УДК 354.42

Олександр Миколайович Косогов *(канд. військ. наук, с.н.с.)*
Анатолій Олександрович Сірик

Військова частина А1906

СУЧАСНА ПОЛІТИКА БЕЗПЕКИ КІБЕРПРОСТОРУ В УМОВАХ ЙОГО МІЛІТАРИЗАЦІЇ

Проаналізовано заходи із забезпечення кібербезпеки провідних держав світу, виділені основні тенденції трансформації внутрішньої політики держав з огляду на активізацію кіберзагроз у світі. Запропоновано шляхи поліпшення кібербезпекової політики України з метою приведення її до вимог сучасності та забезпечення суверенітету держави в умовах мілітаризації кіберпростору.

Ключові слова: *кібербезпека; кіберпростір; кіберзагрози.*

Вступ

Постановка проблеми. Інформаційний розвиток суспільства не лише дає змогу будувати успішне суспільство, й дає нові імпульси традиційним загрозам безпеки держави, створюючи таким чином принципово нові проблеми для системи національної безпеки.

У таких умовах особливого значення набуває пошук нових можливостей для забезпечення безпеки держави з огляду на формування нового поля протиборства – кіберпростору. Сьогодні проблеми кіберпростору, через певну новизну, ще не повністю нормативно врегульовані на міжнародному рівні, тому спецоперації, що здійснюються військовими чи спеціальними підрозділами, не підпадають під визначення "акт війни" і можуть кваліфікуватися як операції "відмінні від війни". Фактично, йдеться про можливість забезпечити ефект військового втручання без подальших офіційних санкцій як з боку держави, що зазнала нападу, так і світової спільноти. З огляду на активізацію упровадження інформаційно-комунікаційних технологій (ІКТ) у всі критично важливі сфери життєдіяльності людини та держави, протистояння у кіберпросторі шляхом проведення кібернетичних атак (ударів) виходить на більш високий рівень міждержавних відносин. Крім того, це призводить до трансформації державної політики більшості провідних держав у питанні контролю за власним кіберпростором та посиленні яскраво виражених обмежувальних тенденцій.

Україна потребує створення надійної системи безпеки у світі, що трансформується, де виклики національній безпеці все частіше набувають рис, відмінних від традиційних загроз. Активність з боку провідних держав світу у кіберпросторі, глибинні зміни відношення до внутрішньої інформаційної політики та формування потужних транснаціональних кримінальних груп, що спеціалізуються на злочинах у кіберпросторі, – все це зумовлює необхідність вироблення рекомендацій щодо коротко- та довгострокових пріоритетів трансформації вітчизняного безпекового сектору.

Аналіз останніх досліджень і публікацій. У зв'язку з недостатнім розвитком інформатизації в нашій країні проблеми, що безпосередньо пов'язані із функціонуванням інформаційних інформаційно-телекомунікаційних, телекомунікаційних систем, почали досліджувати лише протягом останніх років. Більше того, зважаючи на законодавчу невизначеність основної термінології, зокрема понять "кіберпростір", "кіберзахист", "кібератака", "кібертероризм", "кіберзлочини", наукові дискусії здебільшого точаться навколо саме понятійного апарату цієї проблематики. З іншого боку, аналіз зарубіжного досвіду показав, що вивченням кіберпростору як середовища вчинення злочинів займалися Погорецький М.А. та Шеломенцев В.П. В свою чергу, Климчук О.О. зосереджував увагу на вивчення змісту поняття "кібервійна", а питання захисту інформаційної інфраструктури від кіберзагроз досліджував Довгань О.Д. [2;4].

Мета статті. На основі аналізу заходів із забезпечення кібербезпеки провідних держав світу визначити шляхи поліпшення кібербезпекової політики України в умовах мілітаризації кіберпростору з метою приведення її до вимог сучасності.

