УДК 342.951
DOI https://doi.org/10.32841/2307-1745.2023.64.7

Горун О. Ю.,
головний науковий співробітник
Українського науково-дослідного інституту спеціальної техніки
та судових експертиз Служби безпеки України

ЗАРУБІЖНИЙ ДОСВІД ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ТА ОСОБЛИВОСТЕЙ СТВОРЕННЯ КІБЕРВІЙСЬК НА ПРИКЛАДІ ДЕЯКИХ ДЕРЖАВ НАТО

Анотація. У статі досліджуються передумови утворення кібервійськ на теренах НАТО. Визначено засади безпекової політики НАТО у кіберпросторі. Актуалізуються питання забезпечення кібероборони, захисту критичної інформаційної інфраструктури від кібератак, проведення превентивних наступальних операцій у кіберпросторі у рамках нормативних документів НАТО. Розглянуто концепцію кібероборони (Cyber Defense) НАТО та узагальнено здобутки Альянсу у цій площині. Визначено роль та місце кібербезпеки у системі національної безпеки під егідою НАТО. Особлива увага приділяється французькій моделі створення та функціонування кібервійськ. Визначено структуру та склад, нормативно-правове регулювання практичної діяльності кіберкомандування Франції. Розкрито напрями проведення оборонних дій у кібердомені. Деталізовано порядок та особливості здійснення наступальних операцій. Окреслено питання подальшої розбудови структурних підрозділів кібервійськ та фінансування діяльності кіберкомандування. Визначено основні завдання у сфері інформаційно – психологічної боротьби за участю кіберпідрозділів Франції. Деталізовано пріоритети у сфері розвитку системи кібероборони французських збройних сил до 2025 року. Підсумовано, що у Франції створено компактну вузькоспеціалізовану структуру кібервійськ вищого стратегічного рівня. Визначено переваги кібервійськ Франції, порівняно з США та Великобританією. Розглянуто сучасний польський досвід інституційного створення кібервійськ. Акцентовано, що процес створення польських сил оборони кіберпростору ґрунтується на досвіді створення польських спеціальних підрозділів. Унормовано та визначено штатну чисельність підрозділів кібервійськ Польщі. Визначено поняття, структуру та спеціалізовану компоненту військ оборони кіберпростору Польщі. Окреслено законодавчі основи, стратегічні завдання та перспективи діяльності підрозділів кібервійськ Польщі. З'ясовано, що сили оборони кіберпростору Польщі відповідають за безпеку кіберпростору, включаючи оборону, розвідку та наступ, а також протидію психологічним та інформаційним операціям. Висвітлено питання партнерської взаємодії сили оборони кіберпростору Польщі та НАТО. На підставі проведеного аналізу підсумовано, що кібервійська є новим компонентом у складі Збройних сил провідних країнах НАТО, які здійснюють як оборонні, так і наступальні операції у кіберпросторі, реалізують заходи інформаційно – психологічної боротьби. Узагальнено, що як французька так і польська моделі інституційного створення кібервійськ можуть бути використані за основу під час утворення кібервійськ в Україні, що є одним із першочергових завдань сектору безпеки та оборони в умовах тотальної кібервійни з рф.

Ключові слова: кібероборона, кібервійська, кібербезпека, кібердомен, кіберзахист, безпекове середовище, національна безпека, НАТО.

Постановка проблеми. Організація Північноатлантичного договору (НАТО) ще у 2016 році визнала кіберпростір одним із можливих театрів воєнних дій, нарівні з повітрям, сушею та морем. Як наслідок, у НАТО на даний час триває процес створення загальних для всього Альянсу кібервійськ (кібersил). До їх завдань належить не лише забезпечення кібероборони, захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури супротивника шляхом руйнування інформаційних та комунікаційних систем, які управляють такими об'єктами, реалізація доктрини когнітивного ефекту, тобто використання методів, які потенційно можуть посіяти недовіру, знизити моральний дух і послабити здатність противника ефективно планувати та проводити свою діяльність у кіберпросторі. Таким чином, концепція кібероборони (Cyber Defense) є частиною головного завдання НАТО щодо стримування і оборони. У лютому 2017 року міністри оборони Альянсу схвалили оновлений План дій щодо кіберзахисту, а також дорожню карту впровадження кіберпростору як сфери операцій. На саміті НАТО в Брюсселі 2018 року лідери Альянсу погодилися створити новий Оперативний центр у кіберпросторі як частину командної структури НАТО. У лютому 2019 року міністри оборони країн НАТО схвалили керівні рекомендації, які містить низку інструментів для подальшого зміцнення здатності Альянсу реагувати на зловмисні дії у кіберпросторі.

