Сергій БІЛЕЦЬКИЙ,
кандидат технічних наук, доцент,
старший науковий співробітник доцент кафедри
"Безпека праці та навколишнього середовища"
Національного технічного університету
“Харківський політехнічний інститут”
м. Харків, Україна
ORCID: https://orcid.org/0000-0001-9695-2070
e-mail: Serhii.Biletskyi@mit.khpi.edu.ua

Ростислав ЧЕРЕПАХА,
старший викладач кафедри
"Безпека праці та навколишнього середовища"
Національного технічного університету
“Харківський політехнічний інститут”
м. Харків, Україна
ORCID: https://orcid.org/0000-0002-4903-2535
e-mail: Rostyslav.Cherepakha@mit.khpi.edu.ua

DOI: https://doi.org/10.32620/pls.2025.8.47

БАЗОВА ЗАГАЛЬНОВІЙСЬКОВА ПІДГОТОВКА ЯК СКЛАДОВА СЕКТОРУ БЕЗПЕКИ Й ОБОРОНИ В ЧАСТИНІ ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація: *У роботі сформульовані основні проблеми впровадження базової загальновійськової підготовки (БЗВП) у складову сектору безпеки й оборони України. Сконцентровано увагу на підвищення інтелектуального потенціалу та професійної майстерності військовослужбовців ЗС України та подальшу інтеграцію основ кіберзахисту у базову загальновійськову підготовку.*

Ключові слова: *критична інформаційна інфраструктура, базова загальновійськова підготовка, кіберзагроза.*

У контексті збройної агресії Російської Федерації проти України особливо важливо забезпечити Сектор безпеки й оборони, до якого входять Збройні Сили України, Служба безпеки України, Національна гвардія, Державна служба спеціального зв’язку та захисту інформації (ДССЗЗІ) та інші структури достатньою кількістю підготовлених до служби громадян. Це необхідно для виконання обов’язків у запасі, проходження служби у військовому резерві та участі у бойових діях. Крім того, важливо надати громадянам можливість обирати військову професію, здобуваючи відповідні знання, навички та вміння, які потрібні як для виконання військових обов’язків у мирний час, так і для служби під час війни, а також для подальшої професійної реалізації. Всі складові сектору оборони проводити постійну роботу по інтеграції підготовку фахівців з кіберзахисту у військову освіту.

Враховуючи складну військово-політичну обстановку в країні та застосування противником нових форм і методів ведення бойових дій, набуває все більшої актуальності підвищення інтелектуального потенціалу та професійної майстерності військовослужбовців ЗС України та інших співробітників правоохоронних органів. При проведенні бойових дій військові стикаються з озброєним і добре фізично підготовленим противником, що вимагає від них вміння тактично грамотно оцінювати обстановку, керувати підпорядкованими підрозділами, впевнено орієнтуватись на місцевості, ефективно використовувати зброю, злагоджено вести бойові дії.

Аналіз останніх публікацій щодо стану підготовки кадрів для сектору безпеки та оборони свідчить про необхідність впровадження комплексу заходів, спрямованих на його удосконалення і, на наш погляд, доречним є наступні заходи:

- на первинних етапах стратегічне визначення кількості категорій військових фахівців, необхідних для формування і остаточного визначення структури військової освіти;
- посилення роботи щодо якості підбору кадрів в секторі безпеки та оборони України, унеможливлення формального ставлення до якості проведення фізичного відбору, психологічного обстеження та інше;
- налагодження співпраці з міжнародними організаціями з метою отримання і узагальнення зарубіжного досвіду підготовки кадрів для сил безпеки і оборони держави, перейняття досвіду;
- підвищення інтенсивності та короткостроковості навчання фахівців, які здатні діяти у складі

бойової групи та самостійно у різних погодних та географічних умовах, вдень та вночі;

- збільшення практичної складової шляхом наближення проведення занять до реальних бойових умов з метою отримання навичок дій у складі підрозділу, а також навичок керування підрозділами у різних умовах бойової обстановки;

На сучасному етапі найбільш прийнятним і доцільним є навчання молоді, перепідготовка фахівців та підвищення кваліфікації діючих військовослужбовців ЗС України та інших працівників правоохоронних органів на підставі провідного досвіду країн світу, які досягли певних здобутків у визначеній галузі.

