НАЦІОНАЛЬНА БЕЗПЕКА

УДК 004.7.056(477)(1-622НАТО)«20»

КІБЕРБЕЗПЕКА – ГОЛОВНИЙ ВИКЛИК НАТО Й УКРАЇНИ В XXI СТОЛІТТІ

Год Б.В., Лобода Д.О.
Полтавський національний педагогічний університет
імені В.Г. Короленка

Статтю присвячено вивченню забезпечення кібербезпеки в НАТО, а також рівня секьюритизації цієї проблематики в системі відносин Україна – НАТО. Проаналізовано основні заходи Північноатлантичного альянсу і України щодо попередження можливих кібернетичних атак як одного із головних викликів національній безпеці в XXI столітті. Висвітлено хронологію найбільших кібернетичних атак на країни-члени альянсу і Україну, охарактеризовано їхні джерела й спрямованість. Окрім того, охарактеризовано шляхи боротьби з кібератаками в країнах-членах НАТО й Україні.
Ключові слова: гібридна війна, інформаційні технології, кібератака, комп'ютерний вірус, хакер.

Постановка проблеми. Інформаційна безпека є надзвичайно актуальним напрямом діяльності України в умовах сучасних європейського та євроатлантичного інтеграційних процесів. Сьогодні формується єдине європейське та світове інформаційне співтовариство, а інформаційна галузь стала опертям, на якому базуються всі політичні, адміністративні, економічні й інші рішення в усіх сферах людської діяльності. Конституція України називає інформаційну безпеку такою ж важливою, як захист суверенітету, територіальної цілісності та економіки загалом.

Доведено, що сучасні досягнення в галузі інформаційних технологій привели до початку перерозподілу реальної влади від традиційних структур до центрів управління інформаційними потоками. Інформаційні технології стають ключовими, насамперед у таких галузях як фінансовий обіг і ринок цінних паперів, зв'язок, транспорт, високотехнологічні виробництва тощо. Ще більшої ваги вони набувають у держаному управлінні, яке вбирає в себе інформаційну діяльність. Ухвалення важливих рішень стало неможливим без опрацювання гігантських потоків інформації, що циркулюють у суспільстві, обсяг яких постійно зростає. Можна стверджувати, що в розвинених країнах фактично відбулося формування суспільства, в якому більшість працездатного населення залучена до інформаційної сфери та сприяє розвитку нових форм і методів досягнення політичних, економічних та інших цілей на інформаційному рівні.

При цьому зазначимо, що сучасне інформаційне суспільство є надзвичайно вразливим до найзначніших, на перший погляд, упливів на його інформаційні складники. Чим розвиненішою є країна, тим більше вона залежить від впливів на її національну безпеку саме в інформаційній сфері.

Із огляду на це державна політика забезпечення інформаційної безпеки є одним із найважливіших складників політики національної безпеки, яка набуває все більшого самостійного значення. При цьому надання гарантій інформаційної безпеки особі, соціальним групам, суспільству та державі в цілому можливе лише на основі системної превентивної діяльності органів державного управління.

Аналіз останніх досліджень і публікацій. Першим автором, який ще в 1976 р. ввів термін «інформаційна війна» і сформулював основні положення її концепції, був американський учений Т. Рона [22, с. 1, 2]. Сьогодні є низка досліджень, результати яких усебічно розкривають особливості інформаційної війни і психологічних впливів. Серед дослідників, які системно вивчали питання кібербезпеки як одного з різновидів інформаційної війни, варто назвати таких: К. Демчак, П. Домбровський, А. Клімбург, М. Лібіцкі, Дж. Льюіс, Дж. Най, Г. Раттрей, С. Старр, Дж. Шелдон, М. Шмідт та ін. Серед вітчизняних учених відзначимо передусім дослідження В. Бутузова, О. Довганя, М. Ожевана, В. Пилипчука, В. Петрова, В. Шеломенцева та ін.

В останні кілька років терміни з приставкою «кібер» отримали широке вживання в міжнародно-політичному дискурсі та знайшли своє відобиття в стратегічних доктринах не лише держав, але й міжнародних організацій, включаючи НАТО. К. Ґірз, представник США в Центрі кібероборони НАТО, зазначає, що термін «кібер» використовується стосовно комп'ютерів, інформаційних мереж і цифрової інформації [16, с. 21].

