Парламентське дослідження щодо інституційного створення та оцінки спроможностей кібервійськ КНДР*

Анотація. *У дослідженні розглянуто питання функціонування кібервійськ КНДР (Північна Корея). Представлена характеристика розгалуженої системи військових органів та хакерських угрупувань, які виконують завдання в інтересах уряду КНДР щодо здійснення фішингу, викрадення криптовалюти, проведення кібератак, зломів операційних систем тощо. Вказано на темпоральне зростання інтересу КНДР до ведення кібервійни у глобальних вимірах. На підставі узагальнення ризиків північнокорейських кібератак, на які вказують, зокрема, іноземні експерти, обґрунтовано важливість створення спеціальних підрозділів кібервійськ в Україні, які забезпечили б стримування і відсіч російської та північнокорейської агресії у кібердомені, що є особливо актуальним в умовах кіберрвійн.*

Ключові слова: *кібервійська, кіберпростір, кібердомен, кібератака, кіберзброя, кібершпигунство, кібербезпека, кіберзагроза, кібероперація, хакери, хакерське угрупування, національна безпека, критична інфраструктура, інформаційно-комунікаційні системи, шкідливе програмне забезпечення, технології штучного інтелекту, несанкціонований доступ до державної таємниці, криптовалюта, криптобіржі, фінансові ресурси, північнокорейський режим, фішинг, соціальна інженерія, міжнародні санкції, економічна ізоляція, КНДР.*

Вступна частина. У червні 2024 року держава-агресор Росія та КНДР уклали договір про всеосяжне стратегічне партнерство, яким передбачається співпраця для зміцнення «багатополярного світового порядку». Протягом жовтня-листопада 2024 року цей договір був ратифікований вказаними державами[1]. Стаття 2 цього договору визначає, що у разі виникнення безпосередньої загрози акту збройної агресії щодо однієї держави, інша повинна на її вимогу негайно задіяти двосторонні канали щодо надання допомоги з метою сприяння усуненню загрози, що виникла. Одночасно вказаний договір присвячений співпраці в галузі безпеки інформаційних і комунікаційних технологій, визначає передумови та формат подальшої співпраці у кібернетичній сфері, закладає фундамент для проведення подальших спільних досліджень і взаємного навчання, опанування та удосконалення використання сучасних хакерських технологій. У рамках домовленостей сторони планують спільно розробляти та обмінюватися шкідливим програмним забезпеченням, яке може використовуватися для амбітних злочинних цілей: фішингу, кібератак нульового дня, зломів будь-якої операційної системи тощо. Тобто Росія та КНДР запустили

[1] Оборонна угода між Північною Кореєю та росією набула чинності. URL: https://chas.news/news/oboronna-ugoda-mizh-pivnichnoyu-koreeyu-ta-rosieyu-nabula-chinnosti

механізми співпраці для боротьби проти цивілізованого світу і, зокрема, спільної участі у війні проти України, утворивши новий військовий союз.

На переконання представників експертного середовища, які демонструють занепокоєння[2], сучасна тактика КНДР у кіберпросторі стає більш витонченою та агресивною, а північнокорейський провладний режим більше не задовольняється фокусуванням на конкретні звичайні цілі, натомість приймає ширший, невибірковий підхід, розкидаючи мережу хакерів у пошуках будь-яких вразливостей у комп'ютерних системах світу. Ця зміна стратегії в поєднанні із швидким зростанням її робочої сили в ІТ-сфері робить Північну Корею непередбачуваним, підступним і фанатичним супротивником у кібердомені, навіть попри значні дистанційні відстані між державами. Оскільки Північна Корея продовжує інвестувати значні кошти у розвиток свого кібернетичного потенціалу, що є потужним викликом та масштабною загрозою для цивілізованого світу, міжнародна спільнота повинна залишатися пильною та розробляти ефективні механізми стримування військової агресії КНДР, зокрема й у кіберпросторі. Розробка надійних механізмів кіберзахисту, оперативний обмін розвідданими і запровадження суворіших санкцій проти північнокорейського провладного режиму є важливими та дієвими кроками для пом'якшення цієї зростаючої міжнародної загрози, що мають бути реалізовані світовою спільнотою.

На виконання узятих на себе зобов'язань КНДР, починаючи з жовтня 2024 року, почала направляти своїх солдат воювати проти України разом із російськими окупантами до Курської області. За таких умов війна в Україні інтернаціоналізується, виходить за межі двох держав, водночас КНДР стає реальним ворогом для України, як на полі бою, так і у кібердомені. З метою дослідження наявних сил і засобів реального супротивника та оцінки його спроможностей у кібердомені, становлять інтерес структура, повноваження, існуючі особливості підготовки фахівців та діяльності північнокорейських кібервійськ. Формування системи знань про ворога, визначення його кіберпотенціалу, розуміння цілей та завдань КНДР у кібердомені, особливо в умовах масштабної війни РФ проти України, є актуальним і своєчасним та потребує проведення дослідження.

Основна частина. З 2014 року Північна Корея активно розвиває свої кіберможливості, становлячи значну загрозу для світових криптобірж, фінансових корпорацій та установ, урядових закладів, безпекових мереж світу. Північна Корея розглядає кіберпростір як важливу частину свого геополітичного розвитку та військового прогресу. Це єдина держава світу, уряд якої підтримує злочинне хакерство заради отримання грошової вигоди, прибутків за рахунок крадіжок і досягнення власних геополітичних цілей. Водночас КНДР активно інвестує у розробки власної кіберзброї, опановує нову кібертактику після того, як

[2] Cyber Defence Cooperation to Deter North Korea. URL: https://www.cgai.ca/cyber_defence_cooperation_to_deter_north_korea

за фактичними розрахунками її збройні сили поступилися своїм арсеналом військовим США та Південної Кореї. На відміну від міжнародних терористичних організацій, північнокорейські кіберзлочинці не беруть на себе відповідальність за будь-які кібератаки та їхні наслідки. Північна Корея продовжує викрадати сотні мільйонів доларів США із фінансових установ, криптовалютних компаній і бірж світу, оскільки незаконно викрадені фінансові ресурси є важливим джерелом надприбутків, які спрямовуються на розвиток ядерної програми та виробництва балістичних міжконтинентальних ракет.

