УДК 004.056

Куперштейн Л. М.
Немировська Д. О.

АКТУАЛЬНІСТЬ ОЦІНКИ РІВНЯ ОБІЗНАНОСТІ ПРАЦІВНИКІВ ПІДПРИЄМСТВА В КІБЕРГІГІЄНІ

Вінницький національний технічний університет

Анотація

У цій роботі доведено актуальність врахування рівня обізнаності працівників в кібергігієні задля уникнення кібератак та різних втрат для підприємств.

Ключові слова: кібергігієна, кібератаки, втрати, ризики.

Abstract

This article proves the relevance of taking into account the level of employees' awareness of cyber hygiene in order to avoid cyber attacks and various losses for enterprises.

Keywords: cyber hygiene, cyber attacks, losses, risks.

Вступ

Технологічний прогрес став невід'ємним етапом усіх сфер нашого життя. Неможливо уявити сучасні компанії без використання комп'ютерів, мобільних пристроїв та інших технічних засобів, які стали фундаментальними для виконання професійних завдань. Такий стрімкий розвиток технологій сприяє прогресу в багатьох областях, таких як бізнес, медицина та освіта, він пропонує безліч переваг, включаючи оптимізацію та автоматизацію бізнес-процесів, підвищення продуктивності працівників, поліпшення умов праці, а також надає доступ до обширних інформаційних та комунікаційних ресурсів. Водночас це несе в собі ризики для приватності, цілісності та доступності інформації. Тому ці переваги супроводжуються збільшенням загроз кібербезпеці.

Основна частина

Підключення до Інтернет, використання хмарних сервісів та зростання кількості електронних пристроїв створюють умови для кіберзлочинців, які прагнуть виявити слабкі місця для проведення атак та компрометації даних. За словами технічного директора IT-компанії UNITY-BARS, яка спеціалізується на розробці програмного забезпечення для фінансових установ, Україна посідає друге місце серед найбільш атакованих країн у світі, одразу за США. Він також зазначає, що у 2022 році кількість кібератак зросла в 3,5 рази порівняно з 2021 роком. Зокрема, фінансовий сектор України став мішенню для 5% усіх атак, тоді як на IT-галузь припадає 10% цих атак [1]. А вже протягом першої половини 2023 року Державна служба спеціального зв'язку та захисту інформації України зафіксувала 762 інциденти. Це на 123% більше, ніж у другому півріччі 2022 року [2].

У контексті активної інформаційної війни, яка ведеться в нашій країні, критично важливим є глибоке розуміння кібергігієни. Це не просто питання особистої безпеки. Воно стосується захисту корпоративних даних та цілої нації. Ігнорування базових принципів безпечної поведінки в Інтернет може призвести до серйозних ризиків, включаючи витік критичної інформації, яка може бути використана зловмисниками, а також втрату конфіденційних даних. Важливо, щоб організації мали ефективні засоби для оцінки рівня знань своїх співробітників у цій сфері. Розробка спеціалізованих інформаційних систем для оцінки кібергігієни може значно підвищити рівень захисту даних на рівні підприємств та національному рівні.

Під час вступного інструктажу з охорони праці на підприємствах часто упускається важливість кібербезпеки. Це ігнорування може призвести до витоку конфіденційної інформації через недостатнє розуміння працівниками критичної проблеми. Варто пам'ятати, що в системі інформаційної безпеки найбільш вразливим елементом часто є сама людина.

Фактично, понад 95% всіх кібератак виникають саме через людський фактор, а це свідчить про те, що більшість інцидентів інформаційної безпеки відбуваються через навмисні дії або недбалість людей [3]. Помилкові рішення, неправильне використання ресурсів, зловживання обладнанням,

шахрайство та непридатні умови праці можуть призвести до системних збоїв, погіршення якості продукції чи послуг, зниження довіри клієнтів і, як наслідок, до значних фінансових втрат для компанії.

