УДК 342.951

ЖЕРЕБЕЦЬ О.М., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-2059-2045.

ОГЛЯД КРАЩИХ ПРАКТИК ЗАРУБІЖНОГО ДОСВІДУ ТА НОВЕЛ ЗАКОНОДАВСТВА ЩОДО СТВОРЕННЯ ТА ФУНКЦІОНУВАННЯ КІБЕРВІЙСЬК (НА ПРИКЛАДІ ПОЛЬЩІ ТА ЧЕХІЇ)

Анотація. *Визначені загальні тенденції та особливості становлення кібервійськ у таких країнах як Польща та Чехія. Проаналізовано заходи, присвячені створенню кібервійськ у вказаних країнах-членах НАТО. Розглянуто компетенцію, повноваження та функціональні завдання практичної діяльності відповідальних кіберпідрозділів. Узагальнено особливості використання кібервійськ у рамках проведення оборонних та наступальних кібероперацій. На підставі узагальнення позитивного польського та чеського досвіду створення кібервійськ окреслено перспективи законодавчого забезпечення інституційного утворення кіберсил в Україні.*

Ключові слова: *кібероборона, кібероперація, кібердомен, кібервійська, кіберкомандування, кіберсили, НАТО.*

Summary. *The general trends and features of the formation of cyber forces in countries such as Poland and the Czech Republic are determined. The measures devoted to the creation of cyber forces in the mentioned NATO countries have been analyzed. The competence, powers and functional tasks of the practical activities of the responsible cyber units were considered. The peculiarities of the use of cyber troops in the framework of conducting defensive and offensive cyber operations are summarized. Based on the generalization of the positive Polish and Czech experience of creating cyber forces, the prospects of legislative support for the institutional formation of cyber forces in Ukraine are outlined.*

Keywords: *cyber defense, cyber operation, cyber domain, cyber troops, cyber command, cyber forces, NATO.*

Постановка проблеми. В епоху постійної та динамічної зміни ландшафту глобальних кіберзагроз, масштабування та шаленої чисельності кібератак, перманентних посягань на об`єкти критичної інфраструктури, необхідність мілітаризації кіберпростору постійно та динамічно зростає. Очікуваною реакцією на це у багатьох країнах світу став тренд утворення спеціальних підрозділів – кібервійськ, які активно використовуються як для військових, так і розвідувальних цілей у кіберпросторі. У свою чергу, спеціалізовані підрозділи із кібербезпеки офіційно використовуються у 60 країнах світу, а неофіційно – вже майже у сотні іноземних держав. За таких умов важливою складовою забезпечення кібербезпеки є створення та розвиток національних кібервійськ. Завданнями цих підрозділів є ведення збройного протиборства в кіберпросторі, практична реалізація та впровадження організаційно-технічної моделі кіберзахисту, забезпечення взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони між собою під час проведення заходів з кібероборони, організація навчання та фінансового забезпечення таких структур, систематичне проведення кібернавчань тощо.

В Україні на державному рівні у 2021 року на порядку денному перебувало питання про створення власних кібервійськ. Зокрема Указом Президента України від

26 серпня 2021 року, яким було введено в дію рішення РНБО "Про невідкладні заходи з кібероборони держави" [1], була проголошена необхідність створення у системі Міністерства оборони України кібервійськ з метою захисту суверенітету держави, забезпечення її обороноздатності, відсічі збройній агресії у кіберпросторі. План реалізації Стратегії кібербезпеки України, затверджений рішенням РНБО України від 30 грудня 2021 року та введений в дію Указом Президента України від 1 лютого 2022 року [2], регламентував інституційні засади створення у системі Міністерства оборони України кібервійськ (кіберсил) протягом першого півріччя 2023 року. Пункт 2 Плану заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України, затверджений Розпорядженням Кабінету Міністрів України від 19 грудня 2023 року [3] передбачає створення кібервійськ в системі Міноборони протягом 2024 року та одночасне їхнє забезпечення належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії в кіберпросторі та надання відсічі агресору. Проте, на жаль, задекларовані ініціативи щодо створення кібервійськ залишаються нереалізованими, а це питання відкритим. За таких умов, дослідження кращих практик досвіду країн-членів НАТО та союзників України, з якими протягом 2024 року наша держава уклала безпекові угоди (Польща, Чехія) стосовно створення та функціонування кібервійськ, що є актуальним та своєчасним.

