ПРАВИЛА ОФОРМЛЕННЯ ТЕЗ

Обсяг тез – **від 2 до 5 сторінок** (12 шрифт, одинарний інтервал).

До публікації приймаються лише ті, які раніше не друкувалися і на теперішній час не подані на розгляд до інших видань. Мова публікації: українська або англійська. Всі тези, які буде прийнято до друку, проходять перевірку на наявність плагіату.

Тези повинні мати наступну структуру:

Петренко Петро Петрович
науковий ступінь, вчене звання, посада
місце роботи, місто, країна
ORCID: 0000-0000-0000-0000
E-mail: petr@gmail.com

(Назва) **МОДЕЛЬ КІБЕРБЕЗПЕКИ ДЛЯ ІНФОРМАЦІЙНОЇ МЕРЕЖІ ПІДПРИЄМСТВА**

Текст зберігається у форматах: *.doc, *.docx, шрифт TimesNewRoman, розмір 12 пт. (перелік посилань – 10 пт.), інтервал одинарний, вирівнювання по ширині, без переносів, абзацний відступ – 1,0 см. Формат сторінки А4, всі поля по 2 см. Орієнтація сторінок – книжна.

Формули розташовуються по центру робочого поля або у тексті. Формули набираються в редакторах MicrosoftEquation, WordMathType та ін. Нумеруються тільки формули, на які є посилання. Не допускається подання формул у графічному форматі.

Рисунки та фотографії виконуються в стандартних графічних форматах (редактор MicrosoftWord, Visio, .bmp, .jpg, .tif та ін.) і мають бути чіткими, достатньої детальності. Підписи під рисунками і фотографіями обов’язкові, формуються текстом окремо.

Таблиці виконуються засобами Microsoft Word і нумеруються. Орієнтація сторінок – книжна. Шрифт TimesNewRoman, розмір 10 пт. Номер (наприклад: Таблиця 1) розміщується над таблицею з правої сторони. В наступному рядку, посередині наводиться назва таблиці.

Перелік посилань оформлюється згідно з вимогами Державних стандартів України або стандарту APA (https://www.grafiati.com/) з посиланням на індекс DOI або на електронний ресурс. На всі джерела мають бути посилання в порядку цитування у тексті. Наприклад:

Перелік посилань

1. Synergy of building cybersecurity systems: monograph / S. Yevseiev, O. Laptiev, O. Milov, V. Savchenko et al. // Kharkiv: PC Technology Center, 2021. 188 p. https://doi.org/10.15587/978-617-7319-31-2.

2. Федоренко, А. А., Осадчий, Б. І., & Коржик, В. В. (2023). Аналіз методів виявлення вразливостей Web-ресурсів до SQL-ін’єкцій. Сучасний захист інформації, 3(55), 57–61. https://doi.org/10.31673/2409-7292.2023.030008.

3. Top 7 Vulnerabilities In Android Applications 2022 [Електронний ресурс] // CODERSERA. 2022. Режим доступу: https://codersera.com/blog/top-7-vulnerabilities-in-android-applications-2022/

Тези, які не відповідають зазначеним вимогам – **до розгляду не приймаються!**