УДК 342.951
DOI https://doi.org/10.32782/2307-1745.2024.71.23

Федієнко О. П.,
здобувач наукового ступеня

КІБЕРВІЙСЬКА КНДР: ОЦІНКА ВРАЗЛИВОСТЕЙ ТА ЕКЗИСТЕЦІЙНА ЗАГРОЗА ДЛЯ УКРАЇНИ

Анотація. Стаття присвячена дослідженню проблематики використання військово-політичним керівництвом КНДР кібервійськ для досягнення своїх геополітичних цілей. Визначені загальні тенденції та організаційно-правові засади співпраці КНДР та РФ у сфері військово-оборонній сфері. Узагальнено напрями розвитку власного кіберпотенціалу. На підставі оприлюднених звітних матеріалів експертів ООН, національної розвідувальної служби Південної Кореї розкрито сфери діяльності та окреслено загрози, які поширює північнокорейський провладний режим у кіберпросторі. Визначено геополітичну кібернетичну стратегію КНДР та її складові. Висвітлено історичний ракурс формування та інституційного розвитку північнокорейських кібервійськ. Деталізовано склад підрозділів кібервійськ КНДР, їхні функціональні завдання, повноваження, структуру, компетенцію та стратегічні напрями діяльності. Висвітлено компетенцію військово-політичного керівництва КНДР, і зокрема Головного розвідувального бюро як координатора діяльності північнокорейських кібервійськ та хакерських кібероперацій. Узагальнено повноваження Департаменту державної безпеки та Міністерством державної безпеки КНДР в контексті діяльності кібервійськ. Розкрито роль та значення діяльності хакерських угрупувань на державній службі КНДР. Визначено цілі та завдання діяльності північнокорейських хакерів, результати і здобутки їхньої злочинної діяльності у кіберпросторі. Підсумовано, що хакерські угрупування «APT37», «Lazarus» та «BlueNoroff» є аутсайдерами, які працюють під прапором КНДР, здійснюють кібератаки проти державних структур та компаній зарубіжних країн з метою отримання розвідувальних даних та фінансових активів для своїх військових і ядерних програм. Зазначено, що доходи, одержані від атак програм-вимагачів хакери використовують для розширення власної інтернет-інфраструктури, яку потім використовують для здійснення кібершпигунства. Узагальнено зміст та напрямки кібероперацій та кібератак, які здійснюють північнокорейські кіберсили, визначено їхні характерні особливості. Проведено оцінку рівня кіберпотужностей Північної Кореї. Охарактеризовано кібероперації, які проводить КНДР та визначено їхні відмінні характеристики. Узагальнено стан готовності КНДР до ведення кібервійни. Акцентовано увагу на питаннях підготовки кадрів для північнокорейських кібервійськ. Підсумовано, що з метою оптимізації усіх південнокорейських військових ресурсів та можливостей, міністерство оборони КНДР щорічно оновлює генеральний план оборонної кіберполітики, складовою частиною якого є наступальні дії у кіберпросторі, використання сил хакерських угрупувань та порядок обмін кібернетичним досвідом з партнерами – РФ та КНР. Визначено, що КНДР генерує до 50% своїх валютних надходжень саме завдяки протиправній кібердіяльності, при цьому доходи від кібератак спрямовуються безпосередньо для фінансування ядерних та ракетних програм північнокорейського режиму. Зроблено висновок про загрозливі тенденції військової присутності КНДР як супротивника, проведено оцінку її кіберпотенціалу. Визначено подальші перспективні шляхи забезпечення стримування агресивних дій КНДР у кіберпросторі як з боку світової спільноти, так і України.

Ключові слова: кібератака, кіберзахист, кібероперація, кібердомен, кіберпростір, кібервійська, кіберспроможності, кібервійна, хакерські угрупування, збройна агресія, військово-оборонний сектор, оборонні технології, фінансові пограбування, банківська система, шкідливе програмне забезпечення, інформаційно-комунікаційні системи, Північна Корея (КНДР).

Постановка проблеми. 19 червня 2024 року держава-агресор та КНДР уклали договір про всеосяжне стратегічне партнерство, яким передбачається надання взаємної допомоги за умови виникнення агресії проти одного з учасників укладеної угоди, передусім включає такі сфери як: розвиток співробітництва у галузі економіки, політики та військової справи. 9 листопада 2024 року диктатор Путін підписав закон про ратифікацію цього договору, приєднавши його до національного законодавства РФ, а глава КНДР підписав відповідний ратифікаційний указ 11 листопада 2024 року [1]. Стаття 2 цього договору визначає, що у разі виникнення безпосередньої загрози акту збройної агресії щодо однієї країни, інша повинна на її вимогу негайно задіяти двосторонні канали щодо надання допомоги з метою сприяння усуненню загрози, що виникла. Одночасно вказаний договір присвячений співпраці імперій зла у сфері боротьби з міжнародним тероризмом та іншими викликами, у тому числі незаконними фінансовими потоками, фінансуванням поширення зброї масового знищення, в галузі безпеки інформаційних і комунікаційних технологій тощо. Договір визначає передумови та формат подальшої співпраці зокрема у кібернетичній сфері, закладає фундамент для проведення подальших спільних досліджень, опанування та удосконалення використання сучасних хакерських технологій. У рамках домовленостей Північна Корея та Росія спільно розроблятимуть та планують обмінюватися шкідливим програмним забезпеченням, яке може використовуватися для амбітних злочинних цілей: фішингу, успішних кібератак нульового дня, зломів будь-якої операційних систем тощо. Цей потворний альянс може ймовірно призвести до небезпечного обміну досвідом і ресурсами, потенційно підвищивши рівень загроз для як для України, так і міжнародної безпеки. Тобто Росія та КНДР запустили механізми спільної консолідованої співпраці шляхом створення спільного військового альянсу у боротьбі проти цивілізованого світу і зокрема у війні проти України. Після підписання угоди між Росією та