Результати аналізу наукових публікацій. Проблематику створення кібервійськ у зарубіжних країнах досліджували у своїх наукових працях: О. Горун [4], О. Федієнко [5], Н. Ткачук [6], В. Чевардін та О. Мазулевський [7], В. Фіца [8]. Проте жоден їх вказаних авторів предметно не розглядав особливості нормативного забезпечення інституційного створення та функціонування кібервійськ у таких країнах-членах НАТО, як Польща та Чехія. Висвітлення та узагальнення польського і чеського досвіду у сфері утворення та розбудови кібервійськ надасть змогу адаптувати його кращі практики до вітчизняних реалій. Прагнення України прискорити створення власних кібервійськ в умовах правового режиму воєнного стану підкреслює актуальність цієї статті.

Метою статті є узагальнення сучасних тенденцій та визначення особливостей польської та чеської моделей нормативного забезпечення функціонування кібервійськ для розроблення правової та організаційної, технологічної моделі функціонування кібервійськ України з урахуванням європейського досвіду.

Виклад основного матеріалу. У переважній більшості країн світу існує стійка тенденція до значного збільшення кількості та розширення спектру кібератак, спрямованих на порушення конфіденційності, цілісності і доступності державних інформаційних ресурсів, зокрема й тих, що забезпечують функціонування об'єктів критичної інфраструктури. Кібербезпека на теренах НАТО визнана важливою складовою національної безпеки, забезпечення якої здійснюється на підставі єдиної загальнодержавної скоординованої політики у цій сфері, яка ґрунтується на засадах поваги до норм і принципів міжнародного права, забезпечення національних пріоритетних інтересів у кіберпросторі, ефективної протидії у кібердомені. Загальною усталеною практикою цих країн є чітке доктринальне визначення концептуальних засад державної політики у сфері забезпечення безпеки у кіберпросторі у відповідних документах стратегічного планування.

На саміті НАТО у Вільнюсі 2023 року члени Альянсу схвалили нову концепцію посилення внеску кіберзахисту в загальну систему стримування та оборони НАТО. Концепція додатково інтегрує три рівні кіберзахисту НАТО – політичний, військовий і технічний, забезпечуючи цивільно-військову співпрацю з приватним сектором. Зміцнення кіберстійкості має ключове значення для того, щоб зробити Альянс більш безпечним і

здатним пом'якшувати потенціал значної шкоди від кіберзагроз. При цьому НАТО та її союзники покладаються у реалізації цих завдань на потужну та стійку систему кіберзахисту для виконання трьох основних завдань Альянсу: стримування та оборона; запобігання та врегулювання криз; спільна безпека.

Найважливішою з трьох основних задекларованих місій НАТО є стримування та оборона. Ключовими оборонними політичними та військовими процесами й функціями, пов'язаними з підтримкою, розвитком і впровадженням стримування, є оборонне планування на теренах НАТО, успішне виконання спільних оборонних завдань НАТО, у тому числі й проведення результативних операцій у кіберпросторі. Військово-політичне керівництво Альянсу констатує той факт, що потенційні супротивники, використовуючи кіберпростір, прагнуть погіршити критично важливу інфраструктуру НАТО, втручатися у роботу урядових служб, отримувати розвіддані, викрадати інтелектуальну власність і перешкоджати військовій діяльності. Росія також активізувала свої гібридні дії проти союзників по НАТО та партнерів, зокрема через деструктивну діяльність у кіберпросторі. Заявлені амбіції та політика Китаю є викликом інтересам, безпеці та цінностям НАТО. Зловмисні гібридні та кібероперації Китаю, а також конфронтаційна риторика та дезінформація спрямовані проти членів Альянсу. Така діяльність завдає шкоди безпеці країн членів НАТО. З метою сприяння виробленню спільного підходу щодо розвитку спроможності кіберзахисту в масштабах Альянсу, НАТО визначає цілі з реалізації країнами-членами національних можливостей посилення кіберзахисту, зокрема використовуючи процес оборонного планування НАТО в контексті утворення національних кібервійськ. Світовий досвід переконливо доводить, що створення кібервійськ значно посилює здатність протидіяти кіберагресії з боку країн-терористів (рф, кндр, білорусь, іран), а у стратегічній перспективі визнається конструктивною основою для подальшого розвитку кіберпотенціалу та кіберспроможностей тієї чи іншої держави.