Відповідно до звіту ООН «Про санкції проти Північної Кореї» у 2019 році[3], КНДР отримала 2 млрд доларів США завдяки кіберзлочинності та успішних кібератак. У 2021 році було викрадено лише криптовалюти на загальну суму 400 млн доларів США. Під час проведення кібератак використовувалися фішингові приманки, кодові експлойти, зловмисне програмне забезпечення, передова соціальна інженерія для перекачування коштів із підключених до Інтернету «гарячих» гаманців цих організацій на IP-адреси, контрольовані урядом КНДР. Відповідно до оприлюдненого звіту компанії «Microsoft»[4], у 2023 році хакери з КНДР вкрали від 600 млн до 1 млрд доларів США, які були спрямовані Пхеньяном на фінансування більшої половини своїх ядерних розробок й випробувань. Протягом 2023-2024 років було викрито чимало нових північнокорейських хакерських угрупувань, ціллю яких були саме криптовалютні біржі. Такі угрупування використовували власні розробки, зокрема програми-вимагачі, які були спрямовані проти підприємств та організацій у аерокосмічному й оборонному секторах США та країн Європи задля збору розвідданих і отримання фінансової вигоди. Викрадені криптовалютні активи проходять ретельний процес відмивання, щоб якомога скоріше бути переведеними в готівку. Тобто кібератаки, особливо на криптовалютні активи, залишаються важливим джерелом прибутків і доходів північнокорейського уряду в умовах потужного міжнародного санкційного тиску та економічної ізоляції КНДР. Це переконливо засвідчує прагнення північнокорейського політичного керівництва завдяки кіберзлочинцям посилити свої фінансові можливості та здійснювати просування власних стратегічних інтересів[5]. 31 липня 2024 року Національна розвідувальна служба Південної Кореї оприлюднила звітні матеріали щодо оцінки кібернетичного потенціалу КНДР[6]. Кількісна чисельність структур КНДР, пов’язаних із кібероперaціями та

[3] UN Panel of Experts DPRK 2019 Final Report. URL: https://www.ncnk.org/resources/publications/un_poe_march2019_final_report.pdf/file_view

[4] Північнокорейські хакери викрали $3 мільярди криптовалюти для ядерної програми Пхеньяна, – звіт Microsoft. URL: https://ms.detector.media/kiberbezpeka/post/36471/2024-10-17-pivnichnokoreyski-khakery-vykraly-3-milyardy-kryptovalyuty-dlya-yadernoi-programy-pkhenyana-zvit-microsoft

[5] [단독]“北에 해커 8400명… 러와 악성코드 공동 개발”. URL: https://www.donga.com/news/Politics/article/all/20240731/126221495/2

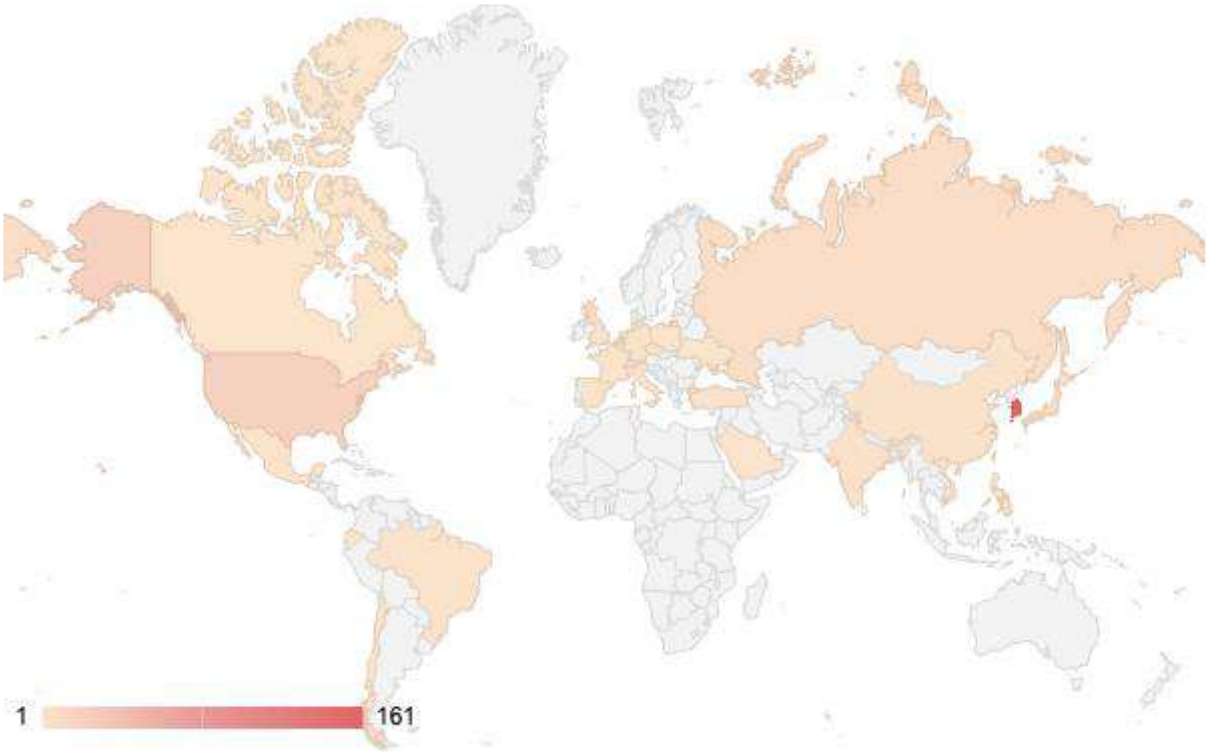
[6] North Korean Cyber-Attacks Cost South Korea $1.2 billion. URL: https://thecyberexpress.com/north-korean-cyber-attacks-cost-south-korea

хакерською діяльністю, складає 8 400 осіб та має стрімку динамічну тенденцію до збільшення.

Геополітична кібернетична стратегія КНДР базується на постулатах, важливими завданнями якої є збір, обробка та узагальнення здобутої аналітичної й статистичної інформації, викрадення державних секретів у ворожих до режиму Кім Чен Ина державах, викрадення значних фінансових ресурсів, проведення підривних та руйнівних кібератак, операцій у кіберпросторі. З цією метою кібератаки КНДР здебільшого проводяться проти Південної Кореї, у меншій кількості – проти державних органів та структур, розташованих на території США (рис. 1)[7].

Рис. 1

Держави-жертви кібератак КНДР
(найбільша кількість постраждалих у Південній Кореї – 161 фізична та юридична особа)



Починаючи з 2013 року, Південна Корея неодноразово звинувачувала КНДР в потужних кібератаках, які призводили до блокування комп'ютерних систем, банківських установ на тижні, водночас такі кібератаки з різною інтенсивністю тривають на перманентній основі. У фокусі уваги кібервійськ КНДР перебувають криптовалютні біржі, які також є мішенню північнокорейських кібератак. Північна Корея час від часу здійснює руйнівні кібератаки, особливо в період загострення геополітичної напруженості, оскільки для північнокорейських кібервійськ становлять чималий інтерес такі галузі, як:

[7] North Korea's Cyber Strategy. URL: https://go.recordedfuture.com/hubfs/reports/cta-nk-2023-0622.pdf

аерокосмічна та військово-оборонна промисловості, фінансовий і банківський сектор, діяльність неурядових організацій-донорів тощо.