Виклад основного матеріалу дослідження

Сьогодні більшість провідних держав світу (США, Росія, ЄС, Китай, Індія та інші) перебувають у процесі трансформації власних військових потенціалів (з огляду на можливості використання мережі Інтернет). За даними компанії McAfee [1], оприлюдненими на Всесвітньому економічному форумі в Давосі, ще в 2010 р., близько 20 країн планували здійснювати або реально здійснювали різноманітні заходи у кіберпросторі протягом 2009–2010 рр. Було сформовано спецпідрозділи, які ставили за мету: ведення розвідки в комп'ютерних мережах, захист власних таких мереж, блокування роботи структур супротивника. Згідно з офіційними заявами, такі підрозділи вже успішно функціонують у США (U.S. Cyber Command), Великобританії (Cyber

Security Operations Centre), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cyber security operations centre), Росії, Індії та інших державах. Активну позицію щодо протидії кіберзагрозам займає і провідна міжнародна безпекова організація НАТО (Cooperative Cyber Defence Centre of Excellence).

Нині найбільш потужними та активними вважаються військові кіберпідрозділи КНР та США.

Даних про потенціал, чисельність чи завдання китайських кібервійськ практично немає. У рамках конференції Black Hat [1] 4 серпня 2010 р. мали бути оприлюднені дані (дослідження компанії Armorize) про реальний потенціал китайських та тайванських кібервійськ, однак на вимогу керівництва Тайваню доповідь виключили з програми. Не містить даних про потенціал кібервійськ Китаю й опублікована у серпні 2010 року доповідь Міністерства оборони США про військову могутність Китаю [5], хоча і висувається припущення, що значна кількість атак на комп'ютерні мережі, що належать уряду США, можуть здійснюватися за підтримки або Народно-визвольної армії Китаю або уряду Китаю.

За даними видання The Daily Beast [6], ФБР підготувало секретний звіт (далі – Звіт), в якому висвітлюється рівень розвитку кібервійськ КНР, а також загрози, які вони несуть США. У Звіті КНР названо "найбільшою цілісною загрозою США у сфері кібертероризму" та силою, що вже нині може володіти потенціалом "знищувати життєво важливу інфраструктуру, отримувати доступ до банківських, комерційних, військових та оборонних баз даних". За даними ФБР, КНР на сьогодні має армію у складі 180 000 хакерів, які займаються здійсненням щоденних атак на кібермережі США. Серед них 30 000 – це військові, а 150 000 – комп'ютерні експерти з приватного сектору, основне завдання, яких є отримання доступу до військових та комерційних секретів США.

Не менш активна політика проводиться США ще з 2009 року у сфері кібербезпеки, зокрема:

оприлюднено "Огляд кібербезпеки" (Cyber Security Review) – комплексний документ, що визначає основні пріоритети нової команди у сфері кібербезпеки;

введено посаду керівника з питань кібербезпеки Ради національної та внутрішньої безпеки;

функціонує Кіберкомандування США (U.S. Cyber Command), приблизна чисельність якого складає 30 000 військових;

здійснено додатковий набір 1000 співробітників до спеціального кібербезпекового департаменту Управління національної безпеки (Department of Homeland Security) США, які займаються виключно безпекою високотехнологічних систем США. Однак навіть 1000 співробітників не забезпечать повною мірою потреби США у фахівцях із кібербезпеки. У супровідному документі до спеціально організованих урядом США змагань "Кіберзмагання США" (U.S. Cyber Challenge) наводиться теза одного з експертів, що реальна потреба уряду в таких фахівцях складає від 10 000 до 30 000;

збільшено держзамовлення на розроблення нових засобів ведення війни, зокрема кіберзброї, та нових більш захищених військових мереж;

створено проекти нормативних документів, спрямованих на вдосконалення взаємодії в сфері кібербезпеки союзниками США та убезпечення власного Інтернет-простору в разі виникнення ситуацій, що загрожують національній безпеці.

Великобританія (потенціал якої у сфері кіберзахисту вважається одним з найпотужніших) все ще розбудовує власні сили безпеки у кіберпросторі. З 2010 року у повноцінному режимі функціонує Оперативний центр з кібербезпеки (20 співробітників) з метою координації вже існуючих різноманітних центрів із кібербезпеки різних відомств та створення майданчика для співпраці між урядом та приватним сектором із проблем кібербезпеки. Крім того, у Великобританії ефективно функціонує Командування урядових комунікацій (Government Communications Headquarters), що забезпечує як захист критично важливої урядової інформації, так і отримання розвідувальних даних за допомогою новітніх комунікативних засобів.