Республіка Польща. У липні 2018 року в Польщі було ухвалено закон "Про національну систему кібербезпеки" [9], за результатами якого було створено перший підрозділ кібервійськ та відповідні структури: Національний центр кібербезпеки, Національна команда реагування на комп'ютерні інциденти (CERT.PL), Національний центр безпеки кіберпростору при міністерстві оборони Республіки Польщі. Прикладом ефективної консолідації сил та засобів з метою забезпечення кіберзахисту став Національний центр безпеки кіберпростору міністерства оборони Польщі, створений на базі Національного криптологічного центру (NCK) та IT-інспекції (I2). Ресурси та повноваження міністерства національної оборони Польщі у кібер-, крипто- та IT-сферах були консолідовані в одній установі, що дозволило поглибити співпрацю між фахівцями, відповідальними за ІКТ-безпеку та криптологічну підтримку, та підрозділами, відповідальними за закупівлю апаратного та програмного забезпечення, а також обслуговування відомчих мереж і систем.

На виконання рекомендацій НАТО у лютому 2019 року розроблено Концепцію організації та функціонування Сил оборони кіберпростору Польщі (CYBER.MIL.PL) [10], положення якої спрямовані на підвищення безпеки держави та громадян у кіберпросторі на 4 стратегічних рівнях. Перший – це консолідація та побудова власне структур кібербезпеки, другий – освіта, навчання та тренінги спеціалістів для кібербезпеки, третій – співпраця та побудова міцної міжнародної позиції із країнами партнерами, четвертий – підвищення рівня безпеки відомчих і військових мереж і систем Польщі. У рамках реалізації цієї Концепції було вжито заходів, спрямованих на консолідацію наявних ресурсів, активізації наукових досліджень та найму досвідченого персоналу, налагодження інтенсивної співпраці Національного центру безпеки

кіберпростору, Служби військової контррозвідки, Командування військ територіальної оборони, Військового інституту зв'язку та військових університетів і навчальних підрозділів. Одночасно було створено штаб-квартиру кіберкомандування цими військами при Національному центрі кібербезпеки.

Уряду Польщі знадобилося два повноцінних роки, щоб перейти від затвердження проекту концепту до його перших кроків практичної реалізації. Згодом Національний центр кібербезпеки було перейменовано на Національний центр кібербезпеки – Командування Сил оборони кіберпростору. В сучасних умовах у цій структурі працює близько 5 тис. військовослужбовців та цивільного персоналу. Функцію директора Національного центру безпеки кіберпростору взяв на себе Уповноважений Міністерства національної оборони з питань створення Сил оборони кіберпростору генерал Кароль Моленд.

18 березня 2022 року Президент Польщі підписав закон "Про оборону" [11], згідно з яким війська оборони кіберпростору являють собою спеціалізовану компоненту Збройних Сил, призначену для виконання повного спектру завдань у кіберпросторі, зокрема, не лише наступальних дій, але й проактивного захисту (постійного виявлення інструментів, методів, мотивації і процедур потенційних супротивників) та активної оборони (розпізнавання потенційних небезпек, загроз у кіберпросторі, безпосередніх дій). Передусім, процес створення польських Сил оборони кіберпростору ґрунтується на досвіді створення польських підрозділів спецназу, які на початку були спеціальним компонентом Збройних Сил Польщі, але згодом були трансформовані в окремий рід військ. Передбачено постійний штат кібервійськ Польщі у кількості 1 тис. осіб. Необхідні фахові оперативні спроможності кіберсил під керівництвом Міністра оборони мають бути сформовані до кінця 2024 року та у перспективі будуть передані в підпорядкування начальнику Генерального штабу Збройних Сил Республіки Польща. Водночас війська територіальної оборони Польщі були розширені за рахунок кіберкомпонента (територіальних кібергруп), де були відкриті вакансії для місцевих молодих спеціалістів. Сили оборони кіберпростору Польщі відповідають за безпеку кіберпростору та здатні проводити повний спектр операцій, включаючи оборону, розвідку та наступ, а також протидію психологічним та інформаційним операціям. Цей підрозділ відповідає за: забезпечення кібербезпеки Міністерства оборони; планування, організацію та використання кіберпростору; проведення оборонних та наступальних операцій у кіберпросторі; створення, підтримку та захист критичної інфраструктури та інформації в кіберпросторі; забезпечення підтримки військових операцій, що проводяться Збройними Силами Польщі, та операцій, які проводяться в рамках Альянсу; координацію з іншими державними установами, відповідальними за оборону; проведення досліджень та підготовку інноваційних рішень для виявлення інцидентів у кіберпросторі; проектування, створення, впровадження та використання національних криптологічних технологій і рішень для забезпечення інформаційної безпеки; розробку нових рішень у сфері сучасних технологій та криптографії; проведення освітніх і навчальних заходів; нагляд за роботою CSIRT MON, яка відповідає за моніторинг мереж МО 24/7 та захист польського кіберпростору.