КНДР у рамках її виконання, починаючи з жовтня 2024 року остання почала направляти своїх солдат воювати проти України пліч-о-пліч з російськими окупантами до Курської області. За таких умов війна в Україні набуває масштабів та інтернаціоналізується, виходить за межі двох держав, при цьому КНДР стає реальним та потужним ворогом для України, як на полі бою, так і у кібердомені.

З метою вивчення наявних сил та засобів реального супротивника, в сучасних умовах становлять не аби який науково-практичний інтерес структура, повноваження, сфера діяльності, існуючі особливості підготовки фахівців північнокорейських кібервійськ, які отримали славу найкращих зловмисників – хакерів у світі. За таких умов обраний тематичний напрям є актуалізованим та таким, що заслуговує на увагу в контексті необхідності формування системи знань про ворога, його спроможності у кіберпросторі, розуміти стратегічні задуми, цілі та завдання КНДР у кібердомені, особливо в умовах приєднання КНДР до війни проти України на боці РФ.

Стан дослідження. Законодавче забезпечення та особливості створення кібервійськ в зарубіжних країнах досліджували: О. Горун [2], Н. Ткачук [3], В.Чевардін та О. Мазулевський [4], В. Фіца [5]. На монографічному рівні питання, присвячені створенню та інституційному становленню кібервійськ частково висвітлювали: О. Задерейко, О. Троянський, Р. Чанишев, А. Дика [6], Ю. Даник, П. Воробієнко, В. Чернега [7]. У зарубіжній науковій літературі досвід діяльності північнокорейських кібервійськ та деякі питання стратегії їхнього розвитку перебували у фокусі уваги: Д. Пінкстона [8], М. Раскі [9] та інших. Проте жоден із вказаних науковців предметно не розглядав питання функціонування північнокорейських кібервійськ, які становлять суттєву загрозу як для цивілізованого світу, передусім для США та Південної Кореї, а з 2024 року і для України. Саме тому висвітлення та узагальнення північнокорейського досвіду створення та діяльності кібервійськ надасть змогу провести на науково-практичному рівні реальну оцінку кіберпотенціалу ворога, визначити його слабкі місця та сильні сторони, можливі сценарії перспективної злочинної та ворожої діяльності у кіберпросторі з прицілом на Україну, державні інформаційні ресурси, інформаційно-комунікаційні системи, об`єкти критичної інфраструктури тощо.

Метою статті є узагальнення особливостей функціонування північнокорейської моделі кібервійськ, визначення мети та стратегічних завдань їхньої хакерської діяльності у кіберпросторі, проведення оцінки спроможностей та загрозливих тенденцій розвитку ворожого для України кібернетичного війська КНДР.

Виклад основного матеріалу. З 2014 року Північна Корея активно та динамічно розвиває свої цифрові можливості, становлячи значну загрозу для фінансових установ, урядових закладів, мереж безпеки навколо світу. КНДР розглядає кіберпростір як важливу частину свого геополітичного планового розвитку, військового прогресу на перманентній основі. Це єдина країна світу, уряд якої підтримує злочинне хакерство заради отримання грошової вигоди, прибутків за рахунок крадіжок та досягнення власних геополітичних цілей. На відміну від міжнародних терористичних організацій, північнокорейські кіберзлочинці жодним разом не брали на себе відповідальність за будь-які кібератаки та їхні наслідки.