Згідно з відкритими даними, активно створюються та функціонують відповідні підрозділи у Південній та Північній Кореї, Російській Федерації, Франції.

Така увага до забезпечення кібербезпеки та створення засобів ведення боротьби у кіберпросторі змушує уряди багатьох держав переглядати і свою внутрішню політику. Це обумовлено, зокрема, й зростанням кількості випадків використання розвідувальними службами та спеціальними військовими підрозділами можливостей та технічних потужностей транснаціональних кримінальних груп, що спеціалізуються у сфері кіберзлочинності. Це логічним чином спричиняє зміни в політиці провідних держав світу до можливостей обмежувальної та, певною мірою, цензурної політики як однієї із форм ведення внутрішньої інформаційної політики. Все активніше застосовується так званий низькотехнологічний (low-tech) рівень контролю, серед яких бюрократичні, організаційні та обмежувальні методи захисту власного інформаційного та кіберпросторів від латентних загроз безпеці даних, а також впровадження іноземного програмного продукту.

Таким чином, політика держав Заходу в сфері власного кіберпростору все частіше набуває окремих рис політики тих країн, що традиційно належать до авторитарних, хоча і з певними суттєвими відмінностями. Якщо в країнах авторитарного типу спостерігається політика

насамперед безпосереднього обмеження доступу, то країни Заходу йдуть шляхом нарощування кількості даних про користувачів, моніторингу в першу чергу національного Інтернет-трафіку та отримання можливостей цільового відключення окремих елементів мережі Інтернет і її користувачів. Такий акцент на "моніторинговому дискурсі" пояснюється зростанням кількості телекомунікаційних послуг та мереж, контроль за якими значною мірою ускладнено для державних правоохоронних служб. Зокрема, це стосується і контролю за особистими перемовинами власників смартфонів та VoIP – системи [5]. Так, наприклад, смартфони Blackberry підтримують не лише систему шифрування даних, що передаються, але й сервери цих компаній, які знаходяться в США та Великобританії. Більшість правоохоронних органів інших країн вважає – це джерелом небезпеки, оскільки унеможливлює контроль за спілкуванням користувачів Blackberry та потенційно робить доступним зміст листування власників для американських та британських спецслужб. Саме це стало причиною введення обмежень на використання зазначених смартфонів (особливо в державному секторі) в таких країнах, як Франція, Німеччина, Індія, Об'єднані Арабські Емірати та Російська Федерація. Крім того, також мали місце випадки заборони керівництвом ЄС своїм службовцям користуватись смартфонами фірми Blackberry.

Щодо VoIP-телефонії, то основні претензії постають до програмного продукту Skype, оскільки він дає змогу забезпечити ефективний криптографічний захист розмов абонентів, що практично унеможливлює їх перехоплення з боку спецслужб. Це стало однією з причин конфлікту між авторами програмного продукту Skype та спецслужбами деяких країн (Італія, Російська Федерація, Індія, Німеччина, Великобританія). Крім того, уряди США для ФБР виділили додатково 234 млн. доларів для спеціального проекту з прослуховування Інтернет-мереж (Advanced Electronic Surveillance – Going Dark), що спрямований, насамперед, на можливість прослуховування Інтернет-комунікаторів (наприклад, Skype).

Слід зазначити, що такі заходи із більш інтенсивного моніторингу контенту Всесвітньої мережі та окремих технологічних рішень, що забезпечують доступ до неї, пояснюються однією з трьох (або їх сукупністю) причин:

зростанням терористичної загрози, використанням терористами та міжнародними кримінальними структурами новітніх інформаційних технологій та зростанням загрози критичній інфраструктурі держави;

боротьбою з комп'ютерним піратством, протидією порушенню авторських прав на ті чи інші продукти (зокрема, аудіо- та відео-контент) тощо;

протидією розповсюдження дитячої порнографії.

Активніше також застосовуються методи безпосереднього впливу та тиску на власників пошукових Інтернет-сервісів, де або розміщуються матеріали, що викликають невдоволення з боку державних інституцій або ж які надають доступ до таких матеріалів. Лідером у цьому вважається Китай. Найбільш показовим є конфлікт між урядом Китаю та IT-корпорацією Google, який виник через небажання Google обмежувати на вимогу уряду пошукові запити китайських користувачів [6].