У 2022 році Сили оборони кіберпростору Польщі підписали Меморандум про взаєморозуміння з НАТО щодо створення цілодобових контактних пунктів, відповідальних за координацію політики кібербезпеки та технічний аналіз кіберзагроз. Крім того, налагоджено співпрацю із Центром передового досвіду НАТО з питань кіберзахисту, розташованим в Естонії [12]. Також у вересні 2022 року Уряди України та Польщі підписали меморандум про співпрацю у сфері кіберзахисту з метою посилення

спільної боротьби зі злочинами у кіберпросторі та налагодження ефективного обміну досвідом й інформацією про кіберінциденти [13].

У 2022 році в Варшаві створили спеціальну Військову ІТ-школу, яка має готувати кандидатів до вступу до Військового технологічного університету з метою вивчення ІТ-сфери, криптологічного захисту інформації та кібербезпеки. Також були відкриті школи сержантського складу для підготовки кандидатів за фахом ІТ та зв'язок. Пізніше освітній компонент був розвинутий шляхом створення літніх шкіл з кібербезпеки та створення класів із профілем "Кібербезпека та сучасні ІТ-технології" в 16 середніх школах Польщі. Ця новація має збільшити кількість потенційних кандидатів, які бажають вивчати кібербезпеку у Військовому технологічному університеті та згодом потенційно приєднатися до армії. Польща також намагалася знайти волонтерів Сил територіальної оборони, які мають досвід у сфері ІТ або кібербезпеки. Ці зусилля призвели до створення малих допоміжних підрозділів – Групи дій у кіберпросторі, які підтримують Сили оборони польського кіберпростору. Під час скоординованих зусиль названі групи будуть виведені зі складу Сил територіальної оборони та підпорядковані Силам оборони кіберпростору Польщі.

Окрім того, Польща створила навчальний центр передового досвіду з кібербезпеки з метою покращення вмінь та навичок військовослужбовців у різних сферах кібербезпеки. Навчання у Центрі передбачає проведення різноманітних тренінгів та опанування спеціальних курсів для кіберсолдат з ІТ, криптографії та кібербезпеки. Польські військові не тільки прагнуть залучити більше особового складу, але й зберегти поточну кількість кібервійськових. Кожен кіберсолдат отримує спеціальну фінансову винагороду, що робить його зарплату ближчою до зарплати у приватному секторі. Масштаб цих переваг залежить від кваліфікації, набутого досвіду та посади.

Міністерство оборони Польщі проводить інші заходи щодо розвитку кіберсил в складі Збройних Силах Польщі. Наразі відбувається впровадження Плану під назвою "Cyber Mil 2.0" [14], який базується на таких принципах: подальший розвиток інфраструктурних проектів у сфері кібербезпеки; пошук та формування кадрового резерву; побудова паритетної міжнародної співпраці у рамках Альянсу. Завдяки успішній роботі кібервійськ ця країна посіла перше місце у Національному індексі кібербезпеки (National Cyber Security Index) [15]. Зокрема Польща здобула 90,83 бала зі 100 можливих. Вона обігнала Австралію (87,50) та Естонію (85,83). До списку увійшли 32 країни з різних куточків світу. Національний індекс кібербезпеки оцінює готовність країн запобігати кіберзагрозам. При оцінці до уваги беруться заходи, націлені на посилення кібербезпеки, які впроваджуються центральними органами влади. За результатами дослідження, в якому оцінюється рівень інформаційно-технологічної безпеки та запобігання кіберзагрозам різних держав світу, з'ясувалося, що саме ця країна найчастіше піддається DDoS-атакам. Незалежні експерти чітко вказують, що більшість атак на польські ресурси виходять саме з Росії, і вони переважно пов`язані з війною в Україні та польською логістикою, зокрема транспортною інфраструктурою.