Відповідно до звіту експертів ООН «Щодо санкцій проти Північної Кореї» [10], тільки у 2019 році КНДР отримала понад $2 млрд. за допомогою кіберзлочинності та успішних кібератак. КНДР продовжує викрадати сотні мільйонів доларів із фінансових установ, криптовалютних компаній і бірж навколо світу, оскільки незаконно викрадені фінансові ресурси є важливим джерелом прибутків, які спрямовуються на розвиток ядерної і ракетної програм. У 2021 році було викрадено криптовалюти на загальну суму 400 млн. доларів шляхом посягань на світові криптобіржі та міжнародні інвестиційні корпорації. Під час проведення кібератак використовувалися фішингові приманки, кодові експлойти, зловмисне програмне забезпечення, передова соціальна інженерія з метою перекачування коштів із підключених до Інтернету «гарячих» гаманців цих організацій на IP-адреси, контрольовані урядом КНДР. Згідно із оприлюдненим звітом компанії «Microsoft» у 2023 році, хакери з КНДР вкрали від 600 мільйонів до $1 млрд, які згодом були спрямовані Пхеньяном на фінансування більшої половини своїх ядерних розробок й випробувань. Це переконливо засвідчує прагнення КНДР завдяки кіберзлочинцям посилити свої фінансові можливості та здійснювати просування власних стратегічних інтересів [11]. 31 липня 2024 року Національна розвідувальна служба Південної Кореї оприлюднила звітні матеріали щодо оцінки кібернетичного потенціалу КНДР [12], відповідно до якого чисельність структур КНДР, пов'язаних із кіберопераціями та проактивною хакерською діяльністю складає 8 тис. 400 осіб та має стрімку тенденцію до постійного збільшення. На цьому фоні Росія і КНДР проводять спільні дослідження в галузі високих технологій, включно із розробками шкідливого програмного забезпечення, використовуючи штучний інтелект. Окрім того, взаємна довіра та співпраця у кіберсфері між РФ, КНР і КНДР в останні роки також є демонстративним фактором світової нестабільності та на переконання експертів є глобальною стратегічною загрозою на перманентній основі.

Геополітична кібернетична стратегія КНДР базується на тому, що важливими для уряду цієї країни є збір та узагальнення здобутої аналітичної й статистичної інформації про держави, які визнані ворожими, викрадення державних секретів у супротивних до режиму Кіма країнах, значних фінансових ресурсів, проведення підривних та руйнівних зовнішніх кібероперацій тощо. З цією метою кібератаки КНДР здебільшого проводяться проти Південної Кореї, меншу кількість – проти державних органів та структур, розташованих на території США [13]. Протягом останніх років північнокорейські військові та хакери розпочали використовувати технології штучного інтелекту з метою проведення складніших кібератак на різні військові та фінансові організації, об'єкти критичної інфраструктури, що цілком підтверджують світові гіганти, розробники технологій ШІ: OpenAI, компанія Microsoft, уряд Південної Кореї, які регулярно фіксують спроби проведення таких кібератак. Здебільшого такі атаки здійснюються через фішинг і соціальну інженерію, а технологічно штучний інтелект допомагає КНДР приховати свої слабкі сторони, як-от погане знання мови або брак комунікативних навичок. Через недоступність західних застосунків військові хакери користуються виключно китайськими розробками, але також самі вивчають й опановують цей напрямок. Таким чином, КНДР отримує прибуток від злому фінансових установ, крадіжки віртуальних активів і поширення програм-вимагачів [14].

Інституційно кібервійська КНДР, які мають офіційну назву «підрозділи кібервійни» почали створюватися ще при Кім Чен Ірі, який вважав, що програмування та розвиток високих технологій має значно покращити економічне становище країни та сприяти прогресу. Основи північнокорейських кібероперацій були закладені ще в 1990-х роках, після того, як північнокорейські фахівці-комп'ютерники повернулися із закордонної подорожі, запропонувавши використовувати Інтернет як засіб для шпигування за ворогами та нападу на військових супротивників, таких як США та Південна Корея. У 2009 році уряд КНДР об'єднав усі свої служби розвідки та внутрішньої безпеки і передав їх під прямий контроль Комісії національної оборони з метою посилення ролі та значення тодішнього лідера країни Кім Чен Іна, який, у свою чергу, стояв у джерел створення кіберпідрозділу «Бюро 121» у складі Управління Генерального штабу Головного розвідувального бюро «General Bureau of Reconnaissance» (RGB) [15], яке вважається ключовим військовим органом розвідки та таємних операцій Північної Кореї та є відповідальним за усі хакерські кампанії. За сприяння Головного розвідувального бюро Пхеньян активно нарощує потенціал для ведення кібервійни, частина його спрямована на Південну Корєю, яка все ще перебуває у стані конфронтації з КНДР.

При цьому, важливе місце посідає підготовка кадрів для кібервійськ. Пом'якшивши сувору соціальну ієрархію, Північна Корея відкрила можливості для молоді з усіх верств населення приєднатися до навчальних ІТ-програм, створивши сучасну групу потенційних новобранців-хакерів. У країні тотального зла соціальний статус, як-от місце проживання та різновид занять, зазвичай суворо визначаються на основі кровної лінії, але винятки становлять щодо тієї категорії осіб, які приєднається до програми навчання хакерів. Саме такі поступки з боку керівництва Пхеньяну надало можливість організувати пошук молодих талантів у математиці та комп'ютерних науках, щоб згодом зробити з них професійних військових хакерів. З цією метою Головне розвідувальне бюро КНДР здійснює відбір дітей віком 14–15 років або навіть молодше, яких спочатку навчають у середній школі Кумсон, а потім вони вступають до Університету Кім Ір Сена або Технологічного університету імені Кім Чаека для проходження подальшого навчання, після закінчення якого випускники отримують призначення до підрозділів кібервійськ при Головному розвідувальному бюро. Для викладання комп'ютерних та технічних дисциплін, теорії та основ інформатики активно залучаються викладачі російської загальновійськової академії збройних сил. Кібервійськові КНДР користуються різними перевагами, зокрема ним надається можливість навчатися або працювати за кордоном, а також різні економічні стимули. Наприклад, якщо було успішно зламано криптобіржу, вони можуть гарантовано отримати 10% від отриманого злочинного прибутку.

