УДК 343.32

Лалак О. А., Leszek Klich*

РИЗИКИ І ВИКЛИКИ КІБЕРБЕЗПЕКИ: ДОСВІД УКРАЇНИ ТА ПОЛЬЩІ

Анотація. *Розвиток інформаційно-комунікаційних технологій сприяє оцифруванню, технічній модернізації предметів щоденного вжитку. Для інформаційної протидії ризикам і викликам кібербезпеки України та Польської Республіки, важливо вдосконалювати технічну спроможність держави зменшувати потенційні кіберзагрози.*

Ключові слова: *кібербезпека, кіберпростір, інформаційна атака, гібридна війна, національна безпека.*

Annotation. *The development of informative and communication technologies entailes the digitising, technical modernisation of the subjects of daily consumption. It is necessary to improve the state's technical ability to diminish potential cyber threats and to provide the informative counteraction to the risks and calls of cybersecurity of Ukraine and Polish Republic.*

Key words*: cybersecurity, cyberspace, informative attack, hybrid war, national safety.*

Аннотация. *Развитие информационно-коммуникационных технологий способствует оцифровке, технической модернизации предметов ежедневного потребления. Для информационного противодействия рискам и вызовам кибербезопасности Украины и*

* Лалак О. А. – кандидат наук із соціальних комунікацій, асистент кафедри міжнародної інформації Національного університету «Львівська політехніка»

Leszek Klich – Magister Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie

Польской Республики, важно совершенствовать техническую возможность государства уменьшать потенциальные киберугрозы.

Ключевые слова: *кибербезопасность, киберпространство, инормационная атака, гибридная война, национальная безопасность.*

Постановка проблеми. Розвиток інформаційно-комунікаційних технологій сприяє оцифруванню, технічній модернізації предметів щоденного вжитку. Йдеться не лише про телевізори, усі різновиди комп'ютерних засобів, але й про персональні ґаджети, переважна більшість яких мають доступ до мережі Інтернет. Звідси випливає розповсюджена проблематика наукових досліджень, як психологічного, так і технічного характеру – ризики і загрози кібербезпеці держави, суспільства, особистості зокрема.

Аналіз останніх досліджень і публікацій. Проблематикою етимології поняття кібер, кіберпростору, «гібридної війни», національної безпеки, інформаційних атак у державних і недержавних структурах займалися провідні українські та польські вчені: І.Кочан, Є.Магда, У.Еко, А.Гловацькі, Е.Ліховські, А.Маєвські, А.Мєлніцки, А.Пікуліцка, Т.Покручинські, М.Терліковскі, В.Гібсон, Т.Влодарчук та ін.

Виділення невирішених раніше частин загальної проблеми. Виходячи з того, що проблема інформаційних загроз кіберпростору є наднаціональною, у статті наведено спробу виділити проблеми та спільні шляхи забезпечення захисту даних України та Польщі.

Основні цілі статті: проаналізувати теоретичні та практичні аспекти інформаційних викликів і ризиків кібербезпеки; навести приклади протиправної хакерської діяльності; запропонувати шляхи технологічної оптимізації інформаційних потоків у кіберпросторі.

Намагання атакувати кіберпростір полягає, перш за все, у прагненні захопити інформацію, як засіб передавання повідомлень. Однак сучасний розвиток комунікаційних технологій вимагає узалежнення будь-яких дій

від так званого «інформаційного суспільства». Виділимо основні його характеристики, посеред яких можливість: генерування, зберігання, отримання, передачі, застосування інформації, а також – технічна спроможність накопичувати, модифікувати та інтерпретувати дані, незалежно від часу чи простору. Залежність від місця проживання, від політичної ситуації та від технічних і фінансових обставин передбачають явище «цифрового виключення». Умберто Еко, прогнозуючи розвиток суспільства, підкреслив, що ті верстви населення, які затрималися в телевізійній епосі і не дають ради з новітніми технологіями, стають цілковито залежними від засобів медіа-впливу [10, с. 531-532].