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 підтверджує уряд Південної Кореї, а також світові гіганти-розробники технологій ШІ, такі як OpenAI та компанія Microsoft, які регулярно фіксують спроби проведення 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. Водночас вони вибудовують тривалі стосунки з потенційною жертвою аж до кількох місяців, перш ніж відправити фішингове посилання. Крім стандартних функцій, військові та хакери КНДР використовують штучний інтелект для створення ефективніших вірусів і програм-вимагачів. Через недоступність західних застосунків вони користуються виключно китайськими розробками, але також самі вивчають й опановують цей напрямок. Інші країни-партнери КНДР, такі як КНР, Іран та Росія, з недавнього часу також почали застосовувати ШІ для проведення кібератак, що передбачає обмін сучасними технологіями між ними. Таким чином, КНДР отримує прибуток від злому фінансових установ, крадіжки віртуальних активів і поширення програм-вимагачів[8]. Також Північна Корея постійно створює та використовує власне шкідливе програмне забезпечення на основі Stuxnet – хакерської атаки, яку багато хто приписує США та Ізраїлю, яка вразила іранські ядерні центрифуги до того, як її виявили ще у 2010 році.

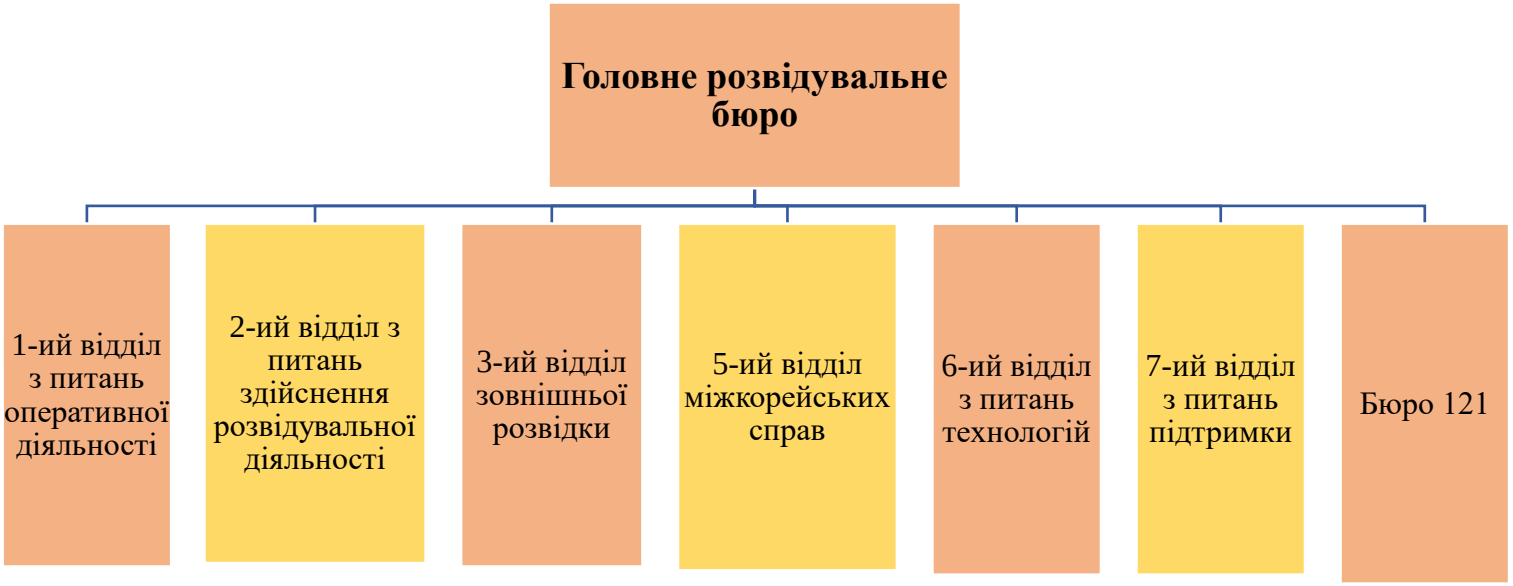
Інституційно кібервійська КНДР почали створюватися ще при Кім Чен Ірі, який вважав, що програмування та розвиток високих технологій має значно покращити економічне становище держави та сприяти розвитку і прогресу. Основи північнокорейських кібероперацій були закладені ще в 1990-х роках, після того, як північнокорейські фахівці-комп'ютерники повернулися із закордонної подорожі, запропонувавши використовувати Інтернет як засіб для шпигування за іноземними державами, у першу чергу США та Південною Кореєю. Згодом студентів відправляли до Китаю, для участі в найкращих програмах з інформатики. З метою підготовки кадрів Головне розвідувальне бюро КНДР (далі – Головне розвідувальне бюро), діючи під прямим керівництвом Кім Чен Ина заснувало «університет хакерів». Пом'якшивши сувору соціальну ієрархію, Північна Корея відкрила можливості для молоді усіх верств населення приєднатися до програми, створивши сучасну групу потенційних новобранців-хакерів. В КНДР соціальний статус, зокрема місце проживання та різновид занять, зазвичай суворо визначаються на основі кровної

[8]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

лінії, але винятки передбачені для осіб, які приєднаються до програми навчання хакерів. Саме такі вчинки з боку військово-політичного керівництва КНДР надали можливість організувати пошук молодих талантів у математиці та комп'ютерних науках, щоб згодом зробити їх кіберзлочинцями. Потенційних кібервійськових відбирають серед підлітків віком 14-15 років або навіть молодше, яких спочатку навчають у школі Кумсон, а згодом вони вступають до Університету Кім Ір Сена або Технологічного університету імені Кім Чаека для здобуття подальшої освіти. Для викладання комп'ютерних і технічних дисциплін, теорії та основ інформатики КНДР активно залучає викладачів російської загальновійськової академії збройних сил. Після закінчення навчання випускники отримують призначення до відповідних підрозділів Головного розвідувального бюро з метою подальшої служби у якості хакерів.

Ще у 2009 році уряд КНДР об'єднав 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 Іра, який, у свою чергу, стояв у витоків створення кіберпідрозділу «Бюро 121» у складі новоствореного на базі Управління Генерального штабу Головного розвідувального бюро. Таким чином, саме Головне розвідувальне бюро вважається основним органом розвідки та таємних операцій Північної Кореї. Нижче наведено структуру цього органу (рис. 2)[9].

