фінансування.

6 Етап. Співставлення рівнів фінансової безпеки акціонерних товариств на основі єдиного індикатора та встановленого за структурним співвідношенням джерел фінансування операційної, фінансової та інвестиційної діяльності.

1. Ареф'єва О.В. Економічні основи формування фінансової складової економічної безпеки: текст. Актуальні проблеми економіки. 2009. № 1. С. 101 – 107.

2. Барановський О.І. Фінансова безпека в Україні (методологія оцінки та механізм забезпечення) : монографія. К.: Київ. нац. торг.-екон. ун-т. 2004. 759 с.

3. Бланк И.А. Управление финансовой безопасностью. К.: Изд-во «Ника-центр». Эльга. 2004. 784 с.

4. Кузенко Т.Б. Управление финансовой безопасностью на предприятии. БИЗНЕСИНФОРМ. 2007. № 12 (1). С. 27 – 29.

5. Мунтіян В.І. Економічна безпека України. К.: КВІЦ, 1999. 464 с.

6. Папехин Р.С. Факторы финансовой устойчивости и безопасности предприятия : дисс…канд. экон. наук: спец. 08.00.10 Волгоград. 2007. – 176 с.

7. Шелест В.В. Управління фінансовою безпекою довірчого товариства. Актуальні проблеми економіки. 2009. № 3. С. 181–184.

ПРОБЛЕМИ БЕЗПЕКИ МАЛИХ І СЕРЕДНІХ ПІДПРИЄМСТВ В УМОВАХ КІБЕР-РИЗИКІВ

Тарасова Кристина Ігорівна
Одеський національний економічний університет

Сьогодні більшість підприємств покладається на технології для успішного ведення бізнесу. Більш того, підприємства будь-якого розміру здатні конкурувати саме завдяки інформаційним технологіям: зокрема, малий бізнес зміг зростати та процвітати в Інтернеті.

У той же час новітні технології дозволили кібер-злодіям і перешкоджати бізнесу. Експерти прогнозують, що кіберзлочинність обійдеться підприємствам в цілому більше ніж в 2 трлн. дол. в 2019 р. (1 трлн. дол. в 2018 р.). Більш того, в строк до 2021 р. збиток, пов'язаний з кіберзлочинністю, досягне 6 трлн. дол. на рік.

Кібер-атаки та порушення безпеки даних є найбільшими загрозами, з якими стикаються підприємства, і невеликі фірми все частіше опиняються під загрозою. Статистика стверджує, що майже дві

третини (61%) малих і середніх підприємств (МСП) зазнали кібер-атаки минулого року, в той час як 54 % визнали факт крадіжки або зміни даних.

МСП часто сприймаються хакерами як легка ціль через брак досвіду та обізнаності щодо кібер-безпеки, а також недостатність часу для реалізації права захисту даних. З огляду на це, особливої актуальності набувають питання дослідження кібер-ризиків малих та середніх підприємств, а також питання управління ними.

Основними кібер-ризиками, з якими стикались МСП у 2018 р. виступили:

- ризик вимагання викупу за викрадені дані. Яскравим прикладом вірусу цього типу є WannaCry, який заразив більш ніж 200 тис. комп'ютерів у 150 країнах світу. Найбільш поширений тип цієї кібер-атаки отримує доступ до комп'ютерів через фішингові листи з інфікованими посиланнями або вкладеннями;
- атаки DDoS, частота виникнення яких зросла на 64 % у порівнянні із 2017 р. Ці атаки затоплюють сервери компанії безліччю запитів, з кількістю яких вона не в змозі впоратися, і змушена зупинити роботу. Це залишає бізнес нездатним торгувати на години або навіть дні з потенційно довгостроковими наслідками;
- інсайдерська загроза. Навмисні чи ні, людські помилки є найпоширенішою причиною кібер-атак і порушень безпеки даних (95 %). Кібер-ризик може бути викликаний будь-яким випадком, коли співробітники випадково посилають конфіденційну інформацію на неправильний електронний лист, втрачаючи смартфон компанії або використовують стандартні паролі. Фактично, нещодавнє дослідження показало, що більшість атак на МСП пов'язані з поганим управлінням паролями [1].

Жодне підприємство сьогодні не може стверджувати, що воно є на 100 % захищеним від кібер-загроз. Однак, якщо ввести певні системи контролю безпеки, кількість атак можна звести до мінімуму. За точкою зору спеціалістів PriceWaterHouseCoopers і Nasstar, основними напрямами зниження кібер-ризиків виступають:

- автоматичне виправлення помилок системи, що дозволить запобігти появи 90 % повторних помилок;
- резервне копіювання. Рекомендовано дотримуватися правила 3-2-1: принаймні три копії, у двох різних форматах з принаймні однією копією за межами підприємства;
- шифрування даних;

- антивірусне та антифішингове програмне забезпечення від авторитетних постачальників (використання платної версії замість безкоштовної із обмеженим функціоналом);
- управління мобільними пристроями, які мають доступ до мережі підприємства;
- безпечна аутентифікація як то двофакторна аутентифікація (2FA), що усуває ризик викрадення паролів; або менеджер паролів, який їх надійно зберігатиме та генеруватиме;
- безпечне співробітництво: деякі хмарні інструменти для синхронізації та спільного доступу можуть запропонувати простий спосіб обміну та співпраці з документами. Необхідно обирати версії корпоративного рівня замість споживчих інструментів;
- інспекція журналу, моніторинг файлів;
- розробка алгоритму відповіді на кібер-інциденти [2, с. 4-5].

1. The Biggest Cyber Threats Facing SMEs in 2018. Fleximise : веб-сайт. URL : https://fleximize.com/articles/011275/cyber-threats-facing-smes (дата звернення : 07.05.2019).
2. Cyber Security for SMEs: a practical guide to protecting your business. Nasstar. 2018. 8 p. URL : https://cdn2.hubspot.net/hubfs/4153852/Marketing-Material/white%20paper%20-%20cyber%20security.pdf (дата звернення : 07.05.2019).

ТЕОРЕТИЧНЕ ТРАКТУВАННЯ ІНКЛЮЗИВНОСТІ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ СОЦІАЛЬНОЇ, ЕКОЛОГІЧНОЇ, ЕКОНОМІЧНОЇ БЕЗПЕКИ СІЛЬСЬГОСПОДАРСЬКИХ ПІДПРИЄМСТВ

Тютюнник Ганна Олексіївна
Інститут проблем ринку та економіко-екологічних досліджень НАН України, м. Одеса

Природним продовженням розвитку загальної концепції щодо встановлення балансу між задоволенням сучасних потреб людства і захистом інтересів майбутніх поколінь стали зусилля боротьби з бідністю та нерівністю. Актуальним є проблема індивідуумів, які не мають доступу до можливостей через свою стать, вік, місце народження або інші обставини і не можуть отримати якісну освіту, низької кваліфікації та обмежених перспектив працевлаштування.