Маринкевич О. М.,
курсант ІІ курсу, кафедра спеціальної фізичної підготовки,
Харківський національний університет внутрішніх справ
(м. Кам'янець-Подільський, Україна)

ВПРОВАДЖЕННЯ МОДУЛІВ З КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В ПІДГОТОВКУ ФАХІВЦІВ ДЛЯ СИЛ ОБОРОНИ

Сучасні загрози в кіберпросторі та інформаційно-психологічній сфері вимагають корінної трансформації підготовки фахівців для Сил оборони, що починається з чіткого визначення необхідних компетентностей. Фахівець повинен вільно володіти знаннями нормативно-правової бази, методів управління ризиками, криптографічного захисту інформації та сучасних моделей протидії кіберзагрозам, включаючи здатність аналізувати вразливості систем і відновлювати їх функціонування після атак. Паралельно формується комплекс навичок для інформаційно-психологічних операцій, що охоплює методи протидії дезінформації, психологічного впливу через цифрові платформи та аналізу ефективності інформаційних кампаній, що дозволяє ефективно протистояти маніпуляціям супротивника та вести власні операції в інформаційному просторі.

На основі визначених компетентностей формується зміст навчальних модулів, який повинен відображати актуальні виклики сучасності. У модулях з кібербезпеки детально розглядаються такі загрози як ransomware-атаки на критичну інфраструктуру, AI-підсилені атаки з використанням deepfake-технологій, кібершпигунство та методи соціальної інженерії, що особливо актуально в умовах геополітичної напруженості. Модулі з інформаційно-психологічних операцій охоплюють вивчення когнітивної війни, методів психологічного впливу через соціальні мережі, технологій створення та спростування фейкової інформації, а також стратегій протидії пропаганді супротивника, що дозволяє майбутнім фахівцям ефективно оперативувати в інформаційному просторі.

Ефективне засвоєння складного матеріалу вимагає застосування інноваційних інтерактивних методів навчання, які дозволяють максимально наблизити освітній процес до реальних умов. Симуляції кібератак у віртуальних діапазонах, кейс-стаді на основі реальних інцидентів кібербезпеки та рольові ігри з відпрацюванням сценаріїв інформаційно-психологічного впливу створюють умови для формування практичних навичок швидкого реагування, критичного мислення та ефективної командної взаємодії в кризових ситуаціях. Такі методи не лише підвищують мотивацію курсантів, але й розвивають їхню здатність до творчого вирішення складних завдань в умовах неповної інформації та тимчасового дефіциту.

Реалізація нових навчальних модулів вимагає розробки чіткого алгоритму їх інтеграції в існуючі освітні програми військових навчальних закладів. Початковим етапом є ретельний аудит поточних навчальних планів з метою виявлення прогалин та можливостей для впровадження нових модулів, після чого проводиться адаптація змісту навчання до специфіки потреб Сил оборони. Важливим елементом є пілотне впровадження оновлених програм у окремих навчальних групах з подальшим аналізом ефективності та корегуванням змісту на основі отриманих результатів, що забезпечує поступовий і контрольований перехід до нової якості освіти.

Для об'єктивної оцінки якості підготовки фахівців розробляється комплексна система моніторингу ефективності навчання, що поєднує традиційні методи теоретичного тестування з інноваційними підходами практичного оцінювання. Теоретичні завдання перевіряють засвоєння нормативно-правової бази, методологічних основ та концептуальних знань, тоді як практичні симуляції дозволяють оцінити вміння застосовувати отримані знання в умовах, що імітують реальні кібератаки та операції інформаційно-психологічного впливу. Така комбінація забезпечує всебічну оцінку як теоретичної підготовки, так і практичних навичок майбутніх фахівців.

Динамічний характер загроз у кіберпросторі та інформаційно-психологічній сфері вимагає створення механізму постійного оновлення змісту навчальних модулів для підтримки їх актуальності. Цей механізм передбачає регулярний моніторинг нових видів загроз, аналіз реальних інцидентів кібербезпеки та інформаційно-психологічних операцій, а також оперативне внесення змін до навчальних програм. Систематичне оновлення практичних кейсів, симуляційних сценаріїв та методологічних матеріалів забезпечує відповідність підготовки фахівців сучасним викликам і вимогам, що особливо критично в умовах швидкої еволюції технологій та методів ведення інформаційної війни.

Список використаних джерел:

1. Кібербезпека та захист інформації - спеціальність рівня бакалавр, URL: https://osvita.ua/consultations/spec-bach/63103/#google_vignette (дата звернення 03.10.2025);
2. Що таке ІпСО і чому про нього все говорять?, URL: https://www.psdinfo.pro/post (дата звернення 03.10.2025);
3. Основні кіберзагрози в умовах ведення інформаційної війни, URL: https://app-journal.in.ua/wp-content/uploads/2024/12/100.pdf (дата звернення 03.10.2025);
4. Використання інтерактивних методів навчання у викладанні охорони праці, URL: https://doi.org/10.36550/2415-7988-2025-1-219-181-187 (дата звернення 03.10.2025);
5. Освітній процес в умовах війни та у повоєнний період: виклики, правила, перспективи, URL:

https://cuesc.org.ua/images/informlist/%D0%9C%D0%B0%D0%BA%D0%B5%D1%82%20advanced_training_UDU.pdf (дата звернення 03.10.2025).