У вересні 2024 року за сприяння кібервійськ спецслужбам Польщі вдалося викрити та припинити діяльність мережі російських та білоруських кібердиверсантів, які планували проникнути у системи державних органів влади та місцевого самоврядування аби викрасти службову інформацію. Кінцевою метою діяльності російських і білоруських хакерів у Польщі було вивідування інформації та подальший шантаж, організація ведення кібервійни [16].

Таким чином, у Польщі існують законодавчі підвалини для створення нової складової Збройних Сил країни – Сил оборони кіберпростору (Wojska Obrony

Cyberprzestrzeni). Передбачено, що сили (війська) оборони кіберпростору Польщі є регулярною армією, яка має оборонні можливості, функції виявлення, а також здійснення наступальних дій, якщо існує така потреба. Перед силами кібероборони як новим родом спеціальних військ ставляться досить конкретні завдання – ведення оборонних, наступальних та розвідувальних дій у кіберпросторі. За задумом, остаточне формування Сили оборони кіберпростору Польщі планується завершити до 2026 року. Тобто Польща демонструє та впроваджує виважену й послідовну державну політику боротьби із сучасними кіберзагрозами у військовій сфері. Важливим аспектом кожного кіберпідрозділу Польщі є його здатність проводити весь спектр операцій, включаючи наступальні кібероперації та використання кіберзброї.

Чехія. У цій країні кібервійська були офіційно утворені 1 липня 2019 року, а перший підрозділ був укомплектований та переданий у розпорядження командуванню 1 січня 2020 року. Тобто фактично з 2020 року кібервійська були інтегровані в організаційну структуру новоствореного командування кібервійськ та інформаційних операцій із загальною чисельністю 1 тис. осіб. Кібервійська Чехії було утворено на базі 103 центру цивільно-військового співробітництва. (Civil-military Cooperation – CIMIC). Загалом концепція CIMIC має 3 основних функції, які предметно відображені в доктрині НАТО "AJP-9" та висвітлені у всіх національних доктринах країн-членів НАТО: 1) цивільно-військовий зв'язок (діяльність, яка будується навколо координації та планування робота із громадськими організаціями); 2) підтримка цивільного середовища; 3) підтримка сили. Така діяльність здійснюється з метою уникнення та попередження перешкоджанню воєнним операціям з боку цивільних суб'єктів. Основні функції доктрини CIMIC НАТО формують концептуальну основу, згідно з якою кожна країна НАТО надає власну інтерпретацію та тлумачення відповідно до своїх стратегічних інтересів та наративів. Залежно від типу операцій і засобів досягнення оперативних цілей відрізняється і сфера застосування CIMIC. Як демонструє досвід ведення збройних конфліктів, військові підрозділи переважно діють серед місцевого населення, яке має власні цілі та повноваження в районах операцій. Спільна діяльність військової та цивільної сторін веде до створення і підтримки ефективних зв'язків між ними й успішного досягнення результатів. Сьогодні CIMIC – це невід'ємна частина сучасних багатовимірних операцій, яка вивчає усіх суб'єктів, які взаємодіють у конфлікті та сприяє взаємній допомозі цивільних сил військовим, і навпаки. Основна мета цієї взаємодії – досягнення певного бажаного кінцевого стану, який має бути однаково корисним для місцевого населення, мирного населення та збройних сил. Тому підвищення ефективності CIMIC відіграє головну роль у досягненні успіху операції та певного бажаного кінцевого стану. Сучасним підходом у цивільно-військовій співпраці стало використання нових напрямків у діяльності CIMIC під час діяльності сил НАТО з підтримки миру.

У Чехії створені та діють кібервійська (Skupina kybernetických sil a informačních operací (SkKySIO), які мають власне командування (VEKYSIO). Штаб кібервійськ розташований у місті Брно [17]. Інформаційні та кібернетичні сили є типом сил, що підпадають під командування армії Чеської Республіки. В структурі командування та управління армією Чеської Республіки вони належать до тактичного рівня разом із сухопутними військами, військово-повітряними силами, силами спеціального призначення, територіальними військами та оперативними силами.