Рис. 2



Основою кібервійськ КНДР є елітний спецпідрозділ «Бюро 121», що створений для боротьби з кібератаками та опікується проведенням спеціальних інформаційних операцій із загальною штатною чисельністю 3 000 осіб, укомплектованого найкращими фахівцями. Стратегічним завданням спецпідрозділу «Бюро 121» визначено проведення наступальних дій у

[9] North Korean Cyber Activity. URL: https://www.hhs.gov/sites/default/files/dprk-cyber-espionage.pdf

кіберпросторі, розробка власних зразків кіберзброї, проведення акцій кібершпигунства. Переважна більшість хакерських підрозділів Північної Кореї проводить свої кібероперації за межами країни. Спецпідрозділ «Бюро 121» (далі – Бюро 121) є причетним до хакерських операцій, що фінансуються КНДР, і використовуються урядом Пхеньяна для шпигування або диверсій проти своїх ворогів. Бюро 121 вважається одним із найбільш навчених і добре забезпечених ресурсами кіберпідрозділів у світі, має завдання виконувати наступальні кібероперації, такі як фінансові крадіжки, корпоративне шпигунство та саботаж критичної інфраструктури. Таким чином, функціональна діяльність Бюро 121 включає спектр від фінансових крадіжок до військового кібершпигунства. У фокусі уваги перебувають міжнародні фінансові системи, включно з криптовалютними біржами. Саме цей підрозділ відіграє вирішальну роль у створенні доходів для режиму Північної Кореї, враховуючи, що міжнародні санкції заблокували доступ країни до традиційних фінансових систем. Кібероперації Бюро 121 є ключовими для стратегії виживання Північної Кореї, забезпечуючи постійний потік коштів для військових і ядерних програм режиму. Бюро 121 використовує зразки власної кіберзброї, що забезпечує Пхеньяну єдину асиметричну стратегію, спрямовану на військовий тиск, у першу чергу, на США. Крім того, КНДР може ефективно протистояти суворим економічним санкціям за допомогою кібероперацій, збираючи сотні мільйонів доларів США на підтримку режиму Кім Чен Ина та його ядерної і балістичної ракетної програм.

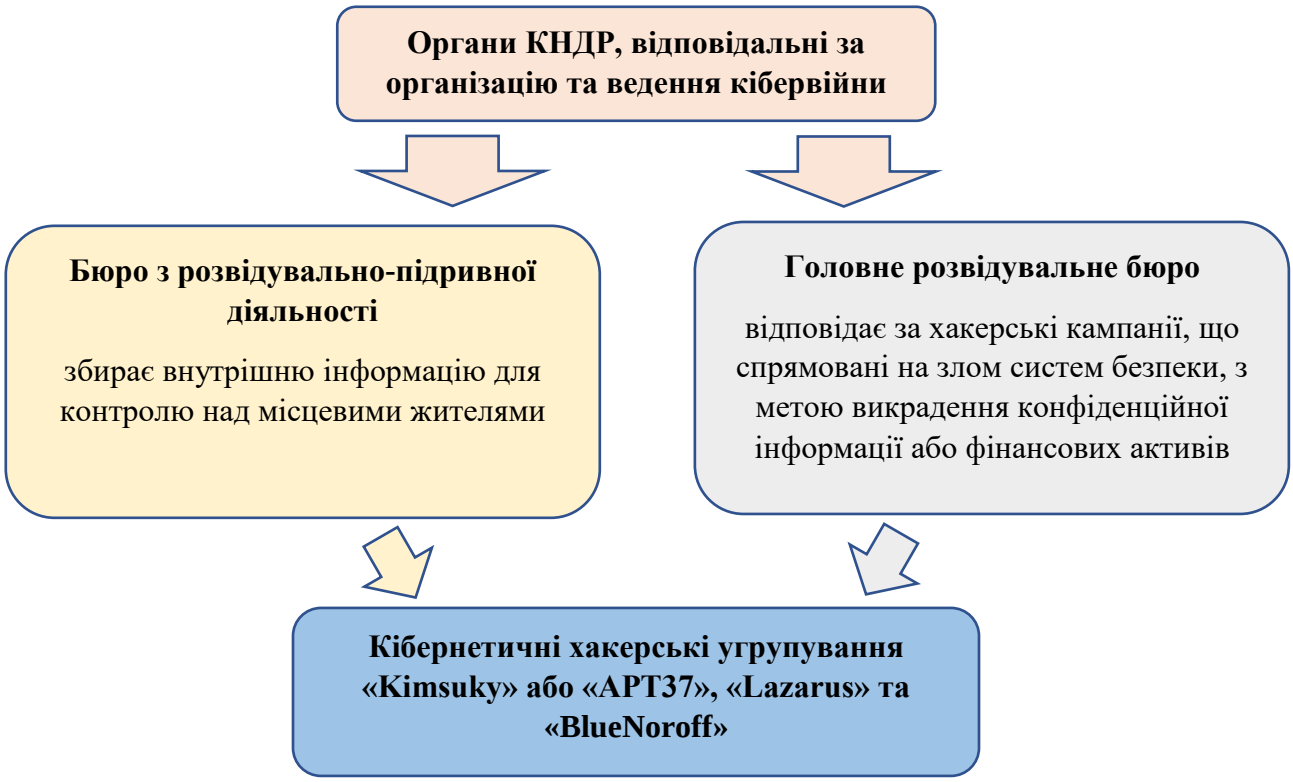
У 2013 році Головне розвідувальне бюро утворило таємний підрозділ під кодовою назвою «№ 180» (далі – підрозділ 180), якому було доручено проводити спецоперації з метою зламу міжнародних фінансових установ задля викрадення валюти на підтримку ядерної програми і програм підготовки балістичних ракет. У рамках реалізації злочинного задуму шкідливі бекдори мали бути встановлені у комп'ютерних системах зарубіжних компаній, які спеціалізуються на розробках програмного забезпечення в США, Японії та Китаї. Також підрозділ 180 активно займається проведенням наступальних кібератак, включно з крадіжками грошей з іноземних банків, у зв'язку з цим для вчинення відповідних злочинних діянь хакери під прикриттям виїжджають за кордон, оскільки за межами КНДР значно краща швидкість Інтернету та вони мають агентурно-оперативні сприятливі можливості здійснювати протиправну діяльність в інтересах військово-політичного керівництва КНДР. Переважна більшість хакерів працює під прикриттям у спільних підприємствах, організованих між КНДР та КНР, іншими державами Південно-Східної Азії (Японія, Тайланд, Філіппіни, Камбоджа, М'янма, Лаос). У фокусі уваги хакерів переважно перебувають банки та фінансові установи, криптобіржі. Згодом підрозділ 180 у сфері своєї злочинної діяльності перемістився в бік криптовалютних бірж, тоді як Бюро 121 розширило свої кібероперації за

межами Південної Кореї, атакуючи іноземну інфраструктуру на інших континентах.

