
6. Міщенко В.І., Науменкова С.В. Банківська система України: проблеми становлення та розвитку. *Фінанси України*. 2016. № 5. С. 7–33.

7. Науменкова С.В., Міщенко В.І. Поняття системного ризику та підходи до визначення системно значущих банків. *Соціально-економічні проблеми сучасного періоду України*. Львів: НАН України. Ін-т регіональних досліджень 2014. Вип. 1 (105). С. 186–196.

8. Кротюк В.Л., Міщенко В.І. Еволюція підходів до оцінки капіталу в Базельських угодах. *Банківська справа.* 2006. № 4. С. 3–9.

9. Науменкова С., Міщенко С. Особливості формування сучасної моделі фінансової системи. *Вісник Національного банку України*. 2006. № 11. С. 26–31.

10. Науменкова С.В. Оцінка впливу галузевої приналежності на рівень перспективної платоспроможності позичальника. *Вісник НБУ*. 2005. № 7. С. 14–21.