сучасної вищої освіти це передбачає аналіз текстів і проведення досліджень за напрямами професійної діяльності.

Зразком для військово-наукової аналітики може слугувати вивчення військово-історичного досвіду, зокрема – аналіз сучасних локальних збройних конфліктів. Існує безліч цікавих фактів, пов'язаних із військовим мистецтвом, які здатні зацікавити сучасного курсанта. Це формує атмосферу змістовного, продуктивного діалогу, в якому здобувач освіти усвідомлює важливість своєї майбутньої служби. У цьому переконливим аргументом слугує діяльність силових структур у провідних країнах світу.

Курсанти виявляють інтерес до матеріалів, що висвітлюють розвиток сучасного силового сектору держави. Уміння працювати з текстом є базовою компетенцією, яка лежить в основі професійного становлення майбутнього військового лідера. Ця навичка розвивається передусім під час особистих виступів, участі в дискусіях та апробації результатів власного дослідження.

У процесі опрацювання конкретної теми майбутній офіцер вчиться елементам грамотного професійного планування.

Вкрай важливою є роль викладача, який має виступати не лише як наставник, а й як модератор навчального процесу. Такий підхід розвивається завдяки педагогічній майстерності, досвіду та постійному самовдосконаленню викладача.

Звичайно, обсяг цих тез не дає змоги охопити всі напрями, необхідні для покращення якості освіти у вищих військових навчальних закладах. Проте зазначені аспекти, на нашу думку, є ключовими для системного розвитку.

Чорненький Володимир,
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Терещенко Олексій,
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Зайко Віктор,
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

АНАЛІЗ СУЧАСНОГО СТАНУ ТА НАПРЯМІВ РОЗВИТКУ СПРОМОЖНОСТЕЙ СУБ'ЄКТІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Упродовж останніх років сектор безпеки і оборони України зазнав суттєвих змін, що обумовлено насамперед масштабною військовою агресією проти нашої держави. В умовах повномасштабної війни постало нагальне завдання — не лише зберегти функціональність ключових

суб'єктів сектору безпеки і оборони, але й забезпечити їхню адаптацію до нових викликів та ефективну трансформацію відповідно до сучасних потреб. Цей сектор охоплює органи військового управління, оборонні сили, сили безпеки, розвідувальні та спеціальні служби, а також інші державні органи, чия діяльність безпосередньо або опосередковано спрямована на забезпечення національної безпеки.

Аналізуючи поточний стан зазначених суб'єктів, варто зауважити, що значною мірою збереження їхньої боєздатності, організаційної цілісності та готовності до виконання завдань стало можливим завдяки гнучкому управлінню, швидкій адаптації до змін та потужній міжнародній підтримці. Водночас стратегічно важливими залишаються питання стандартизації процедур та спроможностей відповідно до принципів НАТО, удосконалення міжвідомчої координації, а також формування єдиного інформаційного простору оборонного призначення.

До основних напрямів розвитку спроможностей сьогодні можна віднести: впровадження цифрових технологій в управлінні оборонними процесами; розвиток інфраструктури кіберзахисту; модернізацію матеріально-технічної бази; удосконалення системи професійної підготовки персоналу та підвищення морально-психологічної стійкості особового складу. Варто також наголосити на необхідності глибокого осмислення отриманого бойового досвіду з метою його подальшого системного врахування у процесах формування спроможностей сектору в мирний час.

Не менш важливою є й трансформація управлінських та командних підходів. Досвід війни засвідчив ефективність децентралізованих моделей управління, гнучкості в ухваленні рішень і автономії на тактичному рівні. Натомість централізовані, бюрократизовані системи, орієнтовані на мирний час, часто виявляються недостатньо ефективними в умовах динамічного конфлікту. У цьому контексті доцільно говорити про необхідність подальшої доктринальної переоцінки функціонування всього сектору безпеки і оборони.

Попри позитивні зміни, існує низка об'єктивних бар'єрів: обмеженість фінансових і людських ресурсів, дефіцит висококваліфікованих фахівців, а також потреба в глибшій нормативно-правовій узгодженості між суб'єктами сектору. Також зростає актуальність розвитку оборонно-промислового комплексу, спроможного забезпечити потреби сектору в національному вимірі.

Отже, підвищення спроможностей суб'єктів сектору безпеки і оборони України — це не лише питання модернізації техніки чи вдосконалення організаційних структур. Це насамперед потребує глибокого переосмислення стратегічних засад безпеки. На мою думку, успішне реформування можливе за умови системного підходу, здатності поєднувати тактичні дії з довгостроковими національними пріоритетами та вміння робити висновки з власного бойового досвіду.

Дуже важливо, щоби всі суб'єкти сектору діяли як єдиний злагоджений механізм, а не як розрізнені інституції зі своїми відомчими інтересами. Не менш значущим є створення нової управлінської культури, заснованої на підтримці ініціативності, відповідальності, партнерських взаємин і відкритості до інноваційних підходів. Ми вже зробили багато, але попереду — не менше. І наше завдання як науковців, аналітиків і фахівців — не просто спостерігати, а пропонувати рішення, які допоможуть наблизити перемогу й забезпечити стабільність у повоєнний період.

Ярема Владислав,
кафедра соціально-гуманітарних та правових дисциплін
Київський інститут Національної гвардії України

Мацюк Микола,
курсант 214 н. гр.
факультету забезпечення державної безпеки,
Київський інститут Національної гвардії України

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ КІБЕРБЕЗПЕКИ У СЛУЖБОВО-БОЙОВІЙ ДІЯЛЬНОСТІ

Сучасний характер збройних конфліктів докорінно змінюється через стрімке поширення інформаційних технологій та зростання ролі кіберпростору. У службово-бойовій діяльності Національної гвардії України та інших структур сектору безпеки й оборони кібербезпека вже стала одним з ключових елементів забезпечення боєздатності та оперативної ефективності.

На сьогодні важливою перспективою розвитку кібербезпеки у службово-бойовій діяльності є впровадження стандартів НАТО, які дозволяють не лише уніфікувати підходи до захисту інформації, але й створити спільний простір взаємодії з міжнародними партнерами. Впровадження цих стандартів є ключовою умовою успішної інтеграції України до євроатлантичної системи безпеки. Проте, на мою думку, для досягнення реального ефекту важливо не просто переймати стандарти, а формувати власні підходи з урахуванням практичного бойового досвіду, зокрема здобутого з 2014 року на сході України.

Ще одним перспективним напрямком розвитку є формування гібридної моделі кібербезпеки, яка передбачає ефективне поєднання військових і цивільних механізмів. Це дасть змогу більш результативно протидіяти комплексним кібератакам, що загрожують як критичній інфраструктурі, так і безпосередньо військовим операціям. На думку Пономарьова О. А. та його колег, інтеграція військово-цивільного компонента створює умови для гнучкої та стійкої системи кіберзахисту.

Нормативно-правове забезпечення — ще одна фундаментальна складова. Сироватченко М. зазначає, що українське законодавство у сфері кібербезпеки має оновлюватися відповідно до стандартів НАТО та ЄС, із чітким визначенням