

*Суков М.В., студент 3 курсу фізико-
математичного факультету
Житомирський державний
університет ім. Івана Франка,
Житомир*

**КОМПЛЕКСНИЙ ПІДХІД ДО РОЗРОБКИ КУРСУ З
КІБЕРБЕЗПЕКИ ДЛЯ ПРОФЕСІЙНИХ НАВЧАЛЬНИХ
ЗАКЛАДІВ**

Сучасний вищий навчальний заклад представляє собою установу з розгалуженою структурою, інформаційне середовище якої обробляє

різноманітну інформацію навчально-методичного, науково-дослідного, фінансово-економічного, управлінського та іншого характеру, що викликає підвищені вимоги до надійності та розподілу прав і обов'язків усіх співробітників.

Актуальність дослідження впливає з того, що кібербезпека стала вкрай важливою в сучасному світі, де все “цифровізується”. Дуже багато сервісів сьогодні залежать від цифрових технологій, що підвищує ризики кібератак. Кібербезпека – ніби невидимий щит, який дозволяє всім службам нормально працювати, починаючи від простої електронної пошти та соцмереж до фінансових та медичних систем. Це є як і ключовим оборонним механізмом від онлайн-загроз, так і засобом захисту національної безпеки.

У сучасному цифровому світі кіберзагрози стають все більш серйознішими та ще агресивнішими, торкаючись всіх без винятку. Так, 2023 року кіберполіція України зафіксувала понад 3600 кіберзлочинів — на 59% більше, ніж у попередньому році [1]. Значна частина цих атак була спрямована на державні установи, приватні підприємства та навчальні заклади. Часто зловмисники використовують програми-вимагачі, фішингові атаки, DDoS-атаки та крадіжку конфіденційних даних. Крім того, завдяки розвитку штучного інтелекту та автоматизації злочинці стають дедалі більш ефективними і безпечними у своїх діях.

Ключові елементи розробки курсу.

Згідно з рекомендаціями Міністерства освіти і науки України, нові освітні програми з кібербезпеки повинні базуватися на міжнародних стандартах сертифікації та зосереджуватися на набутті практичних навичок. Це передбачає запровадження віртуальних лабораторій інформаційної безпеки, виробничу практику та моделювання процесів у дворежимному навчанні.

Деякі навчальні заклади вже мають спеціалізовані курси з кібербезпеки, які поєднують теоретичні знання з практичними завданнями. Паралельно створюються дослідницькі центри для аналізу існуючих загроз і розробки нових методів кіберзахисту, що інтегруються у навчальний процес. Сучасні інтерактивні платформи, віртуальні лабораторії та онлайн-курси забезпечують практичне застосування знань у реальному часі.

Нормативно-правова база в Україні створює умови для інтеграції національних стандартів із міжнародними, побудованих на основі міжнародних зобов'язань, Конституції та законів. Сучасні курси

спрямовані на покращення підготовки висококласних спеціалістів із застосуванням штучного інтелекту, аналізу великих даних, віртуальної та доповненої реальності, що сприяє розвитку передових освітніх систем і доступу до відкритих ресурсів.

Проаналізувавши сучасні науково-педагогічні джерела виникає питання про те, які потрібні навички, уміння та знання для захисту особистих даних та інших аспектів відповідно до поточних світових норм і стандартів. Особлива увага приділяється зіставленню вимог до компетентностей згідно з міжнародним стандартом ISO9001:2015 [3] та освітньо-професійним стандартом – Американською Індустріальною Моделлю Кібербезпеки [4].

Комплексний підхід до розробки навчального курсу з кібербезпеки для фахових коледжів та училищ поєднує найкращі світові надбання, набуття досвіду, інноваційні технології та постійне професійне вдосконалення. Такий підхід забезпечить випускникам навички ефективної протидії сучасним кібернетичним викликам, а їхні знання та практичні вміння стануть вагомим внеском у посилення загальної кібербезпеки.

Список використаних джерел

1. <https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnovi-policziyi-ukrayiny-u--rocz-4792/>
2. <https://mon.gov.ua/>
3. <https://www.iso.org/standard/62085.html>
4. <https://www.nist.gov/cyberframework>
5. https://univd.edu.ua/general/publishing/konf/29_05_2020/pdf/2.pdf
6. <https://zakon.rada.gov.ua/laws>