На виконання стратегічних наративів НАТО у 2020 році в Туреччині з'явилися власні кібервійська (Türk Siber Ordusu) у кількості орієнтовно 13 тис. осіб. До складу кібервійськ Туреччини увійшли військові та цивільні особи, які є фахівцями у сфері кібербезпеки, а переважну більшість складають хакери, які перейшли на роботу до державного сектора [1, с. 160]. На саміті НАТО 2021 року схвалили Всеосяжну політику кіберзахисту НАТО, на виконання якої Альянс має стримувати, захищатися та протидіяти повному спектру кіберзагроз. Члени Альянсу визнали, що вплив значної зловмисної сукупної кібератівності за певних обставин може розглядатися як збройний напад. У вересні 2021 року Північноатлантична рада призначила першого головного інформаційного директора НАТО (CIO) для сприяння інтеграції, узгодженню та згуртованості систем інформаційно-комунікаційних технологій (ІКТ) на теренах Альянсу.

На саміті НАТО у Вільнюсі 2023 року члени Альянсу схвалили нову концепцію посилення внеску кіберзахисту в загальну систему стримування та оборони НАТО. 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, а також спільна безпека. 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.

Таким чином, кібербезпека в країнах НАТО визнана важливою складовою національної безпеки, забезпечення якої здійснюється на підставі єдиної скоординованої політики у цій сфері, що ґрунтується на засадах поваги до норм і принципів міжнародного права, забезпечення національних пріоритетних інтересів у кіберпросторі, побудови ефективної протидії у кібердомені. Загальною усталеною практикою цих країн стає чітке доктринальне визначення концептуальних засад державної політики у сфері забезпечення безпеки у кіберпросторі у відповідних документах стратегічного планування. При цьому важливе місце відводиться розбудові саме кібероборони та її забезпеченню.

Не можна не погодитися з позицією С. Демедюка та О. Користіна, які вказують, що на теренах НАТО сформувалися системні підходи щодо посилення стійкості на основі запобігання та протидії кіберзагрозам. Високий рівень кіберстійкості забезпечується участю усіх суб`єктів системи кібербезпеки, формуванням надійних та ефективних інституцій, структур, агенцій та місій, що сприяють кібербезпеці та реагують на кібератаки [2, с. 78].

Таким чином, враховуючи необхідність та доцільність мілітаризації кіберпростору на виконання програмних документів НАТО, останнім часом під егідою Альянсу в державах-членах активно створюються та функціонують спеціальні підрозділи – кібервійська, які використовуються як для військових, так і для розвідувальних цілей, проведення оборонних та наступальних операцій у кіберпросторі. За таких умов можна констатувати про загальносвітову тенденцію нарощування спроможностей щодо розбудови кібервійськ у тій чи іншій державі Альянсу. За таких умов детальний розгляд інституційного утворення та організаційно-правових засад функціонування кібервійськ у таких країнах НАТО як Франція та Польща заслуговують на увагу.

Результати аналізу останніх досліджень і публікацій. Проблематику створення кібервійськ вивчали у своїх працях: І. Діордиця [3], Л. Котихова [4], В. Чевардін та О. Мазулевський [5], В. Фіца [6]. Організаційно-економічні заходи створення кібервійськ досліджували: Н. Аванесова, Н. Сергієнко, Ю. Любушин [7]. У зарубіжних джерелах інституційне забезпечення кібервійськ перебували у фокусі уваги: М. Смитса [8], Г. Дімітрова [9] та інших. Проте жоден із цитованих авторів предметно не розглядав досвід та особливості нормативного забезпечення й інституційного формування кібервійськ (кіберсил) у таких країнах НАТО як Франція і Польща, що переконливо засвідчує тематичну актуальність цього наукового дослідження.

