УДК 343.34

ПІДГОТОВКА ВІЙСЬКОВИХ ФАХІВЦІВ ПІД ЧАС ВИВЧЕННЯ ДИСЦИПЛІНИ КІБЕРБЕЗПЕКА В УМОВАХ ВІЙСЬКОВОГО СТАНУ

Пащенко Є. М., доктор філософії (PhD), ст. викладач
Військовий-юридичний інститут Національного юридичного університету імені Ярослава Мудрого

Введення в Україні воєнного стану призвело до змін у всіх сферах життя. Не залишилася осторонь і система військової освіти України, оскільки надзвичайно важливо, щоб керівництво держави забезпечило стабільне функціонування закладів вищої військової освіти (ЗВВО) в умовах війни, що прямим чином впливає на якісну підготовку висококваліфікованих військових фахівців, а отже і удосконалення їх професійної майстерності, здатності та готовності виконувати військовий обов'язок.

24 лютого 2022 року життя громадян України змінилося докорінним чином у зв'язку з військовою агресією Російської Федерації проти України та введенням в Україні режиму воєнного стану Указом Президента України № 64/2022 «Про введення воєнного стану в Україні», затвердженого Законом України «Про затвердження Указу Президента України «Про введення воєнного стану в Україні» від 24 лютого 2022 року № 2102-IX. В сучасних умовах сфера освіти, як і інші суспільні сфери життя, зазнала значних змін [1; 3]. Всі українці намагаються вчитися жити в нових умовах – в умовах воєнного стану, хоча іноді це є неймовірно важко зробити, а часом і неможливо. Беручі до уваги всі негативні чинники, що виникли внаслідок збройної агресії, реальну загрозу життю і здоров'ю учасників освітнього процесу Урядом нашої держави,

Міністерством освіти і науки України та іншими державними органами вживається всіх можливих заходів для того, щоб і в цей нелегкий час громадяни України змогли реалізувати право на освіту, гарантоване вищим законом держави – Конституцією України [2].

Цифрові технології нині є ключовим фактором розвитку підприємств, отже, кібербезпека стає дедалі актуальнішим напрямом наукових досліджень. Основними нормативно-правовими документами, що формують політику України в галузі кіберпезпеки є Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016 та Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII. Саме цими документами визначаються основні суб’єкти прийняття рішень у сфері кібербезпеки.

Для координації та контролю діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку у відповідних сферах, у 2016 році Указом президента України було створено Національний координаційний центр кібербезпеки (НКЦК) – робочий орган Ради національної безпеки і оборони України. Указом Президента України від 28.01.2020 №27 було посилено спроможності НКЦК та змінено формат його діяльності, зокрема, до роботи залучено фахівців з приватного сектору, які спеціалізуються на кіберзахисті.

Посилений НКЦК став «хабом», цифровою платформою, аналітичним центром з моніторингу, виявлення, нейтралізації, прогнозування потенційних кіберзагроз та запобігання ним у майбутньому як у державному, так і у приватному секторі.

На сучасному етапі після повномасштабного вторгнення кібербезпека в Україні, як і в кожній розвинутій державі перетворюється на одну з найважливіших галузей високотехнологічного суспільства та предметом для вивчення. Унаслідок надзвичайно широкого використання сучасних інформаційних-комунікативних технологій у всіх сферах свого

існування суспільство стало вразливим від кібернетичних впливів, які все частіше стають ефективним інструментом для досягнення мети несилового контролю та управління як об’єктами інфраструктури держави, підприємств, так і окремо взятими громадянами, їх об’єднаннями. Потоки інформації, що передаються, зберігаються й обробляються в кіберпросторі, постійно збільшуються, що вимагає їх належного захисту від несанкціонованого доступу зі злочинною метою. Тому посилення кібербезпеки є надзвичайно важливим для забезпечення довіри людей до інновацій, взаємозв’язку та автоматизації, отримання переваг від них, а також для захисту основних прав і свобод, зокрема права на приватність та захист персональних даних, а також свободу вираження поглядів та інформації.

У сучасному інформаційному суспільстві комп’ютерні злочини стали характерною ознакою сьогодення. Розріняють різні категорії комп’ютерних злочинців: “хакери”, “кракери”, “пірати”, “шкідники”. Злочини, що утворюються злочинними угрупуваннями з використанням інформаційних технологій: кібертероризм, загроза фізичної розправи, дитяча порнографія, “відмивання” грошей, крадіжка грошей з банківських рахунків, шахрайські операції з пластиковими платіжними картками, розповсюдження інформації про наркотики через Інтернет [4].