З 1 липня 2024 року кібервійська структурно складаються з Центру інформаційних операцій, до якого входять 91-ша група інформаційної боротьби та 92-а група кібервійни. Так, зокрема 91-ша група є виконавчою ланкою сил інформаційних операцій

вищого командування. Група зосереджена на проведенні інформаційно-психологічних операцій, цивільно-військовому співробітництві, моніторингу та аналізі інформаційного середовища, має компетенцію створювати складні аудіовізуальні продукти задля підтримки управління оперативною діяльністю інформаційних та кіберпідрозділів. У свою чергу, 92-га кібергрупа була створена як важлива складова командування інформаційно-кібернетичних військ, яка орієнтується на проведення оборонних і наступальних операцій у кіберпросторі. Також до сфери її компетенції належить забезпечення моніторингу та захист інформаційно-комунікаційних мереж чеської армії, включаючи кіберзахист операційних систем, сприяння забезпеченню кібербезпеки військового інформаційного середовища [18].

Командування інформаційних і кібернетичних сил є стратегічним інструментом, який сприяє безпеці та обороні Чеської Республіки. Командування інформаційно-кібернетичних сил діє самостійно, спільно або у взаємодії з іншими типами сил у багатопрофільних операціях. Таке командування співпрацює з іншими елементами кібербезпеки та оборони Чеської Республіки та надає підтримку Верховному командуванню чеської армії у сфері стратегічних комунікацій.

Кібервійська Чехії забезпечують постійну підтримку стратегічного рівня у сфері комунікації, виконуючи цю діяльність переважно на користь Генерального штабу армії Чеської Республіки. Структурно кібервійська Чехії об'єдналися під егідою Центру інформаційних операцій, який поєднує можливості Центру CIMIC (цивільно-військового співробітництва) та підрозділу PSYOPS (психологічні операції). Кібервійська покликані підтримувати інші підрозділи чеської армії, країн-членів НАТО та ЄС та навіть проводити диверсійно-психологічні операції. Також кібервійська Чехії (SkKySIO) залучаються до виконання спеціальних завдань в закордонних операціях і місіях у таких країнах, як Малі (Тренінгова місія ЄС) та Іраку (виконання операції "Inherent Resolve").

Основними завданнями, які успішно виконує Центр інформаційних операцій, є: забезпечення кібероборони, проведення інформаційно-кібернетичних операцій, спрямованих на вплив на розумові здібності та ментальні можливості супротивника; організація психологічного впливу та тиску на обрані цільові групи; проведення спектрального аналізу інформаційного та кіберсередовища; створення оперативного запису (фото, відео) дій окремих підрозділів збройних сил Чехії; співпраця з органами самоврядування, міжнародними організаціями та неурядовими організаціями за місцем діяльності; моніторинг інформаційного та кіберсередовища на постійній основі; підтримка військової інформаційної діяльності, пов'язаної із впливом та ефектами в інформаційному середовищі на тактичному рівні; розвиток спроможностей задля проведення інформаційних операцій у кіберпросторі як на користь власних елементів (SkKySIO), так і для підтримки операцій НАТО у кіберпросторі; формування високого рівня готовності до реагування на кіберінциденти; розвиток експертної співпраці з відповідними партнерами (комерційними структурами, науковими установами тощо).

У свою чергу, Центр CIMIC є підрозділом, призначеним для виконання завдань цивільно-військового співробітництва на оперативно-тактичному рівні і є одночасно елементом бойового забезпечення. Діяльність CIMIC зосереджена на виконанні основних загально-військових тактичних заходів – плануванні цивільно-військового співробітництва, створенні ситуаційних звітів, проведенні аналізу та оцінки кібербезпекового середовища. Основні завдання CIMIC включають: опанування основ тактичної діяльності у рамках цивільно-військового співробітництва; створення бази даних громадських організацій для подальшого розвитку цивільно-військової взаємодії;

проведення аналізів та оцінок військового та цивільного безпекового середовища; координація відбору та набору активних резервів CIMIC; планування та здійснення загальновійськової та професійної підготовки кадрів кібервійськ.

До складу кібервійськ входить Група підтримки – це підрозділ, який займається забезпеченням мультимедійної безпеки. Фахівці цієї групи призначені для виконання завдань у сфері поліграфічної роботи, аудіо- та відеопродукції та розгортання у складі бойової знімальної групи (групи бойового відеодокументування). Група забезпечує мультимедійну підтримку саме для проведення психологічних та інформаційних операцій, оперативно-стратегічної комунікації та публічної популяризації армії. Також у складі кібервійськ функціонує спеціальний підрозділ – Група підтримки стратегічних комунікацій (StratCom), яка призначена для розвитку стратегічних комунікацій чеської армії у сферах планування, аналізу та консультацій. Основні її завдання включають: реалізацію стратегічного комунікаційного плану Міністерства оборони; відстежування сучасних тенденцій використання соціальних мереж військовослужбовцями; створення аудіовізуальних продуктів для потреб Міністерства оборони; управління закритими соціальними мережами, участь у створенні систем раннього попередження інформаційних та кібернетичних загроз і ризиків тощо.