Метою статті є дослідження нормативно-правових засад інституційного створення кібервійськ (кіберсил) у деяких провідних країнах НАТО (Франція, Польща) та на його підставі узагальнення сучасних тенденцій політики у сфері кібероборони Альянсу та окреслення пропозицій з метою прискорення інституційного утворення кібервійськ (кіберсил) в Україні, особливо в умовах кібервійни.

Виклад основного матеріалу. Перш за все доцільно розглянути особливості французької моделі створення та функціонування кібервійськ. Відповідно до положень «Білої книги з питань національної безпеки і оборони» цієї країни інституційне формування системи кіберзахисту у складі національних збройних сил є одним з пріоритетних направлень військового будівництва, а кіберпростір розглядається як сфера глобального протиборства. З урахуванням викладених у положеннях Воєнній доктрині Франції концептуальних основ, у травні 2017 року було створено кіберкомандування Збройних Сил Франції. Відповідний Декрет «Про зміни організаційно штатної структури Збройних Сил» [10] підписав міністр оборони країни. Загальне керівництво покладається на військову посадову особу у ранзі дивізійного генерала (з вересня 2019 року – Д. Тісейр).

Загалом до складу кіберкомандування Франції входять:

– Кіберштаб (м. Париж), при якому функціонує Центр операцій (Centre des operations CYBER);

– Аналітичний Центр кіберзахисту (м. Париж та м. Ренн, Centre d'analyse en lutte informatique defensive);

– Центр контролю та безпеки інформаційних систем (м. Мезон-Лаффіт, Centre d'audit et de sécurité des systèmes d'information);

– Центр оперативної підготовки та резерву кіберзахисту (м. Гер);

– Центр міжвидової сертифікації (м. Париж, Centre des homologations principales interarmées);

– спеціальні підрозділи кіберзахисту ВМС та ПКС.

Загальна чисельність регулярних формувань складає 4,2 тис. військовослужбовців, з них резервістів – 400 осіб. Кіберкомандування Франції вирішує такі основні функціональні завдання: – адміністративне та оперативне керівництво кіберсилами; – поточне забезпечення захисту інформаційно-телекомунікаційних систем військового відомства, планування та керівництво кіберопераціями; – формування підходів до ведення бойових дій у кіберпросторі у взаємодії з іншими профільними структурами міністерств та відомств країни. Практична діяльність кіберкомандування регламентується нормативно-правовою базою, що включає Наставлення до оборонних (Lutte informatique defensive, затверджене у 2018 році) та наступальних (Lutte informatique offensive – 2019 року) дій у кіберпросторі, а також Доктрину «Інформаційно-психологічної боротьби» (Lutte informatique d'influence – 2021 року) [11].

У рамках оборонних дій у кібердомені вирішуються завдання щодо попередження, виявлення та реагування на реальні та потенційні кіберзагрози, а також щодо захисту інформаційно-комунікаційного середовища (ІКС) військового відомства від несанкціонованого доступу до систем військового управління або виведення їх з ладу, запобігання нештатним ситуаціям. Наступальні операції здійснюються кіберсилами у взаємодії з традиційними військовими засобами для кіберне-

тичного впливу на інформаційно-комунікаційні системи ворога з метою максимального досягнення поставлених цілей (порушення та виведення з ладу працездатності операційних систем, отримання доступу до конфіденційної інформації тощо).

Основними завданнями у сфері інформаційно – психологічної боротьби за участю кіберпідрозділів Франції є: – інформаційна підтримка збройних сил та військових формувань, у тому числі під час виконання гуманітарних або миротворчих операцій за кордоном; – тотальна дискредитація дій супротивника, введення його в оману щодо характеру діяльності власних кіберсил; – перманентний моніторинг кіберпростору та інформаційного простору тощо. Операції подібного роду проводяться переважно за кордоном і виключно в рамках обмежених військових кампаній, затверджених урядом країни.

Аналітичний центр кіберзахисту (АЦКЗ) є черговим компонентом системи забезпечення безпеки інформаційних систем Міністерства оборони Франції. До його функціональних повноважень відносяться постійний моніторинг цифрового простору, виявлення та ліквідація кіберзагроз, відбиття кібератак, оперативне поновлення працездатності виведених з ладу вузлів та агрегатів ІКТ. Для вирішення практичних завдань та забезпечення належного рівня безпеки ця структура проводить плідну співпрацю та взаємодію з Групою реагування на кіберінциденти (Groupes d'intervention en cyberdefense) (CERT-FR). У випадку відсутності можливості усунути наслідки кіберінциденту віддалено, спеціальна група реагування у сфері кіберзахисту направляється до місця з метою фізичного усунення проблеми.

