Чернов О. Ф.,
аспірант,
ПВНЗ "Європейський університет"
Науковий керівник: ***Польова Н. М.,***
канд. екон. наук, доцент,
доцент кафедри менеджменту і маркетингу,
ПВНЗ "Європейський університет", м. Черкаси

КІБЕРГІГІЄНА ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ КОРПОРАТИВНОЇ КУЛЬТУРИ СУЧАСНОГО ПІДПРИЄМСТВА

В епоху глобальних викликів, геополітичних ризиків та інформаційних загроз Україна стала епіцентром протистояння у наймасштабнішій з часів Другої світової війні на Європейському континенті.

Повномасштабне вторгнення з боку агресора повністю змінило погляди українських вчених, менеджерів та працівників на інформаційну безпеку та змінило правила гри в контексті переходу в епоху глобальної цифровізації. Починаючи з 24 лютого 2022 року, термін "кібергігієна" [1, с. 52] остаточно перестав бути чимось специфічним та незрозумілим для широкої публіки, перейшовши зі сфери кібербезпеки та системного адміністрування до загального і повсякденного використання в усіх галузях.

Хакерська атака російського кібертерористичного угруповання "Солнцепьок" на українську телекомунікаційну компанію "Київстар" [2] довела, що навіть величезні за своїм розміром, статками, штатом і клієнтською базою підприємства не застраховані від кризових ситуацій та непередбачуваних кіберзагроз. Саме ця атака стала черговим підтвердженням серйозності намірів геополітичних ворогів України з метою завдавання максимальної шкоди українській інфраструктурі і довела, що підготовка оборони у масштабах кібербезпеки (як на великих державних, так і на малих локальних підприємствах) важлива не менше, ніж розбудова фізичної інфраструктури безпеки.

Це повністю змінює всі раніше розроблені норми корпоративної культури підприємств, виводячи питання кібербезпеки, кібергігієни та відповідальності за них для працівників на новий рівень. Відтепер терміни із галузі кібербезпеки перестали бути звичайним лексиконом відділів системного адміністрування і увійшли до повсякденного вжитку всієї вертикалі організації: від стажерів до керівників найвищої ланки.

У реаліях початку 2026 року втрачена ключ-карта від офісного приміщення (навіть якщо власник картки не мав доступу до інформаційних систем підприємства) може стати фатальною настільки ж, як і використання пароля "1234abcd" на персональному комп'ютері працівника. Враховуючи, що термін "інтелектуальний капітал" настільки ж нематеріальний, як і "інтелектуальна власність", то сьогодні навіть важко підрахувати збитки у разі витоку інформації, адже у зоні ризику потенційних загроз є нематеріальні активи організації: патенти, ідеї, потенційні винаходи тощо. Саме тому

міжнародний стандарт управління інформаційною безпекою «ISO/IEC 27001» [3] розглядає фізичний та логічний доступи, як рівнозначні вектори загрози.

Все це ставить відділи системного адміністрування у дуже відповідальну позицію, адже саме від їхніх рішень залежатиме кібербезпека на підприємстві. Проте для досягнення високих показників кібербезпеки та відповідальності кожного окремого працівника усі рівні компанії мають працювати у тісній синергії та постійній координації. Недостатньо буде лише розробити "корпоративну етику кібергігієни". Потрібно, насамперед, донести важливість розробки такої етики до керівників організації, після чого адаптувати її для використання стажерами, офісними працівниками, керівниками середньої ланки тощо - за допомогою департаменту кадрів.

Відділ кадрів в ієрархії питань відповідальності за кібергігієну на підприємстві посідає друге місце після департаменту системного адміністрування, адже напрацьовані у взаємодії цих двох рівнів норми необхідно буде не лише поширити на вже найнятих працівників підрозділів, а ще й інтегрувати у процес відбору персоналу. Збільшення тривалості співбесіди на 5–10 хвилин за рахунок питань про розуміння потенційним працівником елементарних норм кібергігієни, а також розробка тестів із вищезазначеної теми може дещо зменшити продуктивність роботи відділів кадрів та змусити фірму зіткнутися з непередбачуваними операційними витратами. Але ці збитки будуть значно меншими, ніж від ненадійного пароля корпоративного акаунта працівника чи від "фішингового" листа на його пошті, який цей працівник необдумано відкриє, поставивши під ризик усю компанію.

Отже, на сьогодні кібергігієна була і лишається ключовим складником будь-якого підприємства, яке дбає про свої активи: як матеріальні, так і нематеріальні. Лише комплексна взаємодія усіх відділів організації, відповідальність кожного окремого працівника (на всіх рівнях) за свої дії та фільтр потенційних робітників при прийомі на роботу зможуть дозволити компанії функціонувати та надавати послуги стабільно і ефективно.

Список використаних джерел:

1. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *The international scientific-practical journal "commodities and markets".* 2022. Т. 43, № 3. С. 47–59. URL: https://doi.org/10.31617/2.2022(43)04 (дата звернення: 12.03.2026).

2. Учасники проектів Вікімедіа. Кібератака на «Київстар» (2023) – Вікіпедія. URL: https://uk.wikipedia.org/wiki/Кібератака_на_«Київстар»_. (дата звернення: 12.03.2026).

3. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014; Cor 2:2015, IDT). Київ : ДП «УкрНДНЦ», 2016. 32 с.