Таку ситуацію ілюструє і запущений корпорацією Google сервіс "Transparency Report", що має висвітлювати частоту звернень держави до корпорації із запитами про усунення певного контенту або про надання доступу до персональних даних користувачів сервісів корпорації. З огляду на таке, саме держави Заходу (США та країни ЄС) вважаються лідерами з таких запитів [7]. Не менш активними в цій сфері є і країни БРІКС (крім Росії). Дані про Китай корпорація не розкриває, посилаючись на те, що Китай вважає цензурні вимоги частиною державної таємниці. Таким чином, більшість країн, які традиційно вважаються розвинутими, новими центрами сили, активно використовують авторитарні методи для захисту національного кіберпростору.

Слід зазначити, що нині спостерігаються і активні спроби деяких країн посилити контроль за Інтернет-трафіком громадян та збільшити можливості правоохоронних органів у боротьбі зі шкідливим контентом. Так, у Франції ще з 2010 року урядова агенція HADOPI, що займається охороною авторського права в мережі Інтернет, з метою поліпшення практичного виконання закону про "Три попередження" [8], було внесено пропозицію французьким користувачам на добровільних засадах встановити на свої комп'ютери спеціальне програмне забезпечення, що буде відслідковувати весь їх трафік, шукати встановлене нелегально на комп'ютері програмне забезпечення, надавати відомості правоохоронним органам щодо переглянутого користувачем відео в мережі Інтернет.

На загальноєвропейському рівні відповідно до Директиви ЄС "Щодо охорони прав на інтелектуальну власність" (Directive 2004/48/EC, Intellectual Property Rights Enforcement Directive, IPRED) правоохоронним органам дозволяється збирати особисті дані користувачів, які запідозрені у незаконному файлообміні.

Особлива увага з боку правоохоронних органів приділяється контролю за контентом у соціальних мережах, блогах тощо. З метою контролю за соціальними мережами інвестиційний підрозділ ЦРУ In-Q-Tel вкладає кошти в компанію Visible Technologies, яка займається моніторингом блогів та соціальних мереж. Розробка Visible Technologies дає змогу щоденно піддавати моніторингу більш ніж півмільйона різноманітних сайтів, перевіряючи пости у блогах, а також

коментарі на форумах та сервісах Flickr, YouTube, Twitter та Amazon. За результатами такого моніторингу було закрито блогхостинг Blogetery.com, на якому розміщувалось 73 000 блогів – фахівці ФБР знайшли на ньому посилання на матеріали Аль-Каїди.

В Україні для виконання завдань щодо забезпечення кібербезпеки держави задіяно низку військових та правоохоронних органів, зокрема, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації, Міністерство внутрішніх справ України тощо.

Проте, ситуація у вітчизняній кібербезпековій сфері залишається складною та характеризується неабиякими проблемами [8].

По-перше, в Україні не в повному обсязі відпрацьовано системні нормативно-правові документи, що формували б цілісну державну політику із кібербезпеки в державі.

У Законі України "Про основи національної безпеки" зустрічається лише поняття "комп'ютерний тероризм" та "комп'ютерна злочинність" (без пояснень).

У Стратегії національної безпеки України (від 26 травня 2015 року) [9] використовуються терміни "кіберпростір", "кіберзагрози", "кібербезпека", "кібератака", "кіберрозвідка", "кіберзлочин", але не подано їх тлумачення. У цьому документі визначено загрози кібербезпеці і безпеці інформаційних ресурсів та пріоритетні напрями забезпечення кібербезпеки і безпеки інформаційних ресурсів.

У Доктрині інформаційної безпеки України [10] приділено увагу кібербезпеці та питанням, пов'язаним з нею. Згадуються лише поняття "комп'ютерний тероризм" і "кібератаки", однак пояснень цих термінів у преамбулі немає.

Необхідно відзначити, що ще в 2013 році Уряд схвалив законопроект України про кібернетичну безпеку України але, нажаль, через політичні розбіжності був не прийнятий Верховною Радою України.