У 2014 році лідер КНДР Кім Чен Ин анонсував, що кібервійна разом з ядерною зброєю та ракетами є «універсальним мечем», який гарантує військовим ударні можливості. Враховуючи триваючу політичну та соціально-економічну ізоляцію, військові Північної Кореї перемістили свою увагу на форми асиметричних заходів впливу, досліджуючи будь-яку вразливість альянсу США і Південної Кореї, щоб протистояти їх якісно вищим технологічним перевагам. На додаток до ядерної та балістичної ракетної програми, КНДР розвиває пов'язані з кібернетичними засобами наступальні військові можливості[10].

Корейська народна армія (КНА) відіграє важливу роль у підтримці та нагляді за діяльністю КНДР у кібервійні. Управління Генерального штабу КНА відповідає за координацію всіх військових операцій, включно з тими, що пов'язані з веденням кібервійни. Того ж року в КНДР було створено ще один бойовий підрозділ – «Unit 91» (далі – підрозділ 91), який займається розробками у сфері передових технологій, необхідних саме для ядерних розробок і ракет великої дальності, керує плануванням і виконанням кібероперацій, спрямованих як на військові, так і на цивільні цілі. Підрозділ 91 забезпечує повну інтеграцію кіберпотенціалу Північної Кореї в її більш широку військову стратегію, що дозволяє режиму використовувати кібертактику як доповнення до своїх звичайних військових сил. Підрозділ 91 контролює спеціалізовані кіберпідрозділи, зокрема підрозділ 180.

Рис. 3



[10] Office 91. Unit 110 + Bureau 121. URL: https://www.globalsecurity.org/intell/world/dprk/rgb-cyber.htm#google_vignette

Окрім Бюро 121, підрозділів 180 та 91, які структурно входять до складу Головного розвідувального бюро, на службі уряду перебувають вмотивовані хакери, які об'єдналися в різні угрупування з метою виконання поставлених перед ними завдань. У цьому контексті існують три потужних кібернетичних хакерських угрупувань під кодовими назвами «Kimsuky» або «APT37» (Advanced Persistent Threat), «Lazarus» та «BlueNoroff».

«Kimsuky» або «APT37» є північнокорейською хакерською командою, що була створена у 2012 році і здобула славу успішних кібершпіонів. «APT37» 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» здебільшого здійснюють кібершпигунство проти установ та організацій, що мають локацію у Південно-Східній Азії, зосереджуючись, у першу чергу, на Південній Кореї, а також час від часу здійснюючи кібератаки на США. Починаючи з 2017 року, хакери «APT37» розширили спектр своїх кібератак у глобальних вимірах, постійно вдосконалюючи тактику кібератак та поєднуючи їх із використанням соціальної інженерії. У 2020 році хакери «APT37» вчинили атаку на військові підприємства України, Туреччини та Словаччини шляхом створення підробленої сторінки авторизації в поштовому сервісі Outlook. У 2020 році намагалися отримати доступ до російських військових об'єктів, проводили фішингові розсилки з метою викрадення конфіденційної інформації щодо аерокосмічних і оборонних компаній, а у квітні 2020 року атакували російську державну корпорацію «Ростех». У 2023 році хакери «APT37» зламали комп'ютерні мережі потужного російського розробника ракет «НВО машинобудування», що є лідером у сфері розробки 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 зчитувати дані[11] (рис. 4).

[11] 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/

Рис. 4[12].

На переконання міжнародних експертів, – це є свідченням того, що ізольована від цивілізованого світу країна націлюється навіть на своїх союзників, прагнучи отримати доступ до документальних розробок критично важливих передових технологій, які цікавлять КНДР. Такий жвавий інтерес виник відразу після початку розробки північнокорейської міжконтинентальної балістичної програми з метою створення ракет, здатних завдати удару по материковій частині США. Наприкінці вересня 2024 року хакери «APT37» здійснили кібератаку на німецьку оборонну компанію Diehl Defense[13], 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 фішинг.

Тривалий час діяльність «APT37» була націлена на військово-оборонний сектор Південної Кореї, зосереджуючись на військових підрядниках, ядерних об'єктах і урядових мережах. Ці операції спрямовані на створення довгострокових можливостей для кібердиверсій, що мало дозволити Північній Кореї вивести з ладу критичну інфраструктуру або скомпрометувати військові системи у разі настання конфлікту. Встановлюючи бекдори в ключових мережах, північнокорейські кіберпідрозділи мають на меті порушити можливості супротивника під час підвищеної напруги або військової ескалації.

У свою чергу, хакерське угрупування «Lazarus» та його підгрупи залучаються до операцій більш широкого спектру, які є різноманітними за масштабом і глобальні за характером. Ймовірно, це пов'язано з комплексним розмежуванням сфер відповідальності структурних підрозділів Головного розвідувального бюро щодо відповідних хакерських угрупувань: діяльність «APT37» пов'язана та контролюється 5-м відділом Головного розвідувального бюро, що відповідає за міжкорейські справи, а «Lazarus» – 3-м відділом Головного розвідувального бюро, відповідального за збір зовнішньої розвідувальної інформації. Загалом «Lazarus» є таємною кіберзлочинною групою під егідою уряду КНДР, яка спеціалізується на викраденні фінансів та криптовалют, на постійній основі проводить кібероперації з метою організації крадіжок великих сум грошей по всьому світу. У 2014 році це хакерське угрупування атакувало голівудську студію «Sony», а у 2016 році викрали 81 млн доларів США з Центробанку

[12] 5 Google Dorking Tricks Hackers Don't Want You to Know — Uncover Hidden Vulnerabilities Instantly! URL: https://medium.com/h7w/5-google-dorking-tricks-hackers-dont-want-you-to-know-uncover-hidden-vulnerabilities-instantly-a3fcd4098c16

[13] Північнокорейські хакери атакували німецького виробника IRIS-T. URL: https://nv.ua/ukr/world/countries/hakeri-z-kndr-atakuvali-nimeckogo-virobnika-iris-t-50454322.html

Бангладеш. За вказаними фактами атак у США були порушені кримінальні справи, проте жодного обвинувачення не було висунуто.