Інформаційна боротьба уможливила проведення деструктивних атак на дані, до яких суспільство і держави в цілому, не є підготовлені – ані технічно, ані юридично, ані організаційно. Ефекти атак мають показовий характер, так як традиційно місце боротьби переноситься на іншу місцевість. Відповідно, ускладнюється спостереження за процесами і наслідками інформаційних нападів, а здійснення їхнього аналізу і вибір методів захисту від їх впливу стає об’єктом дослідження вузького кола спеціалістів. Незалежно від типу і методів інформаційних атак, їхній вплив є багатовимірним і каскадним. Детально сплановані напади на кіберпростір можуть спричинити дезорганізацію, матеріальні втрати об’єкта уражень, а у випадку пошкодження систем критичної інфраструктури держави, можуть навіть призвести до особових втрат [12, с. 2].

Ще у 1984 р. В. Гібсон в повісті «Burning Chrome» вперше вжив поняття «кіберпростір», описавши концепцію Інтернету та віртуальної реальності ще перед появої цієї технології. П. Вільям підкреслив, що кіберпростір є «королівством просторових парадоксів» [20].

З огляду на розвиток багатьох сфер діяльності з компонентом «кібер», слід узагальнити значення спільного кореня. Кочан І. подає ґрунтовне дослідження етимології термінів з компонентом «кібер-» [1, с.

277]. У вказаному дослідженні зазначено, що кожен термін може належати до відповідної терміносистеми, наприклад: поняття права і криміналу (кібербулінг, кібербезпека, кіберзакон, кібер-загрози, кіберзалякування, кібермафія, кіберполіція, кібертероризм, кіберзлочинність, кібершпигунство); абстрактні поняття (кіберреальність, кібербезпека; поняття військової справи (кібератака, кібервійна); назви осіб (кіберхакер) та ін. Філолог зауважила, що для національної безпеки існують «чотири основних категорії кіберзагроз, кожна з яких характеризується різним тимчасовим горизонтом: кібервійна та економічне шпигунство, пов'язані, як правило, з державами, а кіберзлочинність і кібертероризм зазвичай пов'язані з недержавними суб'єктами» [1, с. 278-284]. Натомість, Гловацький А. окреслив «кіберпростір» як консенсусну галюцинацію і простір відкритого комунікування за допогою поєднаних комп'ютерів і інформативної пам'яті [11, с. 14].

Очевидно, що динамічне поширення атак на кіберпростір породило ряд проблем в процесі дотримання світового правопорядку. Розвиток загроз кібербезпеці демонструє взаємовплив цифрових доменів на загальний стан національної безпеки, адже при сталому розвитку технологій виникають як внутрідержавні, так і міжнародні суперечки.

Кіберпростір виступає як поле битви, оскільки негативні явища в ньому можуть генерувати втрати і знищення великих розмірів. Наприклад, відомий комп'ютерний хробак Стакснет, який перехоплює і модифікує інформаційний потік з метою несанкціонованого збору даних з організацій державного значення. Будучи розробкою ізраїльських спецслужб, Стакснет спрямований на знищення іранської ядерної програми, оскільки понад тисячею центрифуг знищував уран в підприємствах Ірану в Natanz. З-поміж багатьох комп'ютерних вірусів, саме Стакснет має глобальне значення, оскільки спроможний фізично знищувати пристрої, а не лише наносити шкоду програмному забезпеченню чи викрадати дані [21].

Разом із здобуттям незалежності, Україну чекав нелегкий шлях розвитку, в тому числі – поділ впливу, глобальні загрози, локальні конфлікти. Прагнучидемонстувати не останнє місце на світовий загал, країна бере активну участь у сфері гарантування міжнародної безпеки, позиціонуючи себе як відданого прибічника затверджених основ Статуту ООН. Несподівано сусідня держава – Російська Федерація виявила агресію, здійснюючи не лише збройні повстання, але й інформаційні атаки. Приклад останніх – «Кримська операція», яка підтвердила спроможність неконвенційних засобів боротьби досягати політичних цілей [15]. Декілька років перед незаконною анексією Автономної Республіки Крим, Росія розгорнула безпредентдентну дезінформаційну кампанію, впровадивши федеральні телеканали, локальне радіо, газети та мережеві засоби масової комунікації. До заздалегідь спланованої акції було залучено політиків, дипломатичних представників, політологів, експертів, провідних науковців і культурних діячів. Така різностороння інсайдерська кампанія, під чітким керівництвом держави-агресора, поступово вносила зміни в громадську свідомість і масово згладжувала спірні історичні, економічні, національні питання, щоб під час військового захоплення Криму, аргументи Кремля видати за бажання мешканців півострову.

