УДК 004.056

КІБЕРБЕЗПЕКА ТА ОБІЗНАНІСТЬ ПЕРСОНАЛУ ПІДПРИЄМСТВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ З ПИТАНЬ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ

CYBERSECURITY AND AWARENESS OF CRITICAL INFORMATION INFRASTRUCTURE PERSONNEL ON PROTECTION AGAINST CYBER THREATS

Оксана Жигаревич, Софія Лапчук

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *The article examines the theoretical and methodological aspects of cyber security of critical information infrastructure enterprises, the classification of cyber threats and requirements for the formation of a protection system. Analysis of the potential of personnel in the context of countering cybercrime and the development of recommendations for increasing the awareness and competence of employees.*

Кібербезпека критичної інфраструкутри є життєво важливою для забезпечення безперебійної роботи підприємств та захисту національних інтересів. Захист інформаційних систем, мереж, даних та послуг від кіберзагроз є пріоритетним завданням.

Основна класифікація кіберзагроз: внутрішні загрози – це дії недобросовісного персоналу, помилки працівників; зовнішні загрози – дії хакерів, зловмисні програми, держави-агресори.

Національні та міжнародні стандарти, такі як ISO/IEC 27001, забезпечують систематичний підхід до захисту інформаційних активів. Ініціативи, такі як проект USAID з кібербезпеки критичної інфраструктури в Україні, сприяють підвищенню рівня безпеки через фінансування, технічну підтримку та обмін передовим досвідом.

Ключовим фактором успіху є постійне навчання і підвищення обізнаності працівників про сучасні кіберзагрози та методи їх протидії. Розробка стратегії кібербезпеки включає всі аспекти захисту, від фізичної безпеки до захисту інформаційних систем. Підвищенню обізнаності персоналу сприяють регулярні тренінги, навчальні програми з кібербезпеки, навчання з розпізнавання фішингових атак, правильне використання паролів та реагування на інциденти.

Впровадження сучасних технологій захисту: системи виявлення, шифрування даних, багатофакторна аутентифікація; створення та впровадження процедур управління інцидентами кібербезпеки; налагодження співпраці з державними органами, іншими підприємствами та міжнародними організаціями; регулярний аудит систем кібербезпеки та постійний моніторинг стану захисту.

В роботі розглянуто актуальне визначення об’єктів критичної інфраструктури на рівні законодавства та вимоги до формування безпеки. Виконання рекомендацій забезпечить підвищення стійкості критичної інфраструктури до кіберзагроз та сприятиме надійному захисту інформаційних ресурсів підприємства.

Бібліографія

1. Стратегія кібербезпеки України від 26.08.2021 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/96/2016#Text.
2. Кібербезпека [Електронний ресурс]. – Режим доступу : https://www.usaid.gov/sites/default/files/202301/CYBERSECURITY_ukr%20%281%29.pdf