Таким чином, кібервійська в Чехії перебувають у стадіях свого органічного та інституційного становлення й розвитку, спеціалізуються переважно на проведенні інформаційних операцій у кіберпросторі, забезпечують кібероборону та кіберзахист військових та суміжних систем. Інформаційно-кібернетичні сили Чехії здатні проводити інформаційно-психологічні, кібернетичні операції, здійснюючи одночасно цивільно-військове співробітництво в контексті посилення заходів у сфері гарантування кібербезпеки та залучаючи для цього представників приватного сектору.

10 липня 2024 року Національне управління з кібербезпеки та інформаційної безпеки (NÚKIB) оприлюднило схвалений урядом звіт про стан кібербезпеки за 2023 рік, відповідно до якого кількість зафіксованих кібератак зросла до 262 за рік [19]. Протягом 2023 року поліція Чехії зареєструвала понад 19 тисяч кримінальних правопорушень у сфері кіберзлочинності, що на 6 % більше, ніж у 2022 році. Найбільшою загрозою кібербезпеці Чехії є діяльність кіберзлочинних угруповань, спонсорованих рф. Це пов'язано із повторюваними хвилями DDoS-атак з боку російських хактивістських груп, що пов`язано із наданням Чехією гуманітарної та військової допомоги Україні. Також Чехія визнана однією з держав ЄС, яка найбільше постраждала від країни-агресора. 17 липня 2024 року уряд Чеської Республіки обговорив і схвалив проект тексту нового закону про кібербезпеку, метою якого є посилення кібербезпеки Чеської Республіки в контексті зростаючої кількості кіберзагроз та викликів [20].

Висновки.

Підсумовуючи викладене, слід зазначити, що виходячи із сучасних світових тенденцій, країни-члени НАТО динамічно працюють над інституційними засадами створення власних кібервійськ. При цьому Польща та Чехія не є виключенням. Кожна країна обирає власну модель розвитку кібервійськ та встановлює національні особливості їхньої функціональної діяльності і сфер компетенції. Як у Польщі, так і в Чехії кібервійська проходять експериментальний етап свого становлення. Зростаюча цифровізація більшості країн світу, включаючи актуалізацію значення штучного інтелекту, вимагають адаптації до змін безпекового середовища, що включає мілітаризацію кіберпростору та підготовку кібервійськ.

Таким чином, на підставі проведеного дослідження можна констатувати, що кожна з проаналізованих країн (Польща, Чехія) переймається проблематикою розбудови власних

кібервійськ як важливої компоненти у складі збройних сил. Основними питаннями, які потребують врегулювання під час інституційного створення кібервійськ виступають: правові основи, штатна чисельність кіберпідрозділів, склад та структура кіберкомандування, компетенція та повноваження кібервійськ, стратегічні та функціональні завдання, обсяги щорічного фінансування, умови поповнення кадрового резерву тощо. Сучасний тренд кібервійськ як у Польщі так і Чехії – використання методів та практик інформаційно-психологічних операцій (впливу) на ворога (супротивника) з метою його психічної дестабілізації та тривалого розладу психічного здоров'я (доктрини когнітивного ефекту), забезпечення кібероборони, розвиток військових стратегічних комунікацій.

Проаналізований зарубіжний досвід переконливо доводить, що національні кіберсили є ключовою компонентою в інтегрованому підході щодо посилення стану забезпечення національної безпеки. Таким чином, вивчення, опанування та впровадження кращих практик щодо інституційного створення кібервійськ таких країн-членів НАТО, як Польща та Чехія, надасть змогу прискорити запуск та подальшу розбудову в Україні власних кібервійськ (кіберсил) з метою кіберстримування збройної агресії та надання відсічі агресору у кібердомені. Саме тому кібероборона України, її забезпечення, захист суверенітету та територіальної цілісності нашої держави в кіберпросторі є пріоритетними завданнями державної безпекової політики, а створення спеціальних підрозділів кібервійськ в Україні є важливим та рішучим кроком, який спрямований на запровадження дієвих та ефективних механізмів стримування та відсічі російській агресії у кібердомені, особливо в умовах триваючої кібервійни. Створення кіберсил як окремого роду сил дозволить значно посилити спроможності українського війська, забезпечить ефективне планування та реалізацію повного спектра завдань у кіберпросторі. Тому доцільним є прискорення законодавчого забезпечення інституційного створення кібервійськ в Україні, що передбачатиме розробку відповідної Концепції та підготовку спеціального законопроекту "Про Кіберсили Збройних Сил України" як дорожньої карти стратегічного планування та розвитку кібервійськ в нашій країні.