Основою кібервійськ КНДР є елітний спецпідрозділ «Бюро 121», створений для проведення наступальних дій у кіберпросторі, корпоративного кібершпигунства, фінансових крадіжок, розробки власних зразків кіберзброї, проведення спеціальних інформаційних операцій. Переважну більшість своїх кібероперацій цей спецпідрозділ здійснює за межами країни та є причетним до хакерських операцій, які фінансуються урядом КНДР проти своїх оголошених ворогів. У фокусі уваги перебувають міжнародні фінансові системи, включно з криптовалютними біржами. «Бюро 121» нараховує приблизно 6 тис. співробітників, багато з яких пройшли навчання КНР та РФ і набули досвіду наступальних кібертактик, опанували передові методи злому інформаційно-комунікаційних систем та комплектується військовими хакерами. До складу цього підрозділу входить також «лабораторія 110», яка є відповідальною за матеріально-технічне оснащення та озброєння кібервійськ, та яка одночасно здійснює заходи радіоелектронної боротьби. У 2013 році Головне розвідувальне бюро утворило таємний «відділ 180», якому було доручено проводити спецоперації з метою зламу міжнародних фінансових установ, викрадення валюти на підтримку ядерної програми та програм підготовки балістичних ракет. У рамках реалізації злочинного задуму шкідливі бекдори мали встановлюватися в зарубіжних компаніях, які спеціалізуються на розробках програмного забезпечення в США та Японії. Переважна більшість хакерів-вояків працює під прикриттям у спільних підприємствах, організованих між КНДР та КНР, іншими країнами Південно-Східної Азії (Японія, Камбоджа, М'янма, Лаос). У фокусі уваги хакерів перебувають банки та фінансові установи, криптобіржі. Згодом «відділ 180» отримав спеціалізацію щодо проникнення до криптовалютних бірж, тоді як «Бюро 121» розширило свої кіберспроможності за межі кордонів, атакуючи іноземну інфраструктуру на різних континентах, включаючи Австралію, США, Аргентину, країни ЄС.

У 2014 році лідер КНДР Кім Чен Ін заявив, що кібервійна разом із ядерною зброєю та ракетами є «універсальним мечем», які гарантують ударні можливості у кіберпросторі [16]. На додаток до ядерної та балістичної ракетних програм, КНДР розвиває пов'язані з кібернетичними засобами наступальні військові можливості. У 2014 році було створено ще один бойовий підрозділ – «Підрозділ 91», який займається розробками у сфері передових технологій, керує плануванням і виконанням кібероперацій, спрямованих як на військові, так і на цивільні об`єкти. «Підрозділ 91» забезпечує повну інтеграцію кіберпотенціалу Північної Кореї в її більш широку військову стратегію, що дозволяє режиму Кіма використовувати кібертактику як доповнення до своїх звичайних військових операцій. У складі «Підрозділу 91» функціонують «128 офіс» та «414 офіс», які відповідають за підтримку зв'язку із шпигунськими мережами в Південній Кореї, включаючи контроль за агентурною мережею. Зокрема, «128 офіс» працює над зломом іноземних веб-сайтів інформаційної розвідки та вивчає зарубіжні кіберстратегії, тоді як «офіс 414» готує кіберекспертів для ведення кібервійни. Окрім спецпідрозділу «Бюро 121», 180-ого відділу та «Підрозділу 91», які структурно входять до складу Головного розвідувального бюро на службі уряду перебувають вмотивовані хакери, які об'єдналися в різні угруповання з метою виконання поставлених перед ними злочинних завдань. В КНДР існує три потужних кібернетичних хакерських угрупування під кодовою назвою «Kimsuky» або «APT37», «Lazarus» та «BlueNoroff». «Kimsuky» або «APT37» (Advanced Persistent Threat) створена у 2012 році є північнокорейською хакерською командою, яка є причетною до масованих кібератак на південнокорейські дослідницькі центри, об'єкти промисловості, операторів ядерної енергетики, організації і установи державного та приватного сектору тощо. Під час кібератак