Центр контролю та безпеки інформаційних систем відповідно до функціональних завдань призначений для забезпечення безпеки технічної основи ІС та недопущення витоку конфіденційної та службової інформації навіть через ймовірні випадки побічні випромінювання радіоелектронної апаратури. Функціональні підрозділи цієї структури фізично розташовані у містах: Брест, Орлеан, Тулон, Ренн.

Центр оперативної підготовки та резерву кіберзахисту забезпечує взаємодію військових та цивільних спеціалістів, сприяючи обміну досвідом та розвитку їхніх професійних навичок. Ця структура є відповідальною за набір, підготовку та розподіл спеціалістів з кіберзахисту в рамках потреб військового відомства, бере участь в організації національних та міжнародних профільних навчань, у тому числі, щорічного стратегічного тренінгу з кібербезпеки «DevNet» Збройних Сил Франції з метою відпрацювання процедур забезпечення стабільного та безперебійного функціонування інформаційної інфраструктури в умовах масованих кібератак. «DevNet» – це інтегрована площадка, яка у навчальних цілях використовується програмістами та яка допомагає розробникам та фахівцям у IT – галузі розвивати інтеграцію з продуктами, інтерфейсами, надає змогу обмінюватися досвідом та навичками. Також ця площадка надає можливість використовувати віртуальні інструменти та пісочниці на кшталт (sandboxes) для написання та тестування своїх програм та додатків. У підпорядкуванні цього Центру перебуває оперативний резерв кіберзахисту, представники якого, за необхідності, можуть комплектувати профільні підрозділи Збройних Сил та брати участь у проведенні операцій у кібердомені.

Резервний компонент включає два сегменти. Перший – «резерв реагування» (Réserve d'intervention, головним чином це співробітники профільних підприємств) служить для здійснення моніторингу кіберпростору та виявлення кіберзагроз на ранній стадії. Другий – «резерв поновлення» (Réserve de reconstruction, переважно студенти вищих навчальних закладів старших курсів) виконує нескладні завдання з метою ліквідації наслідків нескладних кібератак.

Центр міжвидової сертифікації є відповідальним за питання контролю виконання програм у сфері інформаційних систем та мереж зв`язку, а також сертифікації технічних засобів, що використовуються у військовому відомстві. В інтересах організації навчання спеціалістів з кіберзахисту у Збройних Силах Франції була створена спеціалізована комісія з питань підготовки у сфері кібербезпеки (CAF Cyber – Commission d'adaptation à la formation Cybersécurité), яка відповідальна за розробки навчальних програм та визначення нормативів для слухачів за відповідними обліковими спеціальностями. Основним навчальним закладом Збройних Сил Франції є військова школа зв`язку (м. Лаваль), яка має у своїй структурі два центри підготовки. У цьому навчальному закладі готують військовослужбовців та цивільний персонал для підрозділів кіберзахисту. Школа перебуває в оперативному підпорядкуванні командування зв'язку та інформаційних систем Збройних Сил Франції.

Пріоритетними завданнями у сфері розвитку системи кібероборони французьких Збройних Сил до 2025 року є нарощування потенціалу наступальних операцій в кіберпросторі, системне удосконалення їх проведення, системна підготовка професійних кадрів, здатність впроваджувати інноваційні технологічні рішення та програми штучного інтелекту у питаннях забезпечення кібербезпеки, розширення кооперації та співпраці з партнерами НАТО та ЄС. При цьому, фінансування діяльності кіберкомандування Франції планується збільшити у 2024 році до показника у розмірі 1,6 млрд. євро на рік.

