ЦИФРОВІ ТЕХНОЛОГІЇ В УМОВАХ СУЧАСНИХ ЗАГРОЗ

Ірина РУДЕШКО
Олег КАЧУРА
E-mail: rudeshko_iryna@nuczu.edu.ua
Національний університет цивільного захисту України

Стрімка цифровізація всіх сфер суспільного життя, включаючи промисловість, енергетику, транспорт, державне управління та об'єкти критичної інфраструктури, зумовлює зростання ролі кібербезпеки як ключового елементу національної та міжнародної безпеки. Використання сучасних цифрових технологій (хмарних сервісів, штучного інтелекту, тощо) суттєво підвищує ефективність управління системами, однак водночас розширює поверхню кібератак. В умовах гібридних та воєнних загроз кіберпростір перетворюється на окремий театр протиборства, де атаки можуть призводити до масштабних техногенних, економічних і соціальних наслідків. Саме тому стандартизація у сфері кібербезпеки набуває критичного значення, оскільки дозволяє уніфікувати підходи до управління ризиками, захисту інформації та забезпечення стійкості цифрових систем [1–6].

Кібербезпека розглядається як сукупність організаційних, технічних та програмних заходів, спрямованих на захист інформаційних ресурсів, мереж та автоматизованих систем від несанкціонованого доступу, порушення цілісності, конфіденційності та доступності даних. Особливу увагу приділяють захисту критичної інформаційної інфраструктури, відмова або компрометація якої може спричинити каскадні наслідки для держави та суспільства. Сучасні кібератаки характеризуються високим рівнем складності, використанням шкідливого програмного забезпечення нового покоління, соціальної інженерії та цільових атак (APT). Це потребує переходу від реактивних до проактивних моделей кіберзахисту, заснованих на аналізі ризиків і постійному моніторингу загроз [3, 6].

Міжнародні та національні стандарти є основою формування єдиних вимог до систем управління інформаційною безпекою [1, 2, 4, 5]. Найбільш поширеними є стандарти серії ISO/IEC 27000, які визначають вимоги до політик безпеки, управління ризиками, контролю доступу та реагування на інциденти.

Важливе значення мають також стандарти NIST, рекомендації ENISA та нормативні документи Європейського Союзу, зокрема Директива NIS2. В Україні питання кібербезпеки регламентуються законами та підзаконними актами, що гармонізуються з міжнародними підходами.

Стандартизація дозволяє [1–5]:

- забезпечити сумісність і взаємодію цифрових систем;
- підвищити рівень довіри до інформаційних технологій;
- створити основу для аудиту та сертифікації систем;
- знизити ризики кібератак за рахунок уніфікованих процедур захисту.

Впровадження цифрових технологій, зокрема хмарних обчислень, призводить до децентралізації обробки даних і збільшення кількості точок доступу. Штучний інтелект використовується як для підвищення рівня кіберзахисту, так і для створення нових інструментів атак. У цьому контексті особливої актуальності набуває концепція «безпеки за проєктом» (security by design), яка передбачає інтеграцію вимог кібербезпеки на всіх етапах життєвого циклу цифрових систем. Стандарти та нормативні документи виступають інструментом формалізації таких вимог [1, 2, 6, 8].

Висновки. Кібербезпека, стандартизація та цифрові технології є взаємопов'язаними елементами сучасної системи безпеки. Ефективний захист цифрових систем неможливий без впровадження міжнародно визнаних стандартів та адаптації їх до національних умов [1–5, 7, 8]. Подальший розвиток цифрових технологій потребує випереджального вдосконалення нормативної бази та підготовки фахівців, здатних працювати в умовах постійно зростаючих кіберзагроз.

Література

[1]. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. — Geneva : ISO, 2022.

[2]. ISO/IEC 27002:2022. Information security controls. — Geneva : ISO, 2022.

[3]. NIST Cybersecurity Framework 2.0. — Gaithersburg : National Institute of Standards and Technology, 2024. — 63 p.

[4]. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2) // Official Journal of the European Union. — 2022.

[5]. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII (зі змін. і допов.). — Режим доступу : https://zakon.rada.gov.ua.

[6]. ENISA. Cybersecurity Threat Landscape : Annual Report. — Heraklion : European Union Agency for Cybersecurity, 2023.

[7]. Шевченко В. Л. Кібербезпека критичної інфраструктури: виклики та підходи до захисту // Наукові праці. — 2022. — № 4. — С. 45–52.

[8]. Козловський С. В. Стандартизація інформаційної безпеки в умовах цифрової трансформації // Вісник Національного технічного університету. — 2023. — № 2. — С. 61–68.