Виділення невирішених раніше частин загальної проблеми. Детальний аналіз підходів НАТО щодо протидії інформаційним загрозам і забезпечення кібероборони представляє інтерес в світлі того, що питання в даній галузі відносять до сфери «м'якої» безпеки (soft security), у той час як головне завдання НАТО – протидіяти конвенціональним викликам безпеки (hard security). Більше того, після розпаду біполярного світопорядку НАТО проходить складний процес трансформації і знаходиться в пошуках набуття свого «raison d'ктre». Звідси виникає необхідність знайти відповіді на низку важливих для євроатлантичного простору безпеки питань. Як розуміють у НАТО кібербезпеку? Який зміст і рівень інформаційних загроз? Хто є їхнім джерелом?

Мета статті. Беручи до уваги фактичну відсутність міжнародної нормативно-правової бази,

що регулює взаємини «акторів» різного рівня в глобальному інформаційному просторі, а також традиційно високі політичні ставки в сфері євроатлантичної безпеки і пов'язаний з ними складний процес діалогу між Росією і країнами НАТО, є нагальна потреба вивчення забезпечення кібербезпеки всередині Альянсу, а також ступеня секьюритизації даної проблематики в системі відносин Україна – НАТО.

У зв'язку з цим ми прагнемо проаналізувати основні заходи Північноатлантичного альянсу і України щодо попередження можливих кібернетичних атак як одного із головних викликів національній безпеці в XXI столітті.

Виклад основного матеріалу. Досвід конфліктів середньої й низької інтенсивності наприкінці XX – на початку XXI століття підтверджує, що в наш час відбувається перехід від воєн механічного руйнівного характеру до воєн із перевагою функціонально-структурного, виборчого впливу на супротивника. Сьогодні сформувалися погляди на війни, як на самостійне суспільно-політичне явище, різноманітне за цілями і застосовуваними видами насильства, але не завжди пов'язане зі збройною боротьбою.

Характер розвитку засобів збройної боротьби і похідна від їхніх можливостей, організація ведення бойових дій у сучасних умовах свідчать про те, що армії багатьох країн світу мають на озброєнні якісно нову зброю – інформаційну та готові до ведення зовсім нового виду війни –інформаційної. Так, за оцінками начальника штабу ВПС США, сьогодні близько 100 країн готові до проведення такого виду воєн (наступального або оборонного характеру). За даними американських спецслужб, програми інформаційних воєн половини цих країн націлені проти США та їхніх союзників, перш за все – по Північноатлантичному альянсу [22, с. 32, 33].

Швидкий розвиток інформаційно-комунікаційних технологій в останні два десятиліття справив потужний вплив і на міжнародні відносини. Як зазначає фахівець у галузі інформаційної безпеки П. Шаріков, «...активне поширення, впровадження та використання інформаційних технологій швидко призвело до того, що ці технології стали застосовуватися не лише як засіб обміну й обробки інформації, але й як спосіб нанесення шкоди» [11, с. 582].

Доведено, що інформаційна зброя – це устаткування, прилади, технології та інші засоби, що використовуються для широкомасштабного, цілеспрямованого, прихованого інформаційного втручання в мислення і настрій людей, а також в інформаційні та телекомунікаційні системи. Інформаційна зброя включає засоби: знищення, викривлення або викрадання інформаційних масивів; подолання систем захисту; обмеження доступу до інформації законних користувачів; дезорганізації роботи технічних засобів, комп'ютерних систем [11].

До атакуючої інформаційною зброї відносять: комп'ютерні віруси, логічні бомби (програмні закладки), засоби інформаційного обміну в телекомунікаційних мережах, фальсифікації інформації в каналах державного і військового управління, засоби нейтралізації тестових програм, різного роду помилки, що свідомо вводяться до програмного забезпечення об'єкта.

Ядром «проблемного поля» інформаційної безпеки є визначення того, яка природа і деструктивний потенціал інформаційних загроз. П. Корніш із лондонського Королівського інституту закордонних справ навів таку класифікацію інформаційних загроз: 1) діяльність хакерів-одинаків; 2) організована злочинність, яка діє в глобальних інтернет-мережах; 3) ідеологічний і політичний екстремізм; 4) державна кіберагресія [7, с. 7-16].

На сьогоднішній день лише перші два різновиди загроз із вище наведеної класифікації знайшли практичне втілення в світовій політиці. Що стосується кібертероризму і кібервійни між державами, то вони є скоріше уявними загрозами, які можуть бути зреалізовані в майбутньому.