хакери використовують рудиментарне, але ефективне шкідливе програмне забезпечення, яке отримало назву «DarkSeoul». Хакери «Kimsuky» або «APT37» здебільшого здійснюють кібершпигунство проти установ та організацій, що мають локацію у Південно-Східній Азії, що є свідченням того, що КНДР демонструє переважно кіберактивність у цьому регіоні, вирішивши зосередитися, у першу чергу, на своєму сусіді – Південній Кореї, а також час від часу здійснюючи кібератаки на свого іншого давнього ворога – США. Починаючи з 2017 року хакери «APT37» розширили спектр своїх нападів у глобальних вимірах, постійно вдосконалюють тактику кібератак, поєднуючи їх з використанням методів соціальної інженерії. У 2020 році хакери «APT37» вчинили кібератаку на військові підприємства України, Туреччини та Словаччини шляхом створення підробленої сторінки авторизації в поштовому сервісі «Outlook». У 2023 році хакери «APT37» таємно зламали комп'ютерні мережі потужного російського розробника ракет «НВО машинобудування», що є флагманом у сфері розробок гіперзвукових ракет, супутникових технологій і балістичних озброєнь нового покоління й проникли до IT-середовища цієї компанії, що надало їм можливість отримати доступ до електронної пошти, перемикатися між мережами та отримувати конфіденційні дані [17]. Наприкінці вересня 2024 року північнокорейські хакери «APT37» здійснили кібератаку на німецьку оборонну компанію «Diehl Defense» [18], яка була спрямована на викрадення конфіденційної інформації, пов'язаної з оборонними проектами та технологіями, що використовуються у виробництві озброєння. Тактично кібероперації, як правило, проводяться за одним і тим же сценарієм, при цьому основним початковим вектором інфікування, який використовує «APT37» є стрімкий та удосконалений фішинг.

У свою чергу, хакерське угрупування «Lazarus» та його підгрупи залучаються до кібероперацій більш широкого спектру, які є різноманітними за масштабом і глобальні за характером. Загалом «Lazarus Group» є таємною кіберзлочинною групою під егідою уряду КНДР, яка спеціалізується на викраденні фінансів та криптовалют навколо світу. Так, у 2014 році це хакерське угрупування атакувало голівудську студію «Sony», а у 2016 році викрали $81 млн з Центробанку Бангладеш [19]. За вказаними фактами цих кібератак у США були порушені кримінальні справи, проте жодного обвинувачення нікому не було висунуто. У 2024 року «Lazarus» розробило нову схему з метою крадіжки персональних даних користувачів соціальних мереж та цифрових активів, у тому числі хакери створили підставну NFT-гру, яка автоматично зламувала «Google Chrome» і викрадала дані [20].

У 2019 році хакери «Lazarus» викрали 10 млн. доларів США з чилійського банку, а 2 вересня 2020 року Всесвітнє товариство міжбанківських фінансових телекомунікацій (SWIFT) офіційно повідомило, що КНДР розпочала відмивати гроші за допомогою криптовалют. Протягом 5 останніх років, у період з 2020 по 2024 роки хакери «Lazarus» сумарно вкрали фінансових активів на загальну суму $2,4 млрд: понад 70% коштів, які опинилися у розпорядженні хакерів було отримано за допомогою компрометації приватних ключів постраждалих компаній та приватних осіб. У березні 2024 року однією з останніх цілей «Lazarus» стала ігрова платформа Munchables, створена на базі L-2 рішення Blast. За наслідками успішної кібератаки хакери вкрали 17 500 ETH ($62,5 млн). Тобто хакерське угруповання «Lazarus» стоїть за безліччю кампаній, серед яких кібершпигунство, посягання на міжнародні фінансові установи.

«BlueNorOff» – фінансово мотивована хакерська група, в основному відома своїми атаками на криптовалютні біржі та фінансові організації, включаючи венчурні підприємства та банківські установи по всьому світу. Міністерство фінансів США вважає BlueNoroff підрозділом хакерського угруповання «Lazarus» проводить кібератаки на світовий криптовалютний сектор, постійно випускаючи нову кампанію шкідливого програмного забезпечення, націлену на криптовалюти. Протягом багатьох років «Bluenoroff» постійно вдосконалювала свої методи злому, щоб випереджати заходи безпеки, які застосовують фінансові установи. «BlueNoroff» тісно пов'язана із сумнозвісною хакерською групою «Lazarus», з 2019 року атакує різні криптовалютні компанії та приватних осіб за допомогою витончених фішингових тактик. Хакери «BlueNoroff» активно використовують методи соціальної інженерії під час кібератак на централізовані біржі та децентралізовані фінансові платформи (DeFi), щоб ввести в оману співробітників та змусити їх перейти за шкідливими посиланнями, замаскованими під тести або заявки на працевлаштування. Особливий інтерес представляють компанії, які обслуговують криптовалютні біржові фонди (ETF) та подібні фінансові продукти. «BlueNorOff» також бере участь у фішингових операціях, під час яких вони надсилають ретельно продумані електронні листи чи повідомлення, щоб оманою змусити користувачв розкрити конфіденційну інформацію.