Світова статистика кіберзлочинів останніх років особливо вражає, враховуючи, що середня вартість витоку даних у 2020 році становила 3.3 мільйонів доларів США. Але це лише один аспект проблеми. У той же рік зловмисники отримали суму в 406,34 мільйонів доларів у криптовалюті. Це велике число, що значно перевищує попередні роки, де суми, сплачені у такий спосіб, були значно меншими: 92,94 мільйонів доларів у 2019 році та 27,3 мільйонів доларів у 2018 році [4]. Кібератаки стають все частішими та складнішими, представляючи значні загрози для підприємств, урядів та приватних осіб. У 2023 році витрати на наслідки кібератак, включаючи витоки даних та крадіжки облікових записів, оцінювалися в 8 трильйонів доларів США по всьому світу (за даними дослідницької компанії Cybersecurity Ventures). Прогнозується, що у 2024 році ці витрати зростуть до 9,5 трильйонів доларів США [5]. Така статистика вказує на те, що кіберзлочинці стають все більш винахідливими та успішними у своїх зусиллях отримати незаконну вигоду за рахунок вразливості людей та їх недбалості у сфері кібербезпеки.

Для мінімізації ризиків, пов'язаних з людським фактором, компаніям варто розробляти політики безпеки, проводити спеціальні навчання для співробітників, контролювати доступ до важливої інформації, а також встановлювати етичні норми та процедури для вирішення конфліктів, а головне – оцінювати обізнаність в безпеці кожного робітника.

Оцінка рівня знань працівників з кібергігієни включає в себе різні методи, які можуть застосовуватися окремо або в комбінації. Наприклад, спеціальні тести дозволяють перевірити знання базових правил кібергігієни в різних областях, а симуляції кібератак допомагають оцінити реакцію людей на реальні загрози, найчастіше на фішингові атаки та розсилку шкідливого програмного забезпечення. Аналіз поведінки працівників в мережі, в свою чергу, дозволяє виявити потенційно небезпечні вчинки; безпосередня перевірка дотримання політики безпеки організації, а також проведення прямих бесід або інтерв'ю допомагає оцінити пряме розуміння критичності безпеки для працівників. На додаток, використання чек-листів та відомих стандартів (наприклад NIST або CIS Controls) встановлює конкретні вимоги та рекомендації щодо оцінювання. Варто зазначити, що періодична комплексна перевірка рівня знань кібергігієни та періодичне навчання персоналу є важливою складовою стратегії кібербезпеки будь-якої організації.

Висновок

Наведені факти породжують проблему, яка вимагає від роботодавців уваги до рівня кібергігієни кожного працівника, а також людини, яка є потенційним кандидатом на певну посаду. Крім того, важливо, щоб інструктори, які проводять інструктажі з охорони праці, мали можливість оцінювати рівень кібергігієни в компанії та працювати над виправленням слабких місць. Таким чином, дослідження та оцінка рівня обізнаності працівників у сфері кібергігієни стають надзвичайно важливими для забезпечення безпеки та захисту інформації в сучасному бізнес-середовищі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бегаль І. У 2022 році кількість кібератак на Україну зросла майже втричі. 90% хакерських груп з РФ контролюють силовики – Forbes.ua. *Forbes.ua | Бізнес, мільярдери, новини, фінанси, інвестиції, компанії*. URL: https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454 (дата звернення: 15.05.2024).
2. Poireault K. Cyber-Attacks on Ukraine Surge 123%, But Success Rates Plummet. *Infosecurity Magazine*. URL: https://www.infosecurity-magazine.com/news/cyberattacks-ukraine-surge-success/ (дата звернення: 16.05.2024).
3. Zhadan A. World Economic Forum finds that 95% of cybersecurity incidents occur due to human error. *Cybernews*. URL: https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/ (дата звернення: 15.05.2024).
4. Top 5 Cybersecurity Breaches Due to Human Error - Threatcop. *Threatcop*. URL: https://threatcop.com/blog/top-5-cyber-attacks-and-security-breaches-due-to-human-error/ (дата звернення: 15.05.2024).
5. Global Cost of Cyber Attacks in 2024 | ExpressVPN Blog. *ExpressVPN Blog*. URL: https://www.expressvpn.com/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/ (дата звернення: 16.05.2024).

Куперштейн Леонід Михайлович – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця email: kupershtein.lm@gmail.com

Немировська Дар'я Олександрівна – студентка групи 1БКС-22б, Факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: nemyrovskadaria@gmail.com

Kupershtein Leonid M. – PhD, Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com

Nemyrovska Daria Oleksandrivna - student of group 1BKS-22b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: nemyrovskadaria@gmail.com