Разом з тим, фахівці Національного університету оборони України імені Івана Черняховського розробили відповідний понятійний апарат, який викладено у Військовому стандарті 01.004.004 (Видання 1) "Воєнна політика, безпека та стратегічне планування. Інформаційна безпека держави у воєнній сфері. Терміни та визначення" [11]. Цей документ уже функціонує в межах Міністерства оборони України та Збройних Сил України і довів свою практичну цінність під час реагування на антиукраїнські заходи у кіберпросторі зі сторони Росії.

Таким чином, в Україні на державному рівні ще недостатньо сформовано цілісну термінологічну систему, що визначала б єдиний понятійний апарат у сфері кібербезпеки: "кібербезпека","кібератака", "кіберпростір" тощо.

Все це призводить до того, що навіть спеціальні підрозділи силових відомств, у назві яких вживаються поняття "кіберзлочинність", "кібербезпека", не забезпечені відповідними нормативними документами для визначення предмету своєї роботи.

По-друге, в Україні не існують загальнонаціональні міжвідомчі координаційні структури, що могли б узгоджувати та координувати діяльність різних силових відомств під час розслідування злочинів у кіберпросторі та створенні ефективної системи захисту вітчизняного кіберпростору (в тому числі – у воєнній сфері). Досі в Україні жодного разу не проводились комплексні навчання, пов'язані із проблемами кібербезпеки (на кшталт навчань "Кіберштурм", що проводяться в США) із залученням усіх відомств, задіяних в системі кібербезпеки держави.

По-третє, більшість представників відомств, структур задіяних у системі забезпечення кібербезпеки України, акцентують увагу на їх незадовільне кадрове забезпечення відповідними фахівцями. Незважаючи на те що низка вищих навчальних закладів (військових, цивільних або відомчих) здійснюють підготовку фахівців за різноманітними спеціальностями, що можуть бути віднесені до сфери кібербезпеки, якість їх підготовки в багатьох аспектах незадовільна. Водночас слід зазначити, що неможливість залучення висококваліфікованих фахівців (молодих спеціалістів) до структур, задіяних у забезпеченні безпеки вітчизняного кіберпростору, пов'язана ще з недостатнім їх мотивуванням (матеріального та нематеріального характеру) залишатись на державній (військовій) службі. Крім того, не вистачає поліпрофільних науково-дослідних інститутів, що займались би комплексним дослідженням питань кібербезпеки (не лише проблеми обмеження доступу до інформації чи забезпечення технологічної безпеки, а й соціально-гуманітарної складової і особливо – їх поєднанням).

По-четверте, не завжди прозорим є розподіл функцій та завдань між державними спеціальними структурами щодо убезпечення кіберпростору держави. Ця проблема є наслідком невизначеності нормативного поля і пов'язана насамперед з відсутністю стратегічних документів, у яких би було здійснено подібний розподіл функцій та завдань (можливо, із визначенням відповідального (головного) відомства).

По-п'яте, незважаючи на зусилля спеціальних служб, відомств у сфері захисту кіберпростору, Україна все ще залишається уразливою (особливо її телекомунікаційна складова), не в останню чергу через надмірно широке впровадження західних програмних продуктів (зокрема, фірми Microsoft) та використання апаратних засобів зарубіжного виробництва. Пошук можливих "закладок" у цій продукції практично неможливий, а залежність нашої держави від згаданих продуктів становить загрозливий рівень для національної безпеки. Актуальною залишається проблема створення

національної операційної системи (принаймні для використання в системі органів державної влади програмного забезпечення з відкритим кодом, хоча для такого переходу є і суттєві зауваження з боку ключових вітчизняних безпекових організацій) та відновлення вітчизняних потужностей із виробництва апаратних засобів (особливо для потреб закритих відомчих інформаційних систем), стимулювання з боку держави створення національного антивірусу.

Висновки й перспективи подальших досліджень.

