

УДК 004:001.102-049.5

РОЛЬ ЦЕНТРІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗАХИСТІ ІТ-ІНФРАСТРУКТУРИ КОМПАНІЙ

*Станіслав Петько**Доцент кафедри міжнародного менеджменту
КНЕУ імені Вадима Гетьмана, м. Київ, Україна*

Анотація. Проаналізовано роль центрів інформаційної безпеки у захисті ІТ-інфраструктури компаній та їх основні принципи функціонування в корпоративному бізнес середовищі. Визначено мету створення центрів інформаційної безпеки, основні обов'язки та підходи персоналу щодо вирішення питань кібербезпеки компаній при потенційних загрозах. Доведено, що менеджери четвертого рівня таких центрів виступають основним елементом комунікації з іншими підрозділами компанії задля запобігання потенційної кіберзагрози та вчасної передачі інформації.

Ключові слова: центр інформаційної безпеки, ІКТ, компанія, ІТ-інфраструктура, кібербезпека.

Abstract. Analyzed the role of security operations center in the company's IT-infrastructure protection and its basic principles of functioning in the corporate business environment. Determined the main purpose of the security operations centers creating, main responsibilities and approaches company's staff of solving cybersecurity issues in case of potential threats.

It has been proven that the fourth-level managers of such centers are going as the main element of communication with other divisions of the company in order to prevent a potential cyber threat and timely transfer of information.

Keywords: security operation center, ICT, company, IT-infrastructure, cybersecurity.

Із цифровізацією бізнес середовища й інтеграцією ІКТ у виробництво та сферу послуг набула потреба в захисті ІТ-інфраструктури компаній. Поява глобальної мережі Internet та подальший бурхливий розвиток ІКТ спричинило появу кіберзлочинності, хакерських атак, веб-підробок, вірусів, витоку корпоративної інформації, що заважає ефективно функціонувати компанії та знижує її конкурентоспроможність. І це не важливо до якої форми власності відноситься компанія – страждають від кіберзлочинності та атак як державні, так і приватні компанії.

Починаючи з 1970 рр. починають виникати центри інформаційної безпеки (SOC – security operations center) у США, а потім в Японії, Вели-

кобританії, Західній Німеччині, Республіці Корея, які з часом стали невід'ємними частинами будь-якої компанії або державної організації. За своєю суттю центр інформаційної безпеки – це група ІТ-фахівців, які моніторять 24/7 інформаційний стан компанії від потенційних внутрішніх та зовнішніх кіберзагроз. Мета створення центрів інформаційної безпеки полягає в своєчасному запобіганні потенційних кіберзагроз, підвищенні рівня захисту корпоративної мережі, зниження ризиків, а у випадку виникнення кіберзагрози – швидко її встановити та знищити.

Основні обов'язки фахівців таких центрів полягають у:

- 1) перевірки мереж компанії на вразливість та аналіз їх кібербезпеки;
- 2) постійному моніторингу та аналізу кіберзагроз;
- 3) фільтрації фейкових обробок та швидкій реакції на підтверджені кіберзагрози;
- 4) підготовці звітів щодо реального стану ІТ-інфраструктури компанії, кількості хакерських атак та ідентифікованих загроз.

Персонал центру інформаційної безпеки складається з аналітиків великих даних, криптографів, інженерів кібербезпеки та мережевої інженерії. Іншими словами, – це професіонали, які спеціально навчені відстежувати та керувати потенційними кіберзагрозами, допомагають створювати та підтримувати безпечну ІТ-архітектуру компанії. Вони не лише вміють користуватися різноманітними інструментами безпеки, але й знають конкретні дії, яких слід дотримуватися у разі зламу ІТ-інфраструктури компанії. Фахівці центру використовують низку інструментів, які збирають дані з мереж та апаратного обладнання, відстежують аномалії та сповіщають персонал компанії про потенційні кіберзагрози.

Більшість центрів інформаційної безпеки у глобальних ТНК використовують ієрархічний підхід до вирішення питань кібербезпеки, де фахівці центру розподіляються на основі їхнього набутого практичного досвіду. Класична команда центру може бути структурована наступним чином:

Рівень 1. “Гаряча лінія” служб реагування на потенційну загрозу. Спеціалісти з безпеки спостерігають за сповіщеннями та визначають терміновість кожного сповіщення та час для його переведення на рівень 2. Спеціалісти першого рівня мають змогу управляти засобами безпеки та надавати регулярні звіти.

Рівень 2. Персонал другого рівня більш досвідчений за колег з першого рівня, тому вони можуть швидше знайти загрозу та оцінити частину ІТ-

інфраструктури компанії, яка піддалася кібератаці. Фахівці дотримуються спеціальних процедур для усунення кіберзагрози, а також визначають знайдену загрозу для її подальшого дослідження.

Рівень 3. На даному рівні персонал складається з провідних експертів-аналітиків кібербезпеки, які активно шукають вразливі місця в мережі. Спеціалісти використовують широкий арсенал інструментів задля виявлення кіберзагрози, здійснюють карантинне діагностування слабких місць мережі задля розробки рекомендацій щодо підвищення рівня загальної кібербезпеки компанії.

Рівень 4. Четвертий рівень складається з топ-менеджерів з найбільшим досвідом роботи, яким підпорядковується уся команда центру інформаційної безпеки. Вони займаються HR-діяльністю, навчанням молодого персоналу, оцінюють індивідуальну та загальну продуктивність спеціалістів нижчих рівнів. Спеціалісти четвертого рівня втручаються в діяльність центру в самих кризових ситуаціях, який можна характеризувати як гармонічний взаємозв'язок центру з іншими підрозділами компанії.

Інформаційні джерела

1. Петько С. М. Вплив цифровізації державного апарату на розвиток демократії в Республіці Корея. Пріоритетні напрями досліджень в науковій та освітній діяльності: проблеми та перспективи: тези II Всеукраїнської науково-практичної конференції з міжнародною участю (м. Рівне, 12–13 жовтня 2022). КЗВО “Рівненська медична академія. Рівне, 2022.

2. Петько С. М. Електронна комерція в цифровій екосистемі Республіки Кореї. *Економічний вісник Національного технічного університету України “Київський політехнічний інститут”*. 2022. № 23. С. 61–67. doi: <https://doi.org/10.20535/2307-5651.23.2022.264630>

3. Петько С. М. Республіка Корея в індексах цифрової економіки. *Цифрова економіка та економічна безпека*. 2022. № 1 (01). С. 66–73. doi: <https://doi.org/10.32782/dees.1-11>

4. Петько С. М. Цифровий прорив Республіки Корея у сфері державного урядування. *Економіка та суспільство*. 2022. № 42. doi: <https://doi.org/10.32782/2524-0072/2022-42-47>

5. Петько С. М. Цифровий техноглобалізм у становленні Республіки Корея на глобальному ринку напівпровідників. *Науковий вісник Полтавського університету економіки і торгівлі. Серія “Економіка”*. 2022. Випуск 1 (65). С. 91–99.