Таким чином, в структурі Збройних Сил Франції функціонує командування кіберзахисту (COMCYBER), яке безпосередньо підпорядковане начальнику штабу оборони країни (CEMA) та є оперативним командуванням, яке об'єднує всі сили кіберзахисту міністерства оборони під спільним керівництвом. Його місія – захист інформаційних систем, а також розробка, планування та проведення військових операцій у кіберпросторі. Для виконання своїх місій «COMCYBER» має дві структури: Штаб кіберзахисту (EM-CYBER) та армійську групу кіберзахисту (GCA), яка розташована в м. Ренні та у м. Париж. На відміну від широкомасштабного підходу, який практикується в США та у Великобританії, саме комбінування кібероперацій з можливостями радіоелектронної розвідки, радіоелектронною протидією, у Франції було створено компактну вузькоспеціалізовану структуру кібервійськ вищого стратегічного рівня. Переваги кібервійськ Франції полягають у зменшеному розмірі штату таких кіберсил та відповідно у зменшеному розмірі фінансових витрат на його утримання. На цьому фоні, на переконання військових експертів, недоліком виступає мінімізація сил, що обмежує кількість завдань, що виконуються.

Заслуговує на увагу сучасний польський досвід інституційного створення кібервійськ. У 2016 році, під час саміту НАТО у Варшаві було констатовано, що захист кіберпростору є одним із основних завдань колективної оборони НАТО, визнавши кіберпростір зоною військових операцій. Наприкінці 2017 року Польща, як активний член НАТО

анонсувала виділення 2 мільярдів злотих (близько 465 млн євро) на створення та інституційного забезпечення власного кібервійська. 5 липня 2018 року у Польщі ухвалено закон «Про національну систему кібербезпеки» [12], за наслідками реалізації якого в державі створено відповідні структури, основними з яких стали Національний центр кібербезпеки, Національна група реагування на комп'ютерні інциденти, Національний центр безпеки кіберпростору міністерства оборони Республіки Польщі, галузеві структури кіберзахисту, тощо. На виконання рекомендацій НАТО, у 2019 році затверджено Концепцію організації та функціонування Сил оборони кіберпростору (WOC) [13], положення якої спрямовані на підвищення безпеки держави та громадян у кіберпросторі та засновані на чотирьох стратегічних рівнях. Перший – це консолідація та побудова власне структур кібербезпеки, другий – освіта, навчання та тренінги спеціалістів, третій – співпраця та побудова міжнародної позиції із країнами партнерами, четвертий – підвищення рівня безпеки відомчих і військових мереж та систем Польщі. Одночасно було створено групу формування командування сил оборони кіберпростору (COK).

18 березня 2022 року Президент Польщі підписав закон «Про оборону» [14], відповідно норм до якого війська оборони кіберпростору – це спеціалізована компонента збройних сил, призначена для виконання повного спектру завдань в кіберпросторі, зокрема не лише в реактивних діях, але й проактивного захисту (постійного виявлення інструментів, методів, мотивації і процедур потенційних противників) та активної оборони (розпізнавання потенційних небезпек, загроз у кіберпросторі, безпосередніх дій). Стаття 23 вказаного законодавчого акту регламентує повноваження та функціональні завдання польського кібервійська.

Таким чином, у Польщі законодавчо визначені підстави створення нового компоненту Збройних сил країни – Сил оборони кіберпростору (Wojska Obrony Cyberprzestrzeni). Передбачено, що сили (війська) оборони кіберпростору Польщі є регулярною армією, яка має згідно із компетенцією оборонні можливості, функції виявлення, а також здійснення наступальних дій, якщо буде така потреба. Перед силами кібероборони як новим родом спеціальних військ ставляться досить конкретні завдання – ведення оборонних, наступальних та розвідувальних дій у кіберпросторі. Сили оборони кіберпростору Польщі, остаточне формування яких планується завершити до 2026 року, стануть спеціальним компонентом Збройних сил Польщі. Процес створення польських Сил оборони кіберпростору ґрунтується на досвіді створення польських підрозділів спецназу, які на початку також були спеціальним компонентом Збройних сил Польщі, проте згодом були трансформовані в окремий військовий рід військ. Сили оборони польського кіберпростору в мирний час підпорядковуватимуться безпосередньо Міністерству оборони, а під час мобілізації та війни підпорядковуватимуться головнокомандувачу, обраному президентом країни. Передбачено постійний штат кібервійськ Польщі у кількості 1 тис. осіб. Необхідні фахові оперативні спроможності кіберсил під керівництвом міністра оборони, повинні бути сформовані до кінця 2024 року, та у перспективі будуть передані в підпорядкування начальнику генерального штабу ЗС Республіки Польща. 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;