У лютому 2024 року хакерське угрупування «Lazarus» розробило нову схему з метою крадіжки даних користувачів і цифрових активів. Експерти виявили, що хакери створили підставну NFT-гру, яка автоматично зламувала браузер «Google Chrome» і викрадала дані. Шкідливе програмне забезпечення виконувало роль розвідника, надаючи змогу виявити відповідні для атаки цілі. Замість розважального контенту користувач отримував на свій ПК шкідливий бекдор «Manuscrypt», який проводив атаку нульового дня на браузер «Google Chrome». За його допомогою хакери отримували доступ до файлів cookie, маркерів аутентифікації, збережених паролів та історії відвідувань. Таким чином, «Lazarus» використовувало свої розробки для проведення розвідки та збору інформації про потенційні цілі. Водночас найбільший інтерес становила інформація про власників криптоактивів. Усі зібрані дані пересилалися на сервер хакерів, а в програмне забезпечення жертви вносили зміни аж до налаштування BIOS. 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 62,5 млн доларів США. «Lazarus», яке тісно пов’язане з урядом КНДР, використовує месенджер «Телеграм» для крадіжки криптовалюти (завдяки можливостям цього месенджеру розповсюджується шкідливе програмне забезпечення для фальшивих криптовалютних гаманців). Непоодинокі випадки інфікування здійснюється через завантажений із «Телеграма» софт, який викрадає конфіденційну інформацію.

У 2019 році хакери «Lazarus» викрали 10 млн доларів США з чилійського банку. У серпні 2020 року США анонсували спільне попередження щодо наслідків кіберкрадіжок північнокорейськими хакерами з прицілом на банківські рахунки і банкомати по всьому світу. Оскільки США стурбовані сучасними схемами відмивання грошей північнокорейськими хакерами, пов’язаних з криптоактивами, Міністерство юстиції США ініціювало конфіскацію 280 криптовалютних рахунків осіб, підозрюваних у зв’язках із північнокорейськими хакерами, які викрадали цифрові валюти. 2 вересня 2020 року Всесвітнє товариство міжбанківських фінансових телекомунікацій (SWIFT) офіційно повідомило, що Північна Корея розпочала відмивати гроші за допомогою криптовалют. Протягом 5 років, у період з 2020 по 2024 роки, хакери «Lazarus» сумарно вкрали фінансових активів на загальну суму 2,4 млрд доларів США. Понад 70% коштів, які опинилися у розпорядженні хакерів, було видобуто за допомогою компроментації приватних ключів постраждалих компаній та приватних осіб. Цей метод надав змогу хакерам вкрасти 1,7 млрд доларів США. У 2023 році «Lazarus» отримало понад 1 млрд доларів США прибутку за наслідками своєї протиправної діяльності. Північнокорейські хакери досить часто використовують фішинг у поєднанні

з методами соціальної інженерії. У комбінації з технічними даними комп'ютерної системи компанії, а також присутніми вразливостями, вони знаходять можливість скомпрометувати потрібні їм приватні ключі. Хакерське угруповання «Lazarus» стоїть за безліччю кампаній, серед яких кібершпигунство, атаки шифрувальників і посягання на 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». Північнокорейська хакерська група «BlueNoroff» 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 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 для встановлення довіри і шахрайських пропозицій щодо роботи на централізованих біржах та децентралізованих фінансових платформах (DeFi), щоб ввести в оману співробітників перейти за шкідливими посиланнями, замаскованими під тести або заявки на працевлаштування. Проникнувши в систему компанії, шкідливе програмне забезпечення спустошує всі доступні криптовалютні гаманці, що призводить до значних фінансових втрат. Північнокорейські зловмисники виявляють пов'язані з криптовалютою підприємства, щоб націлитися на них і намагаються спровокувати десятки співробітників цих компаній, щоб отримати несанкціонований доступ до мережі компанії. 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 людей розкрити конфіденційну інформацію. «BlueNorOff» також був пов'язаний з операціями з криптозлому, коли вони використовували комп'ютерні ресурси жертв для видобутку криптовалюти.

Таким чином, хакерські угрупування «APT37», «Lazarus» та «BlueNorOff» працюють в інтересах уряду Північної Кореї, який стимулює та спонсорує хакерські атаки з метою спрямовування зусиль проти державних структур і компаній демократичних держав, отримання розвідувальних даних та фінансових активів для своїх військових і ядерних програм. Північнокорейські хакерські групи, такі як «BlueNorOff», регулярно атакують бізнес, пов'язаний з криптовалютою, намагаючись викрасти кошти або максимально поширити бекдор-шкідливе програмне забезпечення. Північнокорейські хакери продемонстрували, що вони можуть швидко адаптуватися, використовуючи більш оманливі методи отримання доступу до будь-яких цифрових активів.

Хакери також використовують різновиди програм-вимагачів, щоб вивести з ладу комп'ютери в певному секторі, а потім вимагати від жертв плату за зупинення атаки. Доходи, одержані від атак програм-вимагачів, зловмисники використовують для розширення власної інтернет-інфраструктури, яку потім використовують для здійснення кібершпигунства. Глобальні індустрії безпеки попереджають провідні країни світу вживати додаткових заходів безпеки, оскільки Північна Корея використовує більш складні та добре сплановані методи злому операційних та інформаційно-комунікаційних систем. Головне розвідувальне бюро разом з Департаментом державної безпеки, Міністерством державної безпеки координують діяльність хакерських північнокорейських груп, зокрема «Lazarus», «Bluenoroff», «APT37». Ці спеціалізовані групи зосереджені на фінансових крадіжках, шпигунстві та стратегічних диверсіях, діють згідно з державними директивами, переслідуючи ширші геополітичні цілі. Департамент державної безпеки відповідає за підтримку внутрішньої безпеки і забезпечення лояльності північнокорейських хакерів, дислокованих за кордоном, відіграє вирішальну роль у кібероперації Північної Кореї, здійснюючи нагляд за діяльністю у сфері кібершпигунства та сприяючи хакерам, які залучені до іноземних місій.

Департамент державної безпеки тісно співпрацює з Бюро 121, обмінюючись оперативними та розвідувальними даними, координуючи кібератаки на фінансові установи та критичну інфраструктуру. Багато хакерів працюють у Китаї, Росії та країнах Південно-Східної Азії, де вони видають себе за ІТ-фахівців або бізнес-консультантів. Департамент державної безпеки уважно стежить за хакерами, часто використовуючи їхні родини як важіль для забезпечення відповідності та запобігання дезертирству. Ця система контролю та примусу гарантує, що кіберсили Північної Кореї залишатимуться лояльними і зосередженими на виконанні глобальних кіберцілей північнокорейського режиму. Департамент державної безпеки також відіграє важливу роль у внутрішніх кібероперація Північної Кореї, включаючи збір даних політичної розвідки і стеження за потенційними внутрішніми загрозами. Відстежуючи цифрові комунікації громадян Північної Кореї, він може ідентифікувати дисидентів і забезпечити швидку нейтралізацію будь-якої потенційної опозиції режиму. Ця внутрішня мережа стеження є критично важливим інструментом для підтримки контролю режиму над населенням, гарантуючи, що кіберпотенціал Північної Кореї не лише зосереджений назовні, але й служить для зміцнення внутрішньої стабільності.

