збору інформації безпосередньо у підрозділах. Третім напрямом виступає стандартизація підходів до обліку та звітності, що дозволить забезпечити достовірність і зіставність даних.

Четвертим напрямом впровадження сучасних аналітичних інструментів, зокрема технологій Big Data [6] та машинного навчання, для прогнозування потреб у особовому складі та підтримки прийняття рішень.

П'ятим напрямом є посилення кіберзахисту інформаційних систем з метою протидії інформаційним і кіберзагрозам з боку противника.

Реалізація зазначених заходів сприятиме підвищенню стійкості та результативності функціонування системи збору, обробки та аналізу даних щодо укомплектованості особовим складом, що є важливою умовою забезпечення національної безпеки України в умовах тривалої війни.

Таким чином, виклики, які постають перед цією системою в умовах політики російської федерації, спрямованої на затягування війни, мають комплексний характер і потребують системного вирішення шляхом застосуванням сучасних організаційних та технологічних підходів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Косевцов В., Тіхонов Г., Чайковська О., Онікійчук С. Система збору та аналізу інформації про укомплектованість військових частин особовим складом // Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2025. № 3(86). С. 86-114. DOI: https://doi.org/10.33099/2304-2745/2025-3-86/106-114.
2. Порохня І. М., Кінь Н. В. Система інформаційно-аналітичного забезпечення органів військового управління: проблеми функціонування // Сучасні інформаційні технології у сфері безпеки та оборони. 2025. № 3(54). С. 84-92. DOI: https://doi.org/10.33099/2311-7249/2025-54-3-84-92.
3. Паращук Л. Я., Паращук С. М. Рекомендації стосовно використання інформаційних систем для покращення ситуаційної обізнаності органів військового управління // Сучасні інформаційні технології у сфері безпеки та оборони. 2025. № 1(52). С. 46-54. DOI: https://doi.org/10.33099/2311-7249/2025-52-1-46-54. URL: https://sit.nuou.org.ua/article/view/322311.
4. NATO. Allied Joint Doctrine for the Conduct of Operations (AJP-3). Brussels: NATO Standardization Office, 2019. P. 1-30. URL: https://www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf.
5. Alberts D. S., Hayes R. E. Understanding Command and Control. Washington: CCRP, 2006. P. 33-55. URL: https://www.dodccrp.org/files/Alberts_UC2.pdf.
6. Кондрусь А. В. та ін. Використання технологій Big Data у процесі управління військами // Системи і технології зв'язку, інформатизації та кібербезпеки. 2023. № 3. С. 41-47. DOI: https://doi.org/10.58254/viti.3.2023.05.41

ПОНОМАРЕНКО ВІКТОР ВОЛОДИМИРОВИЧ
викладач кафедри адміністративного права та процесу навчально-наукового інституту права та соціального менеджменту Донецький державний університет внутрішніх справ

КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У сучасному світі, де інформаційні технології проникають практично в усі сфери життя, питання кібербезпеки перестає бути суто технічним і набуває стратегічного значення для держави. Україна, перебуваючи в умовах тривалої збройної агресії, особливо гостро відчуває вплив кіберзагроз, які використовуються як один із інструментів гібридної війни. Саме тому

кібербезпека сьогодні виступає невід'ємною складовою національної безпеки та потребує комплексного підходу до її забезпечення.

Нормативною основою у цій сфері є Конституція України [1], Закон України «Про національну безпеку України» [2] та Закон України «Про основні засади забезпечення кібербезпеки України» [3]. Вказані акти визначають загальні підходи до розуміння кібербезпеки, окреслюють коло суб'єктів, відповідальних за її забезпечення, та встановлюють базові принципи державної політики у цій сфері. Водночас варто зазначити, що законодавче регулювання не завжди встигає за стрімким розвитком технологій, що створює певні труднощі у практичній площині.

Кіберзагрози сьогодні мають різноманітний і складний характер. Йдеться не лише про класичні хакерські атаки, але й про втручання у функціонування державних інформаційних систем, атаки на об'єкти критичної інфраструктури, поширення шкідливого програмного забезпечення, а також інформаційно-психологічні впливи. Особливістю таких загроз є їхня швидкість, масштабність і часто – складність у встановленні джерела походження. Усе це суттєво ускладнює процес їх нейтралізації та вимагає нових підходів до організації системи кіберзахисту.

Важливо розуміти, що кібербезпека – це не лише питання технологій, але й питання права та управління. Вона передбачає чітке визначення повноважень різних органів, налагодження взаємодії між ними, а також встановлення відповідальності за порушення у кіберпросторі. При цьому важливим є дотримання балансу між забезпеченням безпеки та захистом прав людини, зокрема права на приватність і свободу інформації.

Окремої уваги потребує питання захисту критичної інфраструктури. Енергетика, транспорт, банківська система, зв'язок – усі ці сфери сьогодні значною мірою залежать від стабільної роботи інформаційних систем. Відповідно, кібератаки на такі об'єкти можуть мати серйозні наслідки не лише економічного, а й соціального характеру. Саме тому держава має приділяти особливу увагу впровадженню ефективних механізмів їх захисту.

У цьому контексті дедалі більшого значення набувають інноваційні технології. Використання штучного інтелекту, аналізу великих даних, автоматизованих систем виявлення загроз дозволяє підвищити ефективність кіберзахисту. Проте, впровадження таких рішень також потребує належного правового забезпечення та контролю, адже існують ризики зловживань або помилок у їх функціонуванні.

Разом з тим, сучасний стан забезпечення кібербезпеки в Україні не можна вважати ідеальним. Серед основних проблем можна виділити недостатній рівень координації між різними суб'єктами, обмеженість ресурсів, а також нестачу кваліфікованих спеціалістів. Крім того, швидкий розвиток технологій призводить до появи нових загроз, на які система безпеки не завжди встигає своєчасно реагувати.

Вирішення цих проблем можливе лише за умови комплексного підходу. По-перше, необхідно вдосконалювати законодавство з урахуванням сучасних викликів. По-друге, слід посилювати інституційну спроможність органів, відповідальних за кібербезпеку. По-третє, важливо розвивати міжнародне співробітництво, адже більшість кіберзагроз має транскордонний характер. І, нарешті, не менш важливим є підвищення рівня кіберграмотності населення, оскільки людський фактор часто залишається найуразливішим елементом у системі безпеки.

Отже, кібербезпека сьогодні є одним із ключових елементів національної безпеки, який безпосередньо впливає на стабільність держави та її здатність протидіяти сучасним загрозам. В умовах цифровізації та воєнного стану значення цього напряму лише зростає, що обумовлює необхідність його подальшого розвитку як на нормативному, так і на практичному рівнях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

2. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України.* 2018. № 31. Ст. 241.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради.* 2017. № 45. Ст. 403.