Аналіз тенденцій політики провідних держав щодо протидії загрозам у кіберпросторі та зміни внутрішньої інформаційної політики цих держав, зважаючи на посилення кібербезпекової компоненти в світі, дав змогу зробити такі висновки:

1. Більшість держав світу активно модернізує власні сектори безпеки відповідно до викликів сучасності та все більше застосовує потенціал мережі Інтернет для вирішення завдань збройної боротьби. Цей процес відбувається із активним реформуванням систем управління відповідним сектором безпеки (створення спеціалізованих підрозділів, управлінських структур); впорядкуванням нормативного поля, що має забезпечити цілісність державної політики в цій сфері; активною роз'яснювальною роботою серед населення щодо можливих ризиків унаслідок реалізації кіберзагроз; збільшенням чисельності відповідних підрозділів, зайнятих у системі кіберзахисту; розробкою кіберзброї та проведенням пробних кібернетичних атак, ударів у кіберпросторі; посиленням контролю за національним кіберпростором (способами доступу, контентом тощо).

2. З огляду на заяви експертів, задіяних у підготовці нової Стратегічної концепції НАТО, кібернапади на критично-важливу інфраструктуру держави необхідно розглядати як "акт війни". При цьому слід очікувати можливість закріплення відповідних змін у міжнародно-правових актах та статутних документах провідних міжнародних безпекових організацій, що дасть змогу ідентифікувати кібератаки, кіберудари або їх сукупність як збройні напади.

3. Тенденція посилення контролю з боку правоохоронних органів провідних держав світу за контентом національного кіберпростору показує, що панівним сьогодні є неоліберальний підхід до розуміння мережі Інтернет (так звана "Каліфорнійська ідеологія"), яка зазнає кардинальних змін. На зміну їй приходить "технореалізм" з його відношенням до ІКТ як "технології подвійного призначення" та ключовою роллю держави у розвитку мережі Інтернет.

4. Незважаючи на декларовані бажання основних геополітичних суб'єктів протидіяти мілітаризації кіберпростору, можна констатувати збільшення ролі суто військових структур у забезпеченні безпеки національної критичної інфраструктури (національного кіберпростору). У таких умовах Україна має бути готовою не лише до ведення оборонних заходів, а й до оперативнішого створювання власних сил і засобів для ведення активних дій у кіберпросторі.

5. Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективно діючу систему протидії кіберзагрозам. Серед таких проблем, насамперед, слід виділити: термінологічну невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних та технічних продуктів зарубіжного виробництва, складнощі із кадровим забезпеченням відповідних відомств, структур.

Література

1. "Сучасні тренди кібербезпекової політики: висновки для України". Аналітична записка. [Электронный ресурс] / – Режим доступа http://www.nisd.gov.ua/136711.pdf. **2. Горовий В. М.** Концептуальні засади створення системи захисту національної інформаційної інфраструктури від кіберзагроз / В. М.Горовий, О. Д. Довгань // Інформаційна безпека людини, суспільства, держави. – 2011. – № 2. – С. 15-21. **3. Климчук О. О**. Кібервійна у сучасних умовах / О. О.Климчук, Р. М. Кравченко // Інформаційна безпека людини, суспільства, держави. – 2011. – № 1. – С. 78-84. **4. Погорецький М**. Поняття кіберпростору як середовища вчинення злочинів / М. Погорецький, В. Шеломенцев // Інформаційна безпека людини, суспільства, держави. – 2009. – № 2. – С. 77-81. **5. Лайонс Д.** Тайная кибервойна Китая [Электронный ресурс] / Д.Лайонс. – Режим доступа : http://inosmi.ru/world/20110805/172946128.html. **6. Берчак І.** США назвали Китай загрозою для економіки та національної безпеки [Електронний ресурс] / І. Берчак. – Режим доступу : http://www.lvivpost.net/content/view/12509/505/. **7. Контрразведка** США обвиняет Китай и Россию [Электронный ресурс]. – Режим доступа : http://www.russian.rfi.fr/v-mire/20111104- kontrrazvedka-ssha-obvinyaet-kitaya-i-rossiyu. **8. Дубов Д. В**. Кібербезпека: світові тенденції та виклики для України : аналітична доповідь / Д. В.Дубов, М. А.Ожеван. – К. : НІСД, 2011. – 30 с. **9. Про Стратегію** національної безпеки України: указ Президента України від 26 травня 2015 року № 287\2015 [Електронний ресурс]. – Режим доступу:http://www.zakon2.rada.gov.ua/laws/show/287/2015/paran7#n7. **10. Про Доктрину** інформаційної безпеки України: Указ Президента України від 8.07.2009 р. № 514/ 2009 [Електронний ресурс]. – Режим доступу : http: //www.president.gov.ua/ documents/ 9570.html. **11. Військовий** стандарт 01.004.004 (Видання 1) "Воєнна політика, безпека та стратегічне планування. Інформаційна безпека держави у воєнній сфері. Терміни та визначення"