У НАТО під кібербезпекою розуміють підтримання стану готовності до відбиття потенційних загроз, що володіють «високою інтенсивністю» і прийняття відповідних контрзаходів. Експерти з Центру кіберзахисту НАТО розглядають мілітаризацію Інтернету як одного з головних і найбільш небезпечних трендів розвитку світового кіберпростору: «Сучасні військові структури готові використовувати інформаційний простір як «паралельне поле битви» в конфліктах майбутнього». При цьому висловлюється впевненість у тому, що проведення кібернаступу «в чистому вигляді» малоймовірно [20].

Уперше питання кібербезпеки постало в порядку денному НАТО на саміті в Празі в листопаді 2002 року, коли лідери країн Альянсу висловили готовність посилювати можливості з надання протидії інформаційним атакам. Тоді й розпочалося створення спеціальних органів НАТО, наприклад таких, як Агентство НАТО з обслуговування комунікаційних та інформаційних систем. Його вважають першою лінією захисту Альянсу проти кібертероризму [0].

Після того як Естонія в квітні та травні 2007 року зазнала серії кібератак, у НАТО виник консенсус щодо сприйняття кібернетичних загроз як стратегічно важливих. А офіційна політика НАТО в сфері кібероборони (NATO Cyber Defence Policy) була схвалена в січні 2008 року міністрами оборони країн-членів НАТО і представлена учасникам організації в квітні 2008 року на саміті в Бухаресті. Згідно підсумкової декларації цього саміту, даний документ гарантував «...забезпечення можливості для надання підтримки країні-союзниці на її вимогу в протидії кібератаці» [19]. 8 червня 2011 року була прийнята нова політика кібероборони. Проте зміст цих документів недоступний для широкого загалу.

У той же час можна простежити розпочаті НАТО практичні кроки в реалізації політики кібербезпеки. Так, у 2008 році було створено Управління по здійсненню кібероборони. Функціонально воно покликане ініціювати та координувати дії у відповідь у разі кібератаки, спрямованої проти кого-небудь із країн-членів НАТО, або ж самої НАТО [23].

У жовтні 2008 року отримав акредитацію при НАТО Центр передового досвіду в сфері кібероборони в Талліні. Проте він не наділений оперативними функціями і служить як дослідний і навчальний центр, де розробляються доктринальні та концептуальні засади кібербезпеки та проводяться навчальні семінари. Дана структура по-

зиціонує себе як «головне джерело експертизи в сфері спільної кібероборони», який «акумулює, створює і поширює знання з провідних питань кібербезпеки всередині НАТО, між державами Альянсу і його партнерами» [21].

Британський експерт Рекс Хьюз розглядає ці два спеціалізованих органи як елементи єдиної організаційної системи. Управління по здійсненню кібероборони, ймовірно, наділене « ...просунутими можливостями щодо здійснення електронного моніторингу в «реальному часі», діє на оперативно-тактичному рівні. Центр передового досвіду в області кібероборони, розробляючи довгострокову доктрину НАТО в даній сфері та представляючи собою своєрідну «інтелектуальну платформу», є елементом стратегічного рівня [17].

Проблема кіберзагроз представлена і в новій версії Стратегічної концепції НАТО, прийнятій на саміті в Лісабоні в листопаді 2010 року. У документі інформаційні атаки виокремлюються серед найбільш небезпечних викликів і загроз безпеці та процвітанню держав-членів Альянсу [24]. У концепції проблема кібербезпеки виходить з інформаційного простору загроз і розташовується одразу після поширення зброї масового ураження і тероризму. Така увага, у свою чергу, обумовлена феноменом секьюритизації, під яким розуміється артикуляція проблеми в контексті проблем безпеки [4], і завдяки якому кібербезпека з вражаючою швидкістю еволюціонувала від технічної дисципліни до стратегічної концепти [16, с. 9].

Можна з упевненістю говорити, що нині кіберпростір переживає час «неосередньовіччя» з усіма його атрибутами: відсутність чіткого міжнародного права, розбудова системи відносин «клієнт-патрон», формування своєрідних «феодальних угідь» в інформаційній сфері. Однак, якщо в класичному Середньовіччі це було пов'язано передусім із питаннями земельної власності, то тепер ми маємо справу з кіберпростором. Як слушно відзначає Б. Шнаєр, «...ми маємо справу із феодальною моделлю. Користувачі заявляють про свою вірність могутнішим компаніям, що обіцяють їх захистити від тягара системного адміністрування та загроз безпеці» [13, с. 61, 62]. Цими «новими феодалами» стають потужні IT-ТНК на кшталт Apple, Google, Microsoft, Facebook та ін.