Військові та немілітарні атаки Російської Федерації проти України мають на меті, окрім нелегального захоплення суверенних територій, змінити спосіб мислення і поведінки, а також уподобання та історичне минуле в тимчасово анексованих областях. Дослідження «гібридної війни» у сучасних конфронтаціях показує загрози конвенційних, нерегулярних, кібернетичних протистоянь як комплексної стратегії чи типу війни, що поєднує різнорідні елементи деструктивних дій. На жаль, розвиток засобів та способів поширення «гібридної війни», не предбачає пришвидшення відповідальності за вчинені інформаційні атаки. Окрім того, інформація використовується під час військових конфліктів, що не лише в

зовнішньому оточенні (міжнародна безпека держави), але й на внутрішньо-політичній арені займає значну загрозливу позицію.

Так, «гібридну війну» трактують як різновид протистояння, що поєднує у собі звичайні та нестандартні способи ведення війни: класичні прийоми боротьби із залученням військової техніки, військовослужбовців в уніформі; нерегулярні збройні формування (повстанці, терористи, партизани); інформаційну війну. Засоби кібервійни застосовують не лише для доступу до конфіденційних даних держави, але й для пропагандистського поширення матеріалів, політичного шпигунства і вандалізму. Варто зазначити, що триваюча війна в Україні відбувається без кримінальної і процесуальної російської відповідальності за агресію. В той час, як Незалежна намагається всіма можливими способами досягти мирних взаємин і дипломатичних переговорів, Російська Федерація з насмішкою демонструє світовій арені непричетність до війни [8].

Інформаційні атаки у кібрпросторі здійснюються одним фахівцем, або групою підготовлених осіб. І хоча можна виокремити критерії поділу декількох груп за філософією, ідеологією і метою їхньої діяльності, зазвичай, не так легко ідентифікувати кіберзлочинців, оскільки вони можуть представляти інтереси зацікавлених осіб, державних організацій чи недержавних структур. Відповідно, джерело кібератаки може залишитися анонімним. Схожу стратегію обрала Російська Федерація, проводячи інформаційну війну на терені України. Серед численних методів ведення «гібридної» війни держава-агресор успішно аплікує наступні:

- «криве дзеркало» – смислова видозміна фактів і дискурсів;
- «спекуляції на історії» – педалювання дискусійних моментів українсько-російської історії;
- «заперечення очевидного» – перманентна показовість начебто відсутності агресії;
- «килимове бомбардування дезінформацією» – поширення у суспільстві панічних настроїв, зневіри;

- «показова миротворчість» – позиціювання Росії як мирно налаштованої та не причетної до конфлікту сторони (а в дійсності – чого тільки варті так звані гуманітарні конвої) та ін. [2].

Саме тому охорона власних інформаційних даних, програмного забезпечення та стратегічних документів повинна бути на високому рівні, з метою збереження непорушності держави. Загострення та активізація антихакерської діяльності в Україні були спричинені проаналізованою «гібридною війною». Основні визначення викликів і ризиків для кібербезпеки України, а також шляхи протидії інформаційним атакам спостерігаємо в сучасних документах державного значення. Так, проаналізувавши Стратегію кібербезпеки України, внесену Кабінетом Міністрів України, Рада національної безпеки і оборони України, на чолі з О. Турчиновим, відповідно до статті 14 Закону України «Про Раду національної безпеки і оборони України», вирішила утворити Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України. З-поміж визначень, трактованих у Стратегії, виокремимо найбільш-актуальні для поточного дослідження:

- кібернетична безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі;
- кібернетичний простір – середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами автоматизованих, телекомунікаційних та інформаційно-телекомунікаційних систем.

Поділивши на два етапи процес реалізації Стратегії, домовлено протягом 2015-2016 рр. розробляти і вдосконалювати нормативно-правову базу, створювати підготовку спеціалізованих кадрів з протидії кіберзагрозам для сектору безпеки та критичної інформаційної інфраструктури держави та ін. За 2017–2018 рр. вирішено вдосконалювати міжнародні правила поведінки у кіберпросторі та міжнародну нормативно-

правову базу, відповідно до кібербезпекових викликів національній та міжнародній безпеці [3].