Дослідниця Ю. Савчук здійснила пошук шляхів удосконалення професійної підготовки фахівців із кібербезпеці та захисту інформації через призму чинного законадавства Заслуговує на увагу узагальнення вітчизняної дослідниці щодо доцільності виокремлення різних спеціалізацій профілю “Кібербезпека”, удосконалення освітніх програм та стандартів щодо підготовки фахівців з досліджуваного профілю, формування нової парадигми професійної підготовки, здійснення підбору найбільш доцільних технологій та методів навчання фахівців з кібербезпеки та захисту інформації а також формування метасередовища їх

освітньої діяльності. Слушною є точка зору Ю. Савчук організацію системи підготовки фахівців із кібербезпеки у військовій, банківській, енергетичній, правовій, економічній, сільськогосподарській, освітній сфері, бізнесі, логістиці, промисловості, енергетиці, журналістиці, аудиті [5].

Наприкінці 2021 р. в Україні прийнято нову Стратегію здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та План заходів з її реалізації. Зазначені документи прийняті для забезпечення якісної цифрової трансформації у певних сферах господарювання, пов'язаних з обігом матеріальних цінностей: як-от управління державними фінансами, діяльність із державного внутрішнього фінансового контролю, моніторингу та оцінки фіскальних ризиків, максимальна автоматизація бізнес-процесів та ін. У Стратегії як на окрему мету вказано на інформаційну безпеку в Єдиній інформаційно-телекомунікаційній системі Системи управління державними фінансами від сучасних кіберзагроз в умовах цифровізації управлінських процесів та необхідності обміну даними [5].

Зазначимо, що підготовка фахівців з управління інформаційною та кібернетичною безпекою в секторі безпеки і оборони має базуватися на урахуванні різних категорій кібербезпеки, зокрема, як:

- мережева кібербезпека (захист комп'ютерів від зловмисників, шкідливих програм;

- безпека додатків (захист програмного забезпечення і пристроїв від кіберзагроз;

- інформаційна безпека (захист цілісності і конфеденційності данних під час їх зберігання чи передачі);

- аварійна безпека і безперервність бізнесу (реагування на аварійні ситуації в області кібербезпеки, які призводять до втрати операцій або

даних);

- операційна безпека (забезпечення обробки і захист даних).

Впроваджуючи новітні технології, цивілізація у XXI ст. сприяє активному формуванню супутніх ризиків [6, с. 50]. Також спостерігаємо зростання питомої ваги кіберзагроз, і ця тенденція в міру розвитку цифрових технологій у поєднанні зі штучним інтелектом лише посилиться, а зростання такого впливу визначатиме формування нової безпекової ситуації в країні.

Отже, сучасний світ давно зробив перший крок до принципово нової технологічної, економічної та соціальної реальності – епохи цифрової глобалізації. Вивчення такої дисципліни, як кібербезпека військовими фахівцями є одним із вагомих пріоритетів у загальній системі національної освіти та безпеки України в цілому.

Література :

1. "Про Стратегію національної безпеки України" : Рішення Ради національної безпеки і оборони України від 6 травня 2015 року. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text (дата звернення 1.11.24)

2. Конституція України : Закон України від 28.06.1996 № 254к/96-ВВ. URL: http://zakon1.rada.gov.ua (дата звернення 1.11.24)

3. Цифрові трансформації в Україні - URL: http://eap-csf.org.ua/wp-content/uploads/2021/04/ pdf (дата звернення 2.11.24)

4. Криворучко О. В., Костюк І. В., “Стратегія безпеки інформації” *Кібергігієна. Кібербезпека та безпека держави,*: URL: https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf (дата звернення 2.11.24)

5. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її

реалізації : Розпорядження КМ України від 17 листопада 2021 р. № 1467-р URL: https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#Text (дата звернення 3.11.24)

6. Білявська Ю.В., Шестак Я.І. стаття: Кібербезпека та кібергігієна: нова ера цифрових технологій, ДТЕУ, Міжнародний науково-практичний журнал "Товари і ринки". №3-2022, м. Київ, 2022, С 47-59.

УДК 378.091

ПЕДАГОГІЧНІ УМОВИ ПІДГОТОВКИ МАЙБУТНІХ МАГІСТРІВ ДО ОРГАНІЗАЦІЇ МЕДІАОСВІТИ

Горіна Ю.В., здобувач другого (магістерського) рівня вищої освіти
Класичний приватний університет м. Запоріжжя

Під впливом глобалізаційних процесів і суспільно-політичних трансформацій XXI ст., що кардинально змінили вектор вищої освіти, актуалізувалися нові вимоги до професійної підготовки майбутніх магістрів, що зумовило інтенсивний пошук інструментарію підготовки їх до організації медіаосвіти учнів та студентів. Каталізатором цього процесу виступає сучасна ситуація інформаційної війни в контексті повномасштабного ворожого вторгнення на територію України.

Метою сучасної освіти є всебічний розвиток людини як особистості й найвищої цінності суспільства, розвиток її талантів, розумових і фізичних здібностей, виховання високих моральних якостей; формування