Водночас сучасний кіберпростір і ті процеси, які нині відбуваються в ньому, значно нагадують проблеми часів «холодної війни», для якої характерний високий рівень латентних конфліктів на міжнародній арені, непрямі методи боротьби (передусім активізація розвідувальної діяльності всіх сторін глобального протистояння), перенесення конфліктів на територію третіх країн (наприклад у формі протистоянь за сфери впливу) та гонка озброєнь (у даному випадку – «кіберозброєнь»). Ситуація загострюється новим протистоянням Заходу і Росії (Сирія, Туреччина, КНДР, Україна). За таких умов особливого значення для забезпечення національних інтересів та їхнього захисту на міжнародному рівні набувають ефективні механізми забезпечення кібербезпеки держави та вирішення тих проблем, що виникають на шляху їхньої розбудови.

Щодо України, яка також є частиною планетарного інформаційного простору і одним із найактивніших користувачів мережею Інтернет, питання кібербезпеки стоять у авангарді викликів її національній безпеці та обороні. Так, у грудні 2015 року хакери атакували шість енергокомпаній у Західній Україні. За її наслідками 225 тис. українців у 103 населених пунктах держави залишилися без електроенергії внаслідок її навмисного відключення. Це був перший випадок масштабної хакерської атаки на Україну. Найбільш масштабною хакерською атакою на Україну стала атака так званого вірусу «Petya» 27 червня 2017 року. Призводячи до значних матеріальних втрат, такі удари можуть нести пряму небезпеку не лише для економіки країни, але й для її політичного та військового потенціалу [7].

Українська енергетична галузь стає випробувальним полігоном майбутньої кібервійни. Серед мішеней вірусу Petya була і Чорнобильська АЕС. Словацький розробник антивірусів, компанія ESET у опублікованому нещодавно аналізі атак на українську енергетику також називає BlackEnergy «кібезброєю», а Україну – полігоном для її випробування. Цю тенденцію розуміють і західні військові партнери України. Програма з кібербезпеки та посилення захисту енергетичного сектора – один із донорських проектів, що реалізується в рамках партнерства Україна-НАТО. У рамках цього проекту минулого року на базі департаменту захисту інтересів держави в інформаційній сфері СБУ був створений окремий підрозділ із кібербезпеки, що отримав близько мільйона доларів із трастового фонду НАТО [0].

Окрім цього, Центр НАТО з кіберзахисту опублікував книгу про кібервійну між Україною та Росією під назвою «Кібервійна у перспективі: Російська агресія щодо України». У роботі, підготовленій вченими і експертами-практиками, наведено підсумки аналізу біжучої діяльності щодо поширення та захисту інформації, а також запропоновано бачення стратегічних і тактичних наслідків кібервійни. У ній йдеться про період 2013-2015 років. Експерти вказують на те, що поняття «кібератака» вийшло за межі лише інформаційної війни. Сьогодні поняття містить цифрову пропаганду, DDoS-кампанії, дефейси web-сайтів, витоки інформації внаслідок атак активістів, а також використання шкідливого програмного забезпечення для шпигунства [14, с. 7, 8, 9].

Усвідомлюючи зростаючу загрозу кібератак, Україна і Північноатлантичний альянс розпочали процес створення спільного фахового майданчика, у межах якого будуть вестися консультації та обмін досвідом із питань інформаційної безпеки у світі. Так, у 2017 році у м. Києві відбувся перший Глобальний саміт з кібербезпеки Global Cybersecurity Summit. Під час відкриття саміту промову виголосила посол США в Україні Марі Йованович. «...Ми знаємо, що кіберзагрози та кібератаки не мають кордонів, – сказала посол. – Ось чому нам потрібно об'єднуватися, щоб протидіяти цій загрозі. Це означає, що ми маємо бути ближчими, ділитися досвідом і допомагати один одному» [8].

Участь у саміті брав також колишній заступник держсекретаря США (2015–2017) Ентоні Блінкен, який у промові торкнувся теми втручання Росії у виборчий процес у США. За його словами, втручаючись в американські вибори, росій-

ський президент Володимир Путін хотів підірвати віру в демократичний американський процес, водночас намагаючись продемонструвати народу, що всі системи корумповані та заангажовані [8].

Д. Шимків, заступник голови адміністрації Президента України, у ході цього ж саміту зазначив, що Україна має приклад інструментів для боротьби з вигаданими новинами – фейками. Саме українці одними з перших створили ресурс «StopFake.org» для того, щоб виявляти і публічно спростовувати неправдиву інформацію про країну і події поза її межами. За три роки роботи стартапа його учасники виявили понад 1000 російських фейків. Український досвід підтвердив свою ефективність, і може бути застосований в будь-якій країні, яка потрапила в центр уваги зловмисників [12].