15 березня 2016 р. Президент України Петро Порошенко підписав Указ, згідно з яким ввів у дію рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України», разом з тим постановив затвердити «Стратегію кібербезпеки України» [5]. Відтак, Рада національної безпеки і оборони України вирішила створити Національний координаційний центр кібербезпеки (НКЦБ) як робочий орган РНБО. Указом Президента України «Про Національний координаційний центр кібербезпеки», було введено в дію запропонований центр. Вважаємо за необхідне виокремити принципові завдання НКЦБ:

1) слідкувати за даними про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

2) здійснювати системні заходи, спрямовані на посилення спроможностей суб'єктів сектору безпеки та оборони у боротьбі із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом, кіберзлочинністю, та у забезпеченні кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури;

3) координувати розгортання підрозділів кібербезпеки Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних органів спеціального призначення та приведення їх у готовність до виконання завдань в умовах особливого періоду, в умовах воєнного, надзвичайного стану і під час виникнення кризових ситуацій, що загрожують національній безпеці України;

4) моніторити стан розроблення національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих зі стандартами ЄС та НАТО тощо [4].

У сучасних країнах кожна площина державної безпеки дедалі більше узалежнюється від вільного перебігу інформації, від активностей комунікаційних систем, від телеінформаційних мереж, які стрімко розвиваються, від різновекторного перетворення даних тощо. При чому, залежність поширюється на військову сферу, господарську частину, на мас-медіа, на фінансову і транспортну частки державної діяльності, останнім часом – в більшій мірі й на транспортну інфраструктуру (електронні квитки, он-лайн розклад руху транспортних засобів) тощо.

З огляду на часові рамки, розрізняють безпосередні та опосередковані інформаційні атаки. Безпосередні напади характеризуються негайними наслідками (блокування послуг, модифікація і переказ фальсифікованої інформації). На практиці, для збільшення дієвості та стирання слідів кіберзлочину, застосовують атаки, відтерміновані в часі (вони безпосередньо чи опосередковано спрямовуються на ціль). Зовнішні або віддалені інформаційні напади, які здійснюються із системами з-поза простору атаки. Внутрішні ж напади відбуваються зсередини поля інформаційного ураження. Не залежно від вказаних видів та джерел інформаційних атак, спільним для груп кіберзлочинців є володіння достатніми знаннями та належним оснащенням, свідоме застосування нелегальних методик впливу.

Цілісне функціонування розвиненої держави нерозлучно пов’язане із запевненням непорушеної діяльності власних систем транслювання даних, управління і моніторингу. Первинні і вторинні загрози можуть стосуватися усіх державних суб’єктів та бути прерогативом їхньої діяльності, а при врахуванні постаті, масштабу і міжнародної дальності, становлять виклики і для теоретиків, і для практиків безпекової проблематики.

Проблеми інформаційної безпеки чітко показують, що охорона інформації є одним з найважливіших стратегічних завдань кожної держави щодо кіберпростору, оскільки нинішня модель економічно-розвинених

держав визнає інформацію одним із найцінніших засобів, ключем до успіху в політиці,бізнесі, у військовій справі.

Піддатливість інформаційних систем до нападів спричиняє те, що негативний вплив деяких учасників кіберпростору залишається ефективною формою залякування, виманювання та здійснення тиску на державні урядові структури і на поза державні організації. Отже, важливо, щоб інституції, які значну частину власної бізнесової логістики переносять в мережу, уважно стежили за потенційними кіберзагрозами, оскільки цільовим призначення інформаційних атак є як державні установи, так і банки, Інтернет-магазини, аукціони, системи громадського управління, сфера надання послуг громадянам [13].

Трактуючи кіберпростір як віртуальне середовище, в якому відбувається комунікація між комп'ютерами, з'єднаними в одну мережу, А. Мєльніцкий підкреслює приналежність поняття «простір» конкретній території. Тобто учасники певних суспільних, політичних, економічних процесів знаходяться в спільному місці і в однаковий часових рамках, а завдяки безпосереднім контактам можуть ідентифікуватись навзаєм [14].

Різностороннє дотримання нормативних положень, провладний захист публічної та непублічної інформації сприятиме систематичному зростанню рівня національної безпеки, у тому числі й в просторах Інтернету. Розглянемо детальніше законодавчі акти й основні погляди на досліджувану проблематику Польської Республіки. В Урядовій Програмі Захисту Кіберпростору, кіберпростір виникає як цифровий простір перетворення і обміну інформації, створеної телеінформаційними системами і мережами, разом із співвідношенням між її споживачами. А поняття «кіберпростір Польської Республіки» стосується не лише польської території, але й місцевостей, де функціонують державні представники / представництва (дипломатичні установи, військові контингенти) [17].