Таким чином, хакерські угрупування «APT37», «Lazarus» та «BlueNoroff» є аутсайдерами, які працюють під прапором КНДР, уряд якої стимулює та спонсорує хакерські атаки з метою спрямовування зусиль проти державних структур та компаній зарубіжних країн, отримання розвідувальних даних та фінансових активів для своїх військових і ядерних програм. Доходи, одержані від атак програм-вимагачів зловмисники використовують для розширення власної інтернет-інфраструктури, яку потім використовують для здійснення кібершпигунства. Головне розвідувальне управління разом з іншими ключовими структурами, такими як «Бюро 121», Департаментом державної безпеки, Міністерством державної безпеки координують дії хакерських північнокорейських груп. Так, зокрема Департамент державної безпеки відповідає за підтримку внутрішньої безпеки та забезпечення лояльності північнокорейських оперативників, дислокованих за кордоном, відіграє вирішальну роль у кібероперациях КНДР, здійснюючи нагляд у сфері кібершпигунства та сприяючі хакерам, які залучені до іноземних місій. Оперативники Департаменту державної безпеки КНДР тісно співпрацюють з Бюро 121, обмінюючись розвідданими і координуючи кібератаки на політичні організації, фінансові установи та критичну інфраструктуру. Департамент державної безпеки уважно стежить за хакерами, використовуючи їхні родини як важіль для запобігання дезертирству. Відстежуючи цифрові комунікації громадян КНДР, співробітники департаменту можуть ідентифікувати дисидентів і забезпечити швидку нейтралізацію будь-якої потенційної опозиції режиму. У свою чергу, міністерство державної безпеки, яке ще називають таємною поліцією має завдання підтримувати дисципліну серед кібероператорів країни та гарантує,

що кібероперації залишаються під суворим контролем режиму. Департамент військово-цивільного зв'язку керує закордонними кіберопераціями КНДР. Посольства в таких країнах, як Китай, Росія та Малайзія, слугують центрами кібероперацій, а персонал посольств КНДР за кордоном активно залучається до координації кібероперацій і сприяння відмиванню коштів. Участь закордонних дипломатичних представництв КНДР у кібероперацій підкреслює ступінь інтеграції кібервійни в дипломатичну стратегію режиму, який використовує дипломатичні привілеї, щоб уникнути виявлення та кримінального й судового переслідування.

Таким чином кібероперації КНДР відображають щонайменше три відмінні характеристики. По-перше, кіберпідрозділи та хакерські групи демонструють значне розмаїття з точки зору своїх можливостей і досвіду – діапазон, який ускладнив їхню атрибуцію. Межа між кіберопераціями низького та високого рівня в кіберпросторі досить часто є розмитою. По-друге, КНДР поступово демонструє рішучість до кіберескалації – націлювання на національну критичну інфраструктуру інших держав, а також приватні корпорації, банківські установи, фінансові компанії. Північна Корея все частіше прагне отримати незаконну фінансову вигоду, обходячи міжнародні санкції та генеруючи викрадені активи. По-третє, основна «діалектика кіберпростору КНДР» все ще асиметрична. Інтернет-інфраструктура КНДР ізольована від глобальних цифрових мереж, значною мірою відключена від мережі Інтернет та доволі обмежена китайським «Великим брандмауером», оскільки увесь інтернет-трафік країни проходить лише через двох провайдерів – китайський «Unicom» і російський «TransTeleCom».

За експертними оцінками рівень кіберпотужностей Північної Кореї наближений до російського та китайського. Однією з найбільш характерних особливостей кібероперацій Північної Кореї є акцент на довгостроковому стратегічному плануванні. На відміну від багатьох кіберзлочинних організацій, які прагнуть отримати негайну фінансову вигоду, північнокорейські хакерські групи витрачають роки на проникнення в мережі, збір розвідувальних даних і визначення вразливостей перед тим, як розпочати кібератаку. Цей методичний підхід відображає ширшу військову доктрину терпіння та точності режиму, де кібероперації ретельно розраховуються для досягнення максимального ефекту з мінімальним ризиком. У свою чергу, кібератаки ніколи не здійснюються з території КНДР, оскільки такі напади можна легко відстежити, у зв`язку з чим Головне розвідувальне управління КНДР відправляє хакерів, які діють під прикриттям, до Китаю, Росії та навіть Європи, видаючи себе за «програмістів», які хочуть дізнатися про розробку нових комерційних програм. За кордоном працюють 600 хакерів, які займаються викраденням сучасних технологій, кібершахрайством, фішингом, здійснюють несанкціонований доступ до державної та комерційної таємниці.

Типовою схемою, яку використовують хакери КНДР є укладання контрактів на дистанційну роботу з сотнями американських, європейських або азійських компаній. При цьому для працевлаштування хакери подають анкету іншого громадянина, яка доповнюється відредагованою за допомогою штучного інтелекту фотографією. Виявлення таких фактів вимагає від уряду США та інших постраждалих країн відповідного реагування, що передбачає накладення санкцій на окремих осіб або їхнього кримінального переслідування. З вересня 2019 року діють накладені Міністерством фінансів США санкції проти північнокорейських хакерських груп, підпорядкованих Головному розвідувальному бюро, при цьому «Hidden Cobra» – загальний термін, яким США позначають зловмисну кіберактивність уряду КНДР та її хакерських злочинних угрупувань.