Останнім часом, в умовах зростання загроз національній безпеці нашій державі, стають актуальними питання реформування та подальшого розвитку сектору безпеки і оборони держави, який передбачає комплексні зміни у системі підготовки, перепідготовки та підвищення кваліфікації кадрів відповідно до стандартів провідних країн світу. Важливою складовою професійного навчання військовослужбовців ЗС України та інших правоохоронних органів є опанування основ критичної інформаційної інфраструктури (далі – КП), тобто сукупності інформаційних систем, мереж і ресурсів, від функціонування яких залежить національна безпека, обороноздатність, економічна стабільність і життєдіяльність суспільства. Головним змістом цієї підготовки є вдосконалення теоретичних знань, практичних навичок та вмінь особового складу під час бойових дій.

Через поєднання військових, технічних і освітніх заходів формується стійкість держави до кіберзагроз. Серед основних завдань сектору безпеки й оборони у сфері захисту критичної інфраструктури таких, як виявлення та протидія кіберзагрозам; моніторинг інформаційного простору; технічний захист інформації; створення захищених каналів зв'язку; координація діяльності державних органів у сфері кібербезпеки; взаємодія з міжнародними партнерами (НАТО, ЄС) щодо спільного реагування на кіберінциденти, – є і навчання та підготовка особового складу кіберграмотності.

Включення тем інформаційної безпеки до базової загальновійськової підготовки сприяє тому, що кожен військовослужбовець стає не лише захисником території, а й активним елементом кібероборони країни. В цьому напрямку нам вкрай необхідно зосередити увагу на подальшу інтеграцію основ кіберзахисту у базову загальновійськову підготовку, яка формує у військовослужбовців не лише бойові та тактичні навички, а й розуміння важливості інформаційної безпеки у таких напрямках, як:

- ознайомлення з основами кібергігієни (захист паролів, шифрування, уникнення фішингу);

- усвідомлення загроз інформаційного впливу противника;

- розуміння ролі інформаційної дисципліни в умовах війни (заборона розголошення службових даних, фото- та геолокацій);

- використання захищених каналів зв'язку у тактичній ланці.

Захист інформації є одним із пріоритетів державної політики у сфері національної безпеки.

Бібліографічні посилання

1. Закон України «Про військовий обов'язок і військову службу». https://zakon.rada.gov.ua/laws/show/2232-12#n1713

2. Закон України «Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку» (№ 3633-IX), який набрав чинності 18 травня 2024 року.

3. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року № 287/2015 http://zakon5.rada.gov.ua/laws/show/287/2015

4. ПКМУ від 21 червня 2024 р. № 734 «Про затвердження Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських» https://zakon.rada.gov.ua/laws/show/734-2024-%D0%BF#Text

5. Міністерство оборони України. БЗВП у закладах вищої освіти: що потрібно знати. https://mod.gov.ua/news/bzvp-u-zakladah-vishhoyi-osviti-shho-potribno-znati

6. Міністерство освіти України. Започаткування теоретичної частини БЗВП для студентів. https://mon.gov.ua/static objects/mon/sites/1/vishcha-osvita/2025/03/05/bazova-zahalnoviyskova-pidhotovka-zdobuvachiv-vyshchoyi-osvity-05-03-2025.pdf

S. Biletskyi, R. Cherepakha

Basic general military training as a component of the security and defense sector in the part of critical information infrastructure protection.

Abstract: The paper formulates the main problems of implementing basic combined military training (BCMT) as part of the security and defense sector of Ukraine. The focus is on increasing the intellectual potential and professional skills of servicemen of the Armed Forces of Ukraine and further integrating the basics of cyber defense into basic combined military training.

Keywords: critical information infrastructure, basic combined arms training, cyber threat.

Зразок для цитування:

Білецький С., Черепаха Р. Базова загальновійськова підготовка як складова сектору безпеки й оборони в частині захисту критичної інформаційної інфраструктури. Пропілеї права та безпеки, 2025. №8. С. 194-195. DOI: https://doi.org/10.32620/pls.2025.8.47.