Сьогодні в Україні вже діють декілька успішних проектів із кіберзахисту, серед яких можна назвати «Український кіберальянс», «Українські кібервійська», «ІнформНапалм», «Миротворець», «Кіберполіція», а також CERT-UA [3].

Для боротьби з проявами інформаційної та кібернетичної війни Україна готова мобілізувати всі наявні ресурси. Так, у 2017 році в лави ЗСУ почали призивати офіцерів запасу. Серед цієї групи людей досить багато фахівців із вищою технічною освітою, є багато програмістів. «...Звичайно, можна спробувати навчити цих людей чомусь зовсім новому, а можна використати їхню цивільну професію, навчити її військовим особливостям, згуртувати в групи, створивши логічні соціальні зв'язки, які не будуть перериватися і в мирний час, що забезпечить додаткову обороноздатність держави в кіберпросторі», – зазначила народний депутат України, голова постійної делегації України в Парламентській асамблеї НАТО Ірина Фріз. На думку політика, у результаті Україна зможе значно посилити кібервійська, а офіцери запасу отримають мотивацію і можливість удосконалитися в своїй цивільній професії, яка в будь-який час може згодитися Батьківщині [9].

Із найостанніших новин у сфері співробітництва України і США – подвоєння допомоги Україні на кібербезпеку – з п'яти до десяти мільйонів. Про це заявив 2 травня 2018 року, спілкуючись у Києві з пресою, помічник державного секретаря США у справах Європи і Євразії Весс Мітчелл [5].

Висновки з дослідження. Таким чином, питання забезпечення кібербезпеки все активніше постає в колах військово-політичного керівництва країн-членів НАТО і України. Кіберагресія, яка в інформаційну епоху стає інструментом ведення геополітичної боротьби Російської Федерації проти України і Північноатлантичного блоку, визначена як головний виклик світовій системі безпеки і потребує якомога тіснішої співпраці та взаємодопомоги останніх. У той же час, надзвичайна цінність досвіду України в боротьбі проти інформаційної війни вже стала предметом розширення такої кооперації. З огляду на два майбутні ювілеї, які відзначатиме на державних рівнях Україна і країни-члени НАТО у 2019 році – створення альянсу і приєднання України до програми «Партнерство заради миру», логічно назрівають питання інституціоналізації і зміцнення їхніх союзницьких відносин на концептуально новому рівні.

Список літератури:

1. Бурдига І. Україна як полігон для майбутніх кібервійн? [Електронний ресурс] / І. Бурдига. – Режим доступу: http://www.dw.com/uk/a-39491119.
2. Декларація Празького саміту [Електронний ресурс]. – Режим доступу: zakon4.rada.gov.ua/laws/show/950_003.
3. Дрогомирецкий Б. Украино-российская кибервойна: невидимый фронт [Электронний ресурс] / Б. Дрогомирецкий. – Режим доступа: https://www.pravda.com.ua/rus/columns/2018/02/22/7172439.
4. Макарычев А. Безопасность как феномен публичной политики: общие закономерности и проекции на Балтийский регион [Электронний ресурс] / А.С. Макарычев. – Режим доступа: http://megaregion.narod.ru/articles_text_2.htm.
5. Поки Путін не обере мир [Електронний ресурс] / Голос Америки. – Режим доступу: https://ukrainian.voanews.com/a/mitchel-u-kyyevi/4374569.html.
6. Почепцов Г. Информационные войны: тенденции и пути развития [Электронний ресурс] / Георгий Почепцов. – Режим доступа: http://psyfactor.org/psyops/infowar7.htm.
7. Прудка Н. Кібервійна проти України. Перші жертви і висновки [Електронний ресурс] / Н. Прудка. – Режим доступу: https://glavcom.ua/publications/334262-kibervijna-proti-ukrajini.-pershi-zhertvi-i-visnovki.html.
8. Пушкарук Н. Чи готова Україна до «кібервійни»? [Електронний ресурс] / Н. Пушкарук. – Режим доступу: https://day.kyiv.ua/uk/article/den-planety/chy-gotova-ukrayina-do-kiberviyny.
9. Фріз І. Україна має активно готуватися до кібервійни [Електронний ресурс] / І. Фріз. – Режим доступу: https://ukr.lb.ua/blog/irina_friz/357941_ukraina_maie_aktivno_gotuvatisya.html.
10. Цільовий план Україна – НАТО на 2003 рік у рамках плану дій Україна – НАТО [Електронний ресурс]. – Режим доступу: https://www.nato.int/docu/basictxt/b030324u.pdf.
11. Шариков П.А. Информационный комплекс / П.А. Шариков // Безопасность Европы / Ин-т Европы РАН. – М.: Весь мир, 2011. – С. 581-591.
12. Шимкив Д. Кибервойна. Что Украина может предложить миру [Электронний ресурс] / Д. Шимкив. – Режим доступа: https://nv.ua/opinion/shimkiv/kibervojna-chto-ukraina-mozhet-predlozhit-miru-2093806.html.
13. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Брюс Шнайер. – СПб.: Питер, 2003. – 368 с.
14. Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks // Directorate-General for External Policies of the Union, Policy Department. – Brussels: European Parliament, 2009. – 34 p.
15. Geers K. Cyber War in Perspective: Russian Aggression against Ukraine / Kenneth Geers. – Tallinn: NATO CCD COE, 2015. – 175 p.
16. Geers K. Strategic Cyber Security / K. Geers. – NATO Cooperative Cyber Defence Centre of Excellence, 2011. – 169 p.
17. Hughes R.B. NATO and Cyber Security: Mission accomplished [Електронний ресурс] / R.B. Hughes. – Режим доступу: http://www.carlise.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf.
18. McGee J. NATO and Cyber Defense: A Brief Overview and Recent Events / J. McGee. – Electronic text data. – Mode of access: http://csis.org/blog/natoand-cyber-defense-brief-overview-and-recentevents.