З метою оптимізації усіх південнокорейських військових ресурсів та можливостей Міністерство оборони КНДР щорічно оновлює генеральний план оборонної кіберполітики, складовою частиною якого є наступальні дії у кіберпросторі, використання хакерських угрупувань, обмін кібернетичним досвідом з партнерами – РФ та КНР. Оскільки міжнародні санкції руйнують економіку Північної Кореї, кіберзлочинність та хакерство стали критичними та доступними джерелами надприбутків. КНДР генерує до 50% своїх валютних надходжень завдяки протиправній кібердіяльності, при цьому доходи від кібератак спрямовуються безпосередньо для фінансування ядерних та ракетних програм північнокорейського режиму. На теперішній час прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі, розширюється коло держав, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі [21, с. 247].

Висновки. Тоталітарний режим КНДР має власні кібервійська, які використовуються для досягнення амбітних злочинних цілей. Кібервійська КНДР структурно входять до складу Головного розвідувального бюро із загальною чисельністю 8400 осіб, при цьому кібернетичний потенціал КНДР динамічно розширюється із загрозливою швидкістю, створюючи серйозну загрозу глобальній безпеці. Північнокорейські хакерські угрупування «APT37», «Lazarus» та «BlueNorOff» працюють на уряд, завдяки яким ця країна незаконно здобуває криптовалюту, викрадає важливу конфіденційну і безпекову інформацію навколо світу. Провладний режим КНДР застосовує кібервійська та вмотивованих хакерів, поєднує використання складних тактик з метою проведення цілеспрямованих кібератак, спроб працевлаштувати на умовах дистанційної роботи фальшивих ІТ-працівників у великих компаніях зарубіжних країн, застосовує методики приховування шкідливого коду в репозиторіях, які використовуються розробниками програмного забезпечення, масово поширює програми-вимагачі. Таким чином, Пхеньян намагається протистояти запровадженим економічним санкціям за допомогою кібероперацій, збираючи сотні мільйонів доларів на підтримку режиму Кіма та його ядерної й балістичної ракетної програм.

Оскільки КНДР є агресивним ворогом України, то у фокусі уваги кібервійськ цієї країни ймовірно можуть перебувати вітчизняні підприємства оборонно-промислової галузі, державні інформаційні ресурси, об`єкти критичної інфраструктури тощо. У зв'язку з цим потребує удосконалення система розвідувального забезпечення кібербезпеки України в частині створення, розвитку сил, засобів та інструментів упередження загроз національній безпеці у кіберпросторі, особливо які поширює КНДР. Окрім того, в контексті актуалізації північнокорейської військової загрози для України доцільно через можливості ГУР МО посилити спроможності вітчизняних розвідувальних органів щодо виявлення та припинення діяльності хакерської агентури КНДР за кордоном, особливо у сусідніх

з Україною державах. В контексті викладеного, прискорення створення підрозділів кібервійськ в Україні є важливим та рішучим кроком, який спрямований на запровадження дієвих та ефективних механізмів стримування та відсічі російській та південнокорейській агресії у кібердомені, особливо в умовах триваючої кібервійни.

Література:

1. КНДР ратифікувала договір про всеосяжне стратегічне партнерство з Росією. URL: https://www.pravda.com.ua/news/2024/11/12/7484016
2. 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.
3. Ткачук Н.А. Досвід США зі створення та розбудови Кіберкомандування: уроки для України. *Інформація і право.* 2024. № 1 (48). С. 139–149.
4. Чевардін В.Є., Мазулевський О.Є. Аналіз структур кіберкомандувань розвинутих країн. *Збірник наукових праць ВІТІ.* 2020. № 2. С. 121–128.
5. Фіца В.М. Інституційне забезпечення створення кібервійськ в Україні. *Інформація і пбраво.* 2021. № 3 (38). С. 109–114.
6. Задерейко О.В. Концептуальні основи захисту інформаційного суверенітету України : *монографія* / О. В. Задерейко, О. В. Троянський, Р. І. Чанишев, А. І. Дика. 2-ге вид., перероб. і доп. – Одеса : Фенікс, 2022. – 220 с.
7. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. URL: https://metod.suitt.edu.ua/download/686
8. Daniel A. Pinkston. North Korea's Objectives and Activities in Cyberspace. *Asia Policy.* 2020. Vol. 15, № 2. pp. 76–83. URL: https://www.jstor.org/stable/27023903
9. Michael Raska. North Korea's Evolving Cyber Strategies: Continuity and Change. *SIRIUS. Journal of Strategic Analysis.* 2020. № 4. pp. 144–158. URL: https://www.degruyter.com/document/doi/10.1515/sirius-2020-2003/html
10. UN Panel of Experts DPRK 2019 Final Report. URL: https://www.ncnk.org/sites/default/files/UN_POE_March2019_Final_Report.pdf
11. Microsoft Digital Defense Report 2024. URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf
12. 단독]"北에 해커 8400명… 러와 악성코드 공동 개발". URL: https://www.donga.com/news/Politics/article/all/20240731/126221495/2
13. Kim Jong Un Now has a Cyber Army of 8,400 Hackers, South Korean Intelligence Reportedly Said. URL: https://thecyberexpress.com/north-korea-has-a-cyber-army-of-8400-hackers
14. North Korean Cyber-Attacks Cost South Korea $1.2 billion. URL: https://thecyberexpress.com/north-korean-cyber-attacks-cost-south-korea
15. Reconnaissance General Bureau. URL: https://en.wikipedia.org/wiki/Reconnaissance_General_Bureau
16. Ji-Young, K., Lim, J. I., & Kyoung Gon, K. (2019). The All-Purpose Sword: North Korea's Cyber Operations and Strategies. 11th International Conference on Cyber Conflict: Silent Battle, CyCon *Vol. 2019-May.* NATO CCD COE Publications. https://doi.org/10.23919/CYCON.2019.8756954
17. Північнокорейські хакери атакували провідне російське ракетно-конструкторське бюро, − Reuters. URL: https://ms.detector.media/kiberbezpeka/post/32629/2023-08-07-pivnichnokoreyski-khakery-atakuvaly-providne-rosiyske-raketno-konstruktorske-byuro-reuters/
18. Північнокорейські хакери атакували збройову компанію ФРН. URL: https://ua.korrespondent.net/world/4719474-pivnichnokoreiski-khakery-atakuvaly-zbroiovu-kompaniui-frn
19. Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million. URL: https://www.nytimes.com/2016/03/16/world/asia/bangladesh-bank-chief-resigns-after-cyber-theft-of-81-million.html
20. Lazarus Group Exploits Google Chrome Flaw in New Campaign. URL: https://www.infosecurity-magazine.com/news/lazarus-group-exploits-google/
21. Скіцько О., Ширшов Р. Нормативно-правове забезпечення кібероборони України: сучасний стан. *Юридичний вісник.* 2024. № 3. С. 224–250.

Fedienko O. Cybertroops North Korea: assessment of vulnerabilities and existential threat to Ukraine

Summary. The article is devoted to the study of the issues of the use of cyber troops by the military-political leadership of the DPRK to achieve its geopolitical goals. The general trends and organizational and legal principles of cooperation between the DPRK and the Russian Federation in the military-defense sphere are determined. The directions of development of its own cyber potential are summarized. Based on the published reports of UN experts and the national intelligence service of South Korea, the areas of activity are revealed and the threats that the North Korean pro-government regime spreads in cyberspace are outlined. The geopolitical cyber strategy of the DPRK and its components are determined. The historical perspective of the formation and institutional development of the North Korean cyber troops is highlighted. The composition of the units of the DPRK cyber troops, their functional tasks, powers, structure, competence and strategic directions of activity are detailed. The competence of the military-political leadership of the DPRK, and in particular the Main Intelligence Bureau as the coordinator of the activities of the North Korean cyber troops and hacker cyber operations, is highlighted. The powers of the Department of State Security and the Ministry of State Security of the DPRK in the context of the activities of the cyber troops are summarized. The role and significance of the activities of hacker groups in the DPRK civil service are revealed. The goals and objectives of the activities of North Korean hackers, the results and achievements of their criminal activities in cyberspace are determined. It is concluded that the hacker groups «APT37», «Lazarus» and «BlueNoroff» are outsiders who work under the flag of the DPRK, carry out cyberattacks against state structures and companies of foreign countries in order to obtain intelligence data and financial assets for their military and nuclear programs. It is noted that the income received from ransomware attacks is used by hackers to expand their own Internet infrastructure, which is then used to carry out cyber espionage. The content and directions of cyber operations and cyber attacks carried out by North Korean cyber forces are summarized, their characteristic features are identified. The level of North Korea's cyber capabilities is assessed. The cyber operations carried out by the DPRK are characterized and their distinctive characteristics are identified. The state of readiness of the DPRK for waging cyber war is summarized. Attention is focused on the issues of training personnel for North Korean cyber forces. It is concluded that in order to optimize all South Korean military resources and capabilities, the DPRK Ministry of Defense annually updates the general plan for cyber defense policy, an integral part of which are offensive actions in cyberspace, the use of hacker group forces, and the procedure for exchanging cyber experience with partners – the Russian Federation and People's

Republic of China. It was determined that the DPRK generates up to 50% of its foreign exchange revenues precisely due to illegal cyber activities, while the proceeds from cyber attacks are directed directly to financing the nuclear and missile programs of the North Korean regime. A conclusion was made about the threatening trends of the DPRK's military presence as an enemy, an assessment of its cyber potential was carried out. Further promising directions of ensuring the deterrence of the DPRK's aggressive actions in cyberspace by both the world community and Ukraine were identified.

Key words: cyberattack, cyberdefense, cyberoperation, cyberdomain, cyberspace, cybermilitary, cybercapabilities, cyberwar, hacker groups, armed aggression, military-defense sector, defense technologies, financial robbery, banking system, malware, information and communication systems, North Korea (DPRK).