Департамент військово-цивільних зв'язків Центрального комітету відповідає за управління логістикою та фінансування кібероперацій Північної Кореї, координує розподіл ресурсів, інфраструктуру та фінансову підтримку для ключових кіберпідрозділів, таких як Бюро 121 і підрозділ 180. Департамент військово-цивільного зв'язку відіграє життєво важливу роль у забезпеченні достатніх ресурсів для кіберпідрозділів Північної Кореї. Цей департамент також керує закордонними кібероперація КНДР, координуючи дії між

кібероператорами та посольствами Північної Кореї за кордоном. Посольства в таких країнах, як Китай, Росія та Малайзія, служать центрами кібероперацій, надаючи матеріально-технічну підтримку і прикриваючи кібератаки. Персонал посольства часто залучається до координації кібероперацій і сприяє відмиванню коштів, викрадених через кіберзлочинність. Участь дипломатичних представництв Північної Кореї в кіберопераціях підкреслює ступінь інтеграції кібервійни в дипломатичну стратегію режиму, який використовує дипломатичні привілеї, щоб уникнути виявлення та кримінального і судового переслідування.

У 2016 році Генеральний штаб КНДР створив новий відділ командування, управління, зв'язку, комп'ютерів і розвідки (C4I) з метою посилення захисних кіберможливостей командних і контрольних армійських та суміжних систем, впровадження технологій квантового шифрування, намагаючись побудувати високозахищений зв'язок командування та управління між Пхеньяном і ключовими пунктами запуску ракет. Кіберпідрозділи КНДР забезпечують кіберзахист інформаційно-комунікаційних систем, об'єктів критичної військової інфраструктури та поступово розвивають свої ресурсні активи, удосконалюючи арсенали зловмисного програмного забезпечення і можливості кодування на основі здобутого досвіду, покращуючи методологію проведення кібератак, адаптуючи код шкідливого програмного забезпечення таким чином, щоб уникнути будь-якого виявлення. Витонченість кібероперацій свідчить про те, що Пхеньян приділяє дедалі більше уваги економічній і політичній війні за допомогою кібернетичних засобів, а кіберпідрозділи та спонсоровані державою хакерські угрупування мають на меті обходити міжнародні санкції, водночас генеруючи ресурси для поповнення економіки Північної Кореї та фінансуючи за рахунок викрадених коштів військово-технічний розвиток.

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 мереж, значною мірою відключена від глобального Інтернету та обмежена китайським «Великим брандмауером», оскільки увесь інтернет-трафік країни проходить лише через двох провайдерів – китайський «Unicom» і російський «TransTeleCom».

КНДР здійснює незаконні кібероперації з метою спрямування коштів на розробку власної ядерної зброї. За оцінками галузевих спостерігачів, рівень кіберпотужностей Північної Кореї близький до російського та китайського. Однією з найбільш характерних особливостей кібероперацій Північної Кореї є акцент на довгострокове стратегічне планування. 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.

Одночасно існує декілька основних передумов для зростання інтересу Північної Кореї до ведення кібервійни. По-перше, розвиток кібервійськ є важливим стратегічним завданням та вбачається економічно вигідним. Через погіршення економічної ситуації в КНДР вона не може конкурувати з Південною Кореєю чи США у розбудові військових, військово-морських або повітряних сил. На цьому фоні встановлення за сприяння КНР та РФ високошвидкісного Інтернету, закупівля програм і забезпечення умов підготовки фахівців для їх подальшої роботи в Китаї чи іншій третій країні світу значно дешевше, ніж придбання нової зброї чи винищувачів, які коштують сотні мільйонів доларів США. По-друге, Північна Корея надзвичайно впевнена у своїх можливостях розробки власного шкідливого програмного забезпечення, оскільки злам паролів у захищеній системі та пошук патчів у мережах базуються на математичних можливостях та прогнозах. По-третє, кіберпотужність та технології штучного інтелекту забезпечують більшу користь у порівнянні з армійськими можливостями. При цьому, кіберлюдська сила – це потужний карт-бланж, який надає можливості здійснювати викрадення будь-якої секретної інформації з ворожих для КНДР держав, вивести з ладу їхні сервери, викликати соціальну паніку за допомогою успішно реалізованих задумів ведення інформаційно-психологічної війни. По-четверте, кібервійна асиметрично вигідна КНДР, оскільки жоден із серверів не підключений до Інтернету, що робить його захищеним від кібератак. У свою чергу, кібератаки ніколи не здійснюються з КНДР, тому що такі напади можна легко відстежити в кількох комп'ютерних центрах або університетах, які мають вільний доступ до Інтернету в ізольованій країні. Для КНДР хакерство є інструментом, який дозволяє злочинному режиму досягти кінцевої мети: завершити підготовку до остаточного сценарію кібервійни. У межах КНДР Інтернет створено не лише для військових, але й для всієї держави, одночасно доступ до мережі Інтернет вважається дуже небезпечним, у зв'язку з чим він є досить обмеженим.

Політика КНДР орієнтована на людський капітал, сучасні технології та систематизацію і поєднання обох цих елементів. Головне розвідувальне бюро відправляє хакерів, які діють під прикриттям, до різних країн світу, видаючи себе за «програмістів», які хочуть дізнатися про розробку нових комерційних програм.

Таким чином, північнокорейські хакерські групи були відправлені до США, Китаю, Росії, а також країн Південно-Східної Азії та Європи, діючи незалежно та взаємно підтримуючи одна одну на основі своїх конкретних кібермісій.

Рис. 5

За стратегічним задумом військово-політичного керівництва КНДР за кордоном працюють понад 600 хакерів, які займаються викраденням передових і 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. Водночас 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 держав відповідного реагування, що передбачає посилення зусиль з припинення актів кібершпигунства на користь КНДР, зокрема шляхом накладення санкцій на окремих осіб або кримінального переслідування.

США розцінюють усі спроби хакерських атак як посягання на основи національної безпеки. У вересні 2018 року Міністерство юстиції США висунуло північнокорейському програмісту Пак Чжин Хьоку звинувачення у змові з метою вторгнення в комп'ютерні системи та шахрайстві. У вересні 2019 року Міністерство фінансів США запровадило санкції проти північнокорейських хакерських груп, підпорядкованих Головному розвідувальному бюро[14]. «Hidden Cobra» – загальний термін, яким США позначають зловмисну кіберактивність уряду Північної Кореї та її хакерських угрупувань.