19. NATO Bucharest Summit Declaration, Art. 47, 3 April 2008 [Електронний ресурс] / NATO. – Режим доступу: http://www.nato.int/docu/pr/2008/p08-049e.html.
20. NATO CCD CoE General Trends [Електронний ресурс] / NATO Cooperative Cyber Defence Centre of Excellence. – Режим доступу: http://www.ccdcoe.org/8.html.
21. NATO CCD CoE Mission and Vision [Електронний ресурс] / NATO Cooperative Cyber Defence Centre of Excellence. – Режим доступу: http://www.ccdcoe.org/11.html.
22. Rona T. Weapon Systems and Information War [Електронний ресурс] / Thomas P. Rona // Boeing Aerospace Co., Seattle, WA. – 1976. – Режим доступу: http://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf.
23. Stein G. Information Attack: Information Warfare In 2025 [Електронний ресурс] / George J. Stein. – Режим доступу: http://csat.au.af.mil/2025/volume3/vol3ch03.pdf.
24. Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation. Active Engagement, Modern Defence [Електронний ресурс] / NATO. – Режим доступу: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.

Год Б.В., Лобода Д.А.
Полтавский национальный педагогический университет
имени В.Г. Короленко

КИБЕРБЕЗОПАСНОСТЬ – ГЛАВНЫЙ ВЫЗОВ НАТО И УКРАИНЫ В XXI ВЕКЕ

Аннотация
Статья посвящена изучению обеспечения кибербезопасности в НАТО, а также уровня секьюритизации этой проблематики в системе отношений Украина – НАТО. Проанализированы основные мероприятия Североатлантического альянса и Украины по предупреждению возможных кибернетических атак как одного из главных вызовов национальной безопасности в XXI веке. Освещена хронология крупнейших кибернетических атак на страны-члены Альянса и Украину, охарактеризованы их источники и направленность. Кроме того, охарактеризованы пути борьбы с кибератаками в странах-членах НАТО и Украины.
Ключевые слова: гибридная война, информационные технологии, кибератака, компьютерный вирус, хакер.

God B.V., Loboda D.O.
Poltava V.G. Korolenko National Pedagogical University

CYBER-SECURITY IS THE MAIN CHALLENGE OF NATO AND UKRAINE IN THE XXIST CENTURY

Summary
The article is devoted to the study of ensuring cyber security in NATO, as well as the level of securitization of this problem in the Ukraine-NATO relations system. The main activities of the North Atlantic Alliance and Ukraine to prevent possible cyber attacks as one of the main challenges to national security in the 21st century are analyzed. The chronology of the largest cyber attacks on the countries-members of the Alliance and Ukraine is highlighted, their sources and direction are characterized. In addition, the ways of fighting cyberattacks in the NATO member countries and Ukraine are described.
Keywords: computer virus, cyberattack, hacker, hybrid war, information technology.