СОВРЕМЕННАЯ ПОЛИТИКА БЕЗОПАСНОСТИ КИБЕРПРОСТРАНСТВА В УСЛОВИЯХ ЕГО МИЛИТАРИЗАЦИИ

Александр Николаевич Косогов *(канд. воен. наук, с.н.с.)*
Анатолий Александрович Сирык

Воинская часть А1906

Проведен анализ мероприятий по обеспечению кибербезопасности ведущих стран мира, выделены основные тенденции трансформации внутренней политики государств с учетом активизации киберугроз в мире. Предложены пути улучшения кибербезопасной политики Украины с целью приведения ее к требованиям современности и обеспечение суверенитета государства в условиях милитаризации киберпространства.

Ключевые слова: *кибербезопасность; киберпространство; киберугроза.*

THE MODERN CYBERSPACE SECURITY POLICY UNDER CONDITIONS OF ITS MILITARIZATION

Oleksandr M. Kosohov *(Candidate of Military Sciences, Senior Research Fellow)*
Anatoliy O. Siryk

Military Unit A1906

The organized analysis action on provision cyber-security leading countries of the world, are chosen main trends transformations internal politicians state with provision for growing of cyber-threats. The Offered ways of the improvement politicians of Ukraine on provision of cyber-security for the reason adductions it to requirements of modern time and ensuring the sovereignty state in condition of the activations of the process to militarization of cyber-space.

Keywords*: cyber security; cyberspace; cyber threat.*

References

1. "Modern trends in cyber security policy: implications for Ukraine". Policy briefing. [Electronic resource], Access mode:http://www.nisd.gov.ua/136711.pdf **2. Horovyi V.M.,** Dovhan O.D. (2011) The conceptual basis for the creation of national system of protection of information infrastructure cyber threats. [*Kontseptualni zasady stvorennia systemy zakhystu natsionalnoi informatsiinoi infrastruktury vid kiberzahroz*], Informatsiina bezpeka liudyny, suspilstva, derzhavy, No 2, pp. 15-21. **3. Klymchuk O.O.** Kravchenko R.M. (2011) Cyberwar in modern conditions. [*Kiberviina u suchasnykh umovakh*] Informatsiina bezpeka liudyny, suspilstva, derzhavy, No 1, pp. 78-84. **4. Pohoretskyi M.,** Shelomentsev V. (2009), The concept of cyberspace environment as crimes. [*Poniattia kiberprostoru yak seredovyshcha vchynennia zlochyniv*], Informatsiina bezpeka liudyny, suspilstva, derzhavy, No 2, pp. 77-81. **5. Laions D.** Secret Chinese cyberwar [Electronic resource], Access mode:http://inosmi.ru/world/20110805/172946128.html.
6. Berchak I. US called China threat to the economy and national security [Electronic resource], Access mode : http://www.lvivpost.net/content/view/12509/505/.
7. Counterintelligence US blames China and Russia [Electronic resource], Access mode:http://www.russian.rfi.fr/v-mire/20111104-kontrrazvedka-ssha-obvinyaet-kitaya-i-rossiyu. **8. Dubov D.V.** (2011), Cybersecurity: global trends and challenges for Ukraine analytical report. [*Kiberbezpeka: svitovi tendentsii ta vyklyky dlia Ukrainy : analitychna dopovid*], Kyiv, NISD, 30 p. **9. Pro Doktrynu** informatsiinoi bezpeky Ukrainy : ukaz Prezydenta Ukrainy vid 8.07.2009. No 514/2009 [Electronic resource], Access mode: http://www.president.gov.ua/documents/9570.html

Отримано: 28.10.2015 року