Ковтун Олександр Вікторович, *начальник ГУНП в Житомирській області*

ДЕЯКІ ПИТАННЯ ПІДГОТОВКИ КАДРІВ БЕЗПЕКОВОГО СЕКТОРУ

Сучасний безпековий простір вирізняється безпрецедентною динамікою, що зумовлена ескалацією гібридних загроз, технологічною конвергенцією та глобалізацією конфліктів. У цьому контексті ефективність національної системи безпеки детермінується не лише технологічною перевагою, а й переважно рівнем підготовки людського капіталу. Еволюція концепцій національної безпеки свідчить про циклічне переосмислення ролі та функцій відповідних інституцій її формування, забезпечення й реалізації. Вимоги до фахівців сектору безпеки значно розширилися: від класичних моделей, орієнтованих на військове стримування, до сучасних, що охоплюють кіберпростір, економічну стабільність, інформаційну протидію та стійкість критичної інфраструктури. Гібридні загрози поєднують цифрові, інформаційні, економічні й психологічні операції. Протидія їм вимагає від кадрів не лише спеціалізованих технічних навичок, а й розвиненого стратегічного мислення, здатності до комплексного аналізу та прийняття рішень в умовах невизначеності.

Як засвідчує практика, для частини персоналу сектору безпеки та оборони початкові декларації про наміри «служити та захищати» виявилися суто формальними й не були підкріпленими внутрішньою готовністю до ефективного протистояння агресору. Це стало індикатором того, що система професійної підготовки кадрів, сформована у попередні періоди, не забезпечувала належного рівня готовності й не витримала випробувань в умовах надзвичайно складного етапу, спричиненого запровадженням правового режиму воєнного стану.

Суспільно-політичний контекст, що сформувався в Україні після 24 лютого 2022 року, спричинив переосмислення усталених уявлень щодо дієвості фундаментальних принципів правового виховання в освітній системі, а також релевантності та функціональності низки методів добору персоналу, зокрема тих, що ґрунтуються на мотиваційних чинниках до професійної діяльності [4, с. 61].

Сучасна система підготовки кадрів, зокрема для сектору безпеки, потребує кардинального оновлення, з огляду на наявні зовнішні та внутрішні фактори, а також технічний прогрес. Аналіз діяльності навчальних закладів, що здійснюють підготовку фахівців для правоохоронних органів України, підтверджує, що застосування віддаленого (дистанційного) освітнього формату в період епідеміологічних обмежень, спричинених вірусом SARS-CoV-2, зумовило пріоритетність самостійної роботи й саморозвитку здобувачів освіти. Натомість через запровадження режиму воєнного стану та значне залучення кадрів до оперативної діяльності посилену увагу зосереджено на набутті практичних навичок [4, с. 64], зокрема у сфері цифрових технологій.

Інтенсивна еволюція інформаційно-комунікаційних технологій зумовила кардинальні перетворення у системі професійної підготовки. Це відбулося завдяки впровадженню інноваційних методик поширення знань і формування ключових компетентностей. У контексті України інкорпорація передових цифрових інструментів у фахову підготовку спеціалістів безпекового сектору є визначальним фактором забезпечення їхньої оперативної готовності до ефективного виконання службових зобов'язань у поточних геополітичних умовах [1, с. 38].

Дистанційне навчання, інтерактивні цифрові платформи й технології штучного інтелекту (ШІ) створюють безпрецедентні перспективи для всіх суб'єктів освітнього процесу. Ці технологічні інновації не лише демократизують доступ до інформації та освітнього контенту, а й кардинально трансформують дидактичну парадигму, забезпечуючи її гнучкість, персоналізацію та підвищену ефективність.

Завдяки розвитку глобальних комунікаційних мереж і впровадженню передових цифрових освітніх платформ, здобуття освіти стало загальнодоступним незалежно від географічного розташування. Різноманітні формати дистанційного навчання, такі як онлайн-курси, віртуальні семінари й інтегровані освітні програми, надають здобувачам освіти значну автономію у виборі графіка та швидкості опанування матеріалу [5].

Наразі у процесі підготовки здобувачів освіти важливого значення набуває така цифрова технологія, як ШІ. Його використання уможливлює розроблення індивідуалізованих навчальних траєкторій, враховуючи унікальні потреби та когнітивні стилі кожного здобувача освіти. Алгоритми машинного навчання здійснюють аналіз академічних показників, забезпечуючи студентів і курсантів навчальним контентом та завданнями, що відповідають їхньому актуальному рівню знань і можливостям. Концепція інтеграції ШІ в освітній процес передбачає синергетичну взаємодію між автоматизованими системами та людським викладацьким складом. Її основна ідея полягає у використанні оптимальних характеристик кожної сторони для досягнення максимальної ефективності навчання та сприяння найвищим освітнім результатам для всіх здобувачів знань.

Упровадження ШІ в освітню сферу сприяє автоматизації численних аспектів педагогічної діяльності. Це охоплює формування персональних планів навчання, комп'ютеризовану перевірку робіт, адаптивне оцінювання, а також підтримку викладацького складу під час аналізу успішності й контролю знань студентів. ШІ надає ефективний інструментарій для аналізу освітніх даних. Моніторинг прогресу, ідентифікація слабких місць і прогнозування академічних досягнень стають точними й оперативними завдяки алгоритмічним рішенням ШІ, що сприяє оптимізації освітніх стратегій та раціональному використанню ресурсів [3, с. 175, 178–179].