За таких умов для України оптимальним є створення власної організаційної моделі кібервійськ (кіберсил) з урахуванням внутрішньої специфіки та необхідності консолідації зусиль щодо формування єдиного кіберкомандування. Також набувають актуальності питання посиленого захисту цивільних осіб, задіяних у проведенні кібероперацій та забезпеченні кібероборони, надання цій категорії правового статусу комбатантів на національному та міжнародному рівнях.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави": Указ Президента України від 26.08.21 р. № 446/2021. URL: https://www.president.gov.ua/documents/4462021-40009

2. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України": Указ Президента України від 01.02.22 р. № 37/2022. URL: https://www.president.gov.ua/documents/372022-41289

3. Про затвердження плану заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 19.12.23 р. № 1163. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text

4. Горун О.Ю. Зарубіжний досвід правового забезпечення та особливостей створення кібервійськ на прикладі деяких держав НАТО. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2023 № 64. С. 33-37.

5. Федієнко О.П. Сучасні тенденції нормативного забезпечення інституційного формування кібервійськ (кіберсил): досвід деяких країн НАТО. *Інформація і право.* № 1(48)/2024. С. 150-161.

6. Ткачук Н.А. Досвід США зі створення та розбудови Кіберкомандування: уроки для України. *Інформація і право.* № 1(48)/2024. С. 139-149.

7. Чевардін В.Є., Мазулевський О.Є. Аналіз структур кіберкомандувань розвинутих країн: збірник наукових праць ВІТІ. 2020. № 2. С. 121-128.

8. Фіца В.М. Інституційне забезпечення створення кібервійськ в Україні. *Інформація і право.* № 3(38)/2021. С.109-114.

9. Ustawa "O krajowym systemie cyberbezpieczeństwa", 05.07.2018. URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/krajowy-system-cyberbezpieczenstwa-18746756

10. Концепція організації та функціонування Сил оборони кіберпростору (CYBER.MIL.PL). – (Міністерство оборони Польщі). URL: https://www.cyber.mil.pl

11. Ustawa "O obronie Ojczyzny" 11.03.2022. URL:https://eli.gov.pl/eli/ DU/2022/655/ogl

12. Polish cyber claws. Building of the cyber army of the rising military power in Europe. URL: https://pulaski.pl/polish-cyberclaws-buildingof-the-cyberarmy-of-the-rising-military-power-in-europe-2

13. Уряди України та Польщі підписали меморандум про співпрацю у сфері кіберзахисту. URL: https://www.kmu.gov.ua/news/uriady-ukrainy-ta-polshchi-pidpysaly-memorandum-pro-spivpratsiu-u-sferi-kiberzakhystu

14. Cyber Mil 2.0. URL: https://www.cyber.mil.pl/kim-jestesmy

15. Польща посіла перше місце у рейтингу кібербезпеки. URL: https://www.pol skieradio.pl/398/7856/artykul/3346094

16. У Польщі викрили мережу російських і білоруських диверсантів, які планували "кібервійну". URL: https://www.eurointegration.com.ua/news/2024/09/9/7193811

17. Skkysio: Úvodní stránka. URL: https://skkysio.army.cz

18. Velitelství informačních a kybernetických sil. URL: https://www.doarmady.cz/o-ar made/poznejte-armadu/utvary-a-posadky/velitelstvi-informacnich-a-kybernetickych-sil

19. Vláda schválila Zprávu o stavu kybernetické bezpečnosti ČR za rok 2023. URL: https://nukib.gov.cz/cs/infoservis/aktuality/2139-vlada-schvalila-zpravu-o-stavu-kyberneticke-bezp ecnosti-cr-za-rok-2023

20. Vláda schválila návrh nového zákona o kybernetické bezpečnosti. URL: https:// nukib.gov.cz/cs/infoservis/aktuality/2141-vlada-schvalila-navrh-noveho-zakona-o-kyberneticke-bezpecnosti

* * *