– Координація з іншими державними установами, відповідальними за оборону;

– Проведення досліджень та підготовка інноваційних рішень для виявлення інцидентів у кіберпросторі;

– Проектування, створення, впровадження та використання національних криптологічних технологій і рішень для забезпечення інформаційної безпеки;

– Розробка нових рішень у сфері сучасних технологій та криптографії;

– Проведення освітніх та 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 [15]. Крім того, налагоджено співпрацю з Центром передового досвіду НАТО з питань кіберзахисту, розташованим в Естонії. Таким чином, Польща демонструє та впроваджує виважену й послідовну державну політику боротьби із сучасними кіберзагрозами у військовій сфері, свідченням чого є сформовані законодавчі та організаційні засади функціонування військ (сил) оборони кіберпростору.

Узагальнюючи викладене вище, заслуговує на увагу позиція Є. Живила про те, що створення колективних систем протидії кіберзагрозам є перспективним напрямком подальших досліджень з метою створення потужних систем кібервпливу [16, с.42].

Висновки. Світова тенденція сучасності – кожна провідна держава світу динамічно розвиває власні кібервійська. У більшості країн НАТО діє власна модель нормативного забезпечення та інституційного створення кібервійськ (кіберсил). Як правило, створення кібервійськ задекларовано у спеціальних нормативних актах переважно військового спрямування (стратегіях, концепціях, доктринах) провідних держав світу, на підставі яких розроблюються локальні документи, присвячені актуальним питанням функціональності та компетенції кібервійськ, їхнього фінансування та підготовки відповідних кадрів. Основними питаннями, які потребують нормативного врегулювання під час інституційного створення кібервійськ у досліджуваних країнах НАТО стали: правові засади, штатна чисельність створеного кіберпідрозділу, склад та структура кіберкомандування, функціональні завдання та повноваження кібервійськ, стратегічні та функціональні завдання та повноваження кібервійськ, обсяги щорічного фінансування. Остання тенденція сучасних кібервійськ (кіберсил) – прове-

дення наступальних операцій у кібердомені, використання методів та практик інформаційно-психологічних операцій (впливу) на ворога (супротивника) з метою його психічної дестабілізації та тривалого розладу психічного здоров'я. Проаналізований зарубіжний досвід деяких країн НАТО (Франція, Польща) переконливо доводить, що національні кіберсили є ключовим компонентом в інтегрованому підході щодо посилення стану забезпечення національної безпеки. Вбачається, що вивчення, опанування та впровадження кращих практик країн НАТО (Франція, Польща) щодо інституційного створення кібервійськ надасть змогу прискорити запуск та подальшу розбудову в Україні власних кіберсил в умовах тотальної війни з метою запровадження механізмів кіберстримування збройної агресії та надання відсічі агресору у кібердомені, успішного проведення превентивних наступальних кібероперацій.

Література:

1. Красніков С.А. Організаційно-правові засади посилення спроможностей держави у сфері забезпечення кібероборони. *Інформація і право.* 2021. № 4(39). С. 155-161.
2. Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. *Наука і правоохоронна.* 2023. №1 (59). С. 77-85.
3. Діордиця І.В. Адміністративно-правовий зміст національної системи кібербезпеки як складника системи національної безпеки України. *Актуальні проблеми вітчизняної юриспруденції.* 2021. №1. С. 79-83.
4. Котихова Л.Д. Дослідження використання ІТ для протидії поширенню російської дезінформації в медіапросторі в умовах війни. *Вісник Приазовського Державного Технічного Університету. Серія: Технічні науки*, (44), 5–9. https://doi.org/10.32782/2225-6733.44.2022.1
5. Чевардін В.Є., Мазулевський О.Є. Аналіз структур кіберкомандувань розвинутих країн. *Збірник наукових праць ВІТІ.* 2020. № 2. С. 121-128.
6. Фіца В.М. Інституційне забезпечення створення кібервійськ в Україні. *Інформація і право.* 2021. № 3 (38). С.109-114.
7. Аванесова Н., Сергієнко Ю., Любушин Р. Посилення кіберзахисту держава та створення кібернетичних військ: стан, проблеми та організаційно-економічні заходи для України. *Економічні іновації.* 2022. №1(82). С.25-40. URL: https://doi.org/https://doi.org/10.31520/ei.2022.24.1(82).25-40
8. Smeets Max. No Shortcuts: Why States Struggle to Develop a Military Cyber-force. *Oxford University Press. Hurst,* 2022. 296 p. URL: https://doi.org/10.1093/oso/9780197661628.001.0001
9. Gueorgui Dimitrov. A Brief history of Cyber Intelligence: How did Computer Data Evolve to Be Used for Intelligence Operations. *American Intelligence Journal.* 2020. Vol 37. №1. P. 107-114.
10. Arrêté du 4 mai 2017 modifiant l'organisation de l'état-major des armées URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000034581382/2021-07-15/
11. Élements Publics de Doctrine Militaire de lute informatique d'influence URL: https://www.defense.gouv.fr/sites/default/files/ema/doctrine_de_lutte_informatique_dinfluence_l2i.pdf
12. Ustawa «O krajowym systemie cyberbezpieczeństwa» 05.07.2018 URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/krajowy-system-cyberbezpieczenstwa-18746756
13. Міністерство оборони Польщі. Концепція організації та функціонування Сил оборони кіберпростору (CYBER.MIL.PL). URL: https://www.cyber.mil.pl
14. Ustawa «O obronie Ojczyzny» 11.03.2022 URL:https://eli.gov.pl/eli/DU/2022/655/ogl
15. Polish cyber claws. Building of the cyber army of the rising military power in Europe URL: https://pulaski.pl/polish-cyberclaws-building-of-the-cyberarmy-of-the-rising-military-power-in-europe-2/
16. Живило Є.О., Шевченко Д.Г., Черноног О.О. Типологія систем кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) призначення. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2021. №3 (42). С. 37-44.

Horun O. The foreign experience of legal security and features of the creation of cybertroops on the example of some NATO states

Summary. The article examines the prerequisites for the formation of cyber troops on NATO territory. The principles of NATO's security policy in cyberspace are defined. The issues of ensuring cyber defense, protecting critical information infrastructure from cyber-attacks, conducting preventive offensive operations in cyber space within the framework of NATO normative documents are updated. The concept of cyber defense (Cyber Defense) of NATO is considered and the achievements of the Alliance in this area are summarized. The role and place of cyber security in the national security system under the auspices of NATO is defined. Special attention is paid to the French model of creation and functioning of cyber forces. The structure and composition, regulatory and legal regulation of the practical activity of the French cyber command have been determined. The directions of conducting defensive operations in the cyber domain have been revealed. The order and features of offensive operations are detailed. The questions of further development of structural units of cyber forces and funding of cyber command activities is outlined. The main tasks in the field of information and psychological warfare with the participation of French cyber units have been determined. The priorities in the field of development of the cyber defense system of the French Armed Forces until 2025 are detailed. It was concluded that a compact highly specialized structure of cyber troops of the highest strategic level has been created in France. The advantages of France's cyber forces compared to the USA and Great Britain are determined. The modern Polish experience of the institutional creation of cyber troops is considered. It was emphasized that the process of creating Polish cyber defense forces is based on the experience of creating Polish special units. The number of units of Poland's cyber forces has been normalized and determined. The concept, structure and specialized component of the Polish cyberspace defense forces are defined. The legislative foundations, strategic tasks and prospects of the activities of the units of the Polish cyber forces are outlined. It is understood that the Polish Cyber Defense Force is responsible for cyber security, including defense, intelligence and offensive, as well as countering psychological and information operations. The issue of partnership cooperation between the cyberspace defense force of Poland and NATO is highlighted. On the basis of the conducted analysis, it was concluded that cyber troops are a new component of the Armed Forces of the leading NATO countries, which carry out both defensive and offensive operations in cyberspace, implement measures of informational and psychological combat. It is summarized that both French and Polish models of institutional creation of cyber troops can be used as a basis for the formation of cyber troops in Ukraine, which is one of the primary tasks of the security and defense sector in the conditions of a total cyber war with the russian federation.

Key words: cyber defense, cyber military, cyber security, cyber domain, cyber defense, security environment, national security, NATO.