З метою оптимізації усіх північнокорейських 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. Північна Корея змінила свої методи злочинної діяльності і все частіше покладається на хакерські угрупування для кібершпигунства та поширення дезінформації. Оскільки міжнародні санкції руйнують економіку Північної Кореї, кіберзлочинність і хакерство стали критичними та доступними джерелами надприбутків. Хакерські угрупування пов'язані з Головним розвідувальним бюро і відомі своїми зухвалими кібератаками від криптовалютних бірж до державних установ інших країн. КНДР генерує до 50% своїх валютних надходжень завдяки протиправній кібердіяльності. Доходи від кібератак спрямовуються безпосередньо в ядерну та ракетну програми північнокорейського провладного режиму. КНДР на постійній основі проводить навчання хакерів, оскільки вони виявилися економічно досить ефективними. Іноземні гроші, незаконно зароблені північнокорейськими хакерами, є основним джерелом фінансування північнокорейського режиму, який підпадає під різні санкції. В сучасних умовах США і Південна Корея не змогли остаточно знищити ВПК КНДР. Тому ця країна активно розвиває у тому числі й власний кіберпотенціал у поєднанні з ядерними та балістичними ракетними програмами як асиметричну відповідь, що забезпечує відносно недорогий, але досить ефективний спосіб, надаючи Пхеньяну можливість демонструвати військову міць та здійснювати залякування без збройного конфлікту в контексті масштабного світового протистояння.

Висновки. Кібервійська КНДР комплектуються спецпідрозділом «Бюро 121», підрозділами 91 та 180, які структурно входять до складу Головного

[14] U.S. imposes sanctions on North Korean hacking groups blamed for global attacks. URL: https://ipdefenseforum.com/2019/10/u-s-imposes-sanctions-on-north-korean-hacking-groups-blamed-for-global-attacks

розвідувального бюро. Загальна чисельність кібервійська дорівнює 8 400 осіб. Водночас кібернетичний потенціал КНДР розширюється із небезпечною швидкістю, створюючи серйозну загрозу глобальній безпеці. Хакерські угрупування «APT37», «Lazarus» та «BlueNorOff» виконують завдання в інтересах уряду КНДР, завдяки яким ця країна незаконно здобуває та масштабує криптовалюту, викрадає важливу конфіденційну і безпекову інформацію. Такі хакерські угрупування здійснюють масштабні фінансові крадіжки, націлюючись на біржі криптовалют, платформи децентралізованого фінансування (DeFi) і традиційні банківські системи. Ці операції приносять режиму мільярди доларів США, допомагаючи фінансувати ядерну зброю та програми розробки балістичних ракет Північної Кореї. Одночасно за кордоном працюють понад 600 хакерів, які займаються викраденням високих технологій, кібершахрайством, фішингом, здійснюють несанкціонований доступ до державної та комерційної таємниці, криптовалюти. Провладний режим КНДР застосовує кібервійська та вмотивованих хакерів, поєднує використання складної тактики для крадіжки криптовалютних активів, проводить цілеспрямовані кібератаки, здійснює спроби працевлаштувати на умовах дистанційної роботи хакерів під прикриттям за кордоном, використовує методики приховування шкідливого коду в репозиторіях, які застосовуються розробниками програмного забезпечення тощо. Пхеньян ефективно протистоїть запровадженим економічним санкціям за допомогою саме кібероперацій, збираючи сотні мільйонів доларів США на підтримку режиму Кім Чен Ина та його ядерної і балістичної ракетної програм.

Окрім фінансових крадіжок, північнокорейські кіберпідрозділи займаються майнінгом криптовалют в країнах із слабким регуляторним наглядом, генеруючи цифрові валюти, які використовуються для фінансування кібероперацій або конвертуються у тверду валюту. Північнокорейські хакери також були пов’язані з маніпулятивними практиками на ринках DeFi, створюючи штучні коливання цін, щоб отримати прибуток від ринкових коливань. Ці дії підкреслюють важливість кіберзлочинності в економічній стратегії Північної Кореї, дозволяючи режиму обходити санкції та підтримувати свої військові амбіції.

Кібероперації Північної Кореї є спонсорованими державою зусиллями, які відображають залежність режиму від кібервійни як критичного інструменту для виживання, економічної вигоди та геополітичного впливу. Цими операціями керують Головне розвідувальне бюро, Департамент державної безпеки, Департамент військово-цивільних зв’язків Центрального комітету, які організовують напади, починаючи від фінансових крадіжок і закінчуючи стратегічними кібердиверсіями. Інтеграція кіберскладової у військові та розвідувальні структури Північної Кореї підкреслює визнання провладним режимом Кім Чен Ина важливості кіберможливостей у сучасному світовому протистоянні. Оскільки КНДР продовжує стикатися з міжнародними економічними санкціями та дипломатичною ізоляцією, цілком ймовірно, що її

залежність від кібероперацій лише динамічно зростатиме. За таких умов міжнародне співтовариство має розробити ефективні проактивні заходи протидії північнокорейським хакерським кібератакам, які є серйозною загрозою та сучасним викликом для глобального кіберпростору, що ставлять за мету збагачення та отримання військової переваги над іншими державами.

У контексті викладеного актуалізується питання створення спеціальних підрозділів кібервійськ в Україні, що є важливим і рішучим кроком, спрямованим на запровадження дієвих та ефективних механізмів стримування і відсічі російській та північнокорейській агресії у кібердомені, особливо в умовах триваючої кібервійни. Доцільним є законодавче забезпечення інституційного створення кібервійськ в Україні, прискорення схвалення проекту закону України «Про Кіберсили Збройних Сил України»[15], що визначає організаційно-правовий статус та засади діяльності кібервійськ, на які покладається кібероборона України, захист її суверенітету та територіальної цілісності в кіберпросторі. Цілком логічно, що створення кібервійськ як окремого роду сил надасть змогу значно посилити спроможності українського війська в умовах кібервійн, забезпечити ефективне планування та реалізацію повного спектру завдань у кіберпросторі, що на рівні із суходолом, морем, повітрям та космосом визнаний окремим операційним доменом.

Принагідно слід зазначити, що Дослідницькою службою підготовлено аналітичну записку з питань порівняльного законодавства щодо нормативного забезпечення, особливостей створення та інституційного становлення кібервійськ (кіберсил) країн-членів НАТО, з текстом якої можна ознайомитися на вебсайті Дослідницької служби[16].

Дослідницька служба
Верховної Ради України

**Цей документ підготовлений Дослідницькою службою Верховної Ради України як довідковий інформаційно-аналітичний матеріал. Інформація та позиції, викладені в документі, не є офіційною позицією Верховної Ради України, її органів або посадових осіб. Цей документ може бути цитований, відтворений та перекладений для некомерційних цілей за умови відповідного посилання на джерело.*

[15] Про Кіберсили Збройних Сил України: проект закону № 12349 від 19.12.2024 року. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/45453

[16] Аналітична записка з питань порівняльного законодавства щодо інституційного створення кібервійськ (кіберсил) в країнах НАТО. URL: https://research.rada.gov.ua/documents/analyticRSmaterialsDocs/nscur_defense/analytical_notes-nb/74097.html