Водночас інтенсифікація використання інтернет-ресурсів слугує для впровадження в освітній процес ще однієї складової – кібербезпеки. Спеціалісти цієї сфери повинні володіти не лише технічними компетенціями, а й глибоким усвідомленням стратегічних і тактичних аспектів цієї дисципліни. Кібербезпека часто асоціюється переважно з інженерно-технічними заходами захисту інформаційно-комунікаційних систем від різноманітних кіберзагроз, зокрема несанкціонованих втручань, шкідливого програмного забезпечення та інших протиправних дій у кіберпросторі. Це вимагає від спеціалістів компетентності у сфері ідентифікації та аналізу потенційних загроз, розроблення архітектури кіберзахисту, імплементації передових криптографічних рішень, а також оптимізації механізмів виявлення вторгнень. Проте кібербезпека також потребує поглибленого дослідження суб'єктивного чинника, оскільки методи соціальної інженерії та фішингові кампанії часто виявляються надзвичайно ефективними векторами для несанкціонованого доступу. Експерти мають усвідомлювати психологічні аспекти поведінки потенційних жертв і формувати ефективні превентивні стратегії для протидії загрозам, що ґрунтуються на маніпуляції людською поведінкою.

Невід'ємною складовою сучасної кібербезпеки є цифрова криміналістика та розслідування інцидентів, пов'язаних з кіберзлочинністю. Для цього спеціалісти повинні володіти глибокими знаннями в галузі збирання, аналізу та збереження цифрових доказів з метою забезпечення подальшого юридичного переслідування суб'єктів кіберзлочинів [2, с. 654].

Ще одним з основоположних напрямів упровадження інформаційних технологій у професійну підготовку фахівців безпекового сектору, на якому слід зосередити увагу, є використання симуляційних комплексів і технологій віртуальної реальності. Віртуальні симуляційні платформи забезпечують можливість відпрацювання практичних навичок у середовищі, максимально наближеному до реальних обставин, без потенційного ризику для життя та здоров'я. Використання віртуальних симуляцій дає змогу моделювати різноманітні сценарії – від оперативних тактичних дій до комплексного кризового менеджменту, що суттєво підвищує ефективність освітнього процесу й адаптивні можливості майбутніх кадрів [1, с. 39].

Отже, підготовка кадрів для сектору безпеки в сучасних умовах є неперервним, стратегічно важливим процесом, що потребує глибокого наукового підґрунтя та постійної адаптації. Перехід від традиційних, вузькоспеціалізованих моделей до інтегрованого, інтердисциплінарного підходу, поєднаного з активним упровадженням інноваційних технологій, є ключовою умовою формування висококваліфікованого, адаптивного й етично орієнтованого персоналу. Інвестиції у людський капітал сектору безпеки є запорукою стійкості національної безпеки в умовах перманентної трансформації світового порядку.

Список використаної літератури

1. Богуславський В. В. Сучасні інформаційні технології у підготовці фахівців сектору безпеки та оборони: вітчизняний та міжнародний досвід. *Педагогічні науки* : зб. наук. праць / гол. ред. Л. А. Пермінова. Івано-Франківськ : ХДУ, Вип. 112. С. 38–43.

2. Булавка С. О., Комих Н. Г. Підготовка фахівців для сектору безпеки і оборони. *Міжнародна та національна безпека: теоретичні і прикладні аспекти* : матеріали VIII Міжнар. наук.-практ. конф. (Дніпро, 15 бер. 2024 р.); у 2-х ч. Дніпро : ДДУВС, 2024. Ч. ІІ. С. 651–654.

3. Гуревич Р. С., Коношевський Л. Л., Коношевський О. Л., Воєвода А. Л., Люльчак С. Ю. Інтеграція штучного інтелекту в сферу освіти: проблеми, виклики, загрози, перспективи. *Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми.* 2024. Вип. 72. С. 171–187.

4. Гусарєв С. Д., Старицька О. О. Формування професійної культури поліцейських у сучасній Україні: форми та зміст. *Альманах права.* 2022. Вип. 13. С. 61–67. DOI: 10.33663/2524-017X-2022-13-9

5. Як технології трансформують освіту та онлайн-навчання. *Юридична газета.* 2026. URL: https://yur-gazeta.com/publications/sferi-praktiki/lifestyle/yak-tehnologiyi-transformuyut-osvitu-ta-onlaynnavchannya.html

Козаченко Ганна Володимирівна, *професор кафедри економіко-правових дисциплін НАВС, доктор економічних наук, професор;*
Фаїзов Анатолій Вікторович, *завідувач кафедри економіко-правових дисциплін НАВС, кандидат економічних наук, доцент*

ЗАПОБІГАННЯ КОРУПЦІЇ В ПУБЛІЧНИХ ЗАКУПІВЛЯХ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Публічні закупівлі в умовах воєнного стану в Україні перебувають у зоні підвищеного ризику, що зумовлює неодмінне використання ризик-орієнтованого підходу до їхнього аудиту, в якому значну увагу приділено аналізу корупційних ризиків. Зростання корупційних ризиків при веденні тендерної діяльності в умовах воєнного стану, необхідність суттєвого посилення контролю за її процедурами зумовлюють необхідність використання в аудиті публічних закупівель настанови GUID 5280 «Керівництво з аудиту публічних закупівель» [1].