Доктрина кібребезпеки Польської Республіки пояснює наступні причини недостатнього рівня безпеки в контексті ризикових ситуацій:

- непрецизійне визначення відповідальності за протидію виникненню кіберзагроз;
- поширені проблеми ризиків щодо недостатньої можливості здійснювати контроль за вихідними кодами у ситемах національної безпеки (мілітарної і позамілітарної), за системами технічної підтримки (особливо інонаціональних продуктів);
- джерела ризиків через недостатнє фінансування утворень, покликаних координувати та реагувати на комп'ютерні інциденти на державному рівні [9, с. 11-12,16].

Відносно зовнішнього виміру, у Доктрині, загрозами названо кіберкризи і кіберконфлікти за участю державних і недержавних суб'єктів. Кібервійну трактовано як сукупність гібридних конфліктних операцій в кібепросторі, що зазвичай становлять інтегральну частину класичних конфліктів та військово-політичних криз. Документ виділяє також істотну зовнішню загрозу, яка може мати серйозні наслідки у вигляді доступу до стратегічних державних даних – кібершпигунство, що здійснюється службами інших держав та недержавними суб'єктами. Як і в Стратегії кібербезпеки України, Доктрина виокремлює необхідну термінологію, показує шанси і ризики загроз кібербезпеці, зазначає цілі, способи та умови діяльності, спрямованої на гарантування безпечного функціонування держави як цілісності, що включає юридичних, ізичних осіб, підприємців та інших суб'єктів [9, с. 8-13].

Намагаючись випередити засоби оборони, методи негативного впливу постійно еволюціонують. Метою дотримання державної та національної безпеки повинне стати вдосконалення охоронних засобів, програмна і технічна підтримка критичної інфраструктури [18].

Часто цитованим прикладом успішної інформаційної атаки були події в Естонії у 2007 р. Ставши жертвою кібернападів, держава зазнала

впливу на вітрини www, тому усі види електронного банкінгу, поштові домени та інші суспільні потреби були заблокованими. Через рік після атаки, естонське Міністерство Оборони зазначило, що кіберзлочинці підірвали функціонування громадських і державних інформаційних систем [19; 7]. Аналогічно у Польщі в 2012 році жертвою кіберзлочинців стали урядові портали. В результаті чого, були тимчасово недоступні сервіси канцелярії Прем'єр-Міністра, Сейму та Міністерства культури. Додатковим ускладненням процесу протидії інформаційним атакам становили несвідомі користувачі Інтернету, які, почувши з медіа-джерел про бездіяльність певних сайтів, намагалися особисто перевірити достовірність новин. Таким чином, приватні мережеві користувачі вичерпали доступність серверів, які не були готові до таких насичених відвідувань. На щастя, згадувані кібератаки 2012 року не становили загрози для Польщі в цілому, однак сприяли усвідомленню владою необхідності дотримання кібернетичної безпеки у державі. Єдиним негативним наслідком нападів на польські урядові портали стало підірвання довіри частини суспільства до провладних органів [6].

Стосовно польської безпекової політики, на першому місці стоїть діяльність державної влади, урядів і коаліцій, функціональність якої полягає у: створенні пов'язаних законоположень у сфері національної безпеки; передбачення загроз безпеці держави і союзникам; формування необхідних умов для міжнародної співпраці і для можливості реалізації союзницьких зобов'язань в глобальній безпековій системі; охорону духовного і матеріального національного спадку; пошук нових методів діяльності, відповідно до сучасних викликів і загроз безпеці [16].

Висновки. Як і Польська Республіка, Україна прагне стати впливовим та технологічно-прогресуючим актором міжнародної арени у сфері захисту і обслуговування кіберпростору. Тому вдосконалення системи народної оборони інформаційного простору, підвищена

відповідальність щодо процесів обміну даними, всебічне навчання суспільства і фахова обізнаність кадрів дозволять здійснювати протидію ворожим інформаційним операціям та контрпереказу змістових потоків.

У випадку недостатньої оборони державної інформації, виникають загрози перехоплення даних, які мають критичну цінність для апарату керівництва військових формувань, організацій щодо хімічного та нуклеарного захисту країни. Відповідно, захист кібербезпеки повинен регулюватися на державному рівні, паралельно із політикою національної безпеки, поєднуючи процедури: телеінформаційної оборони, убезпечення баз даних від викриття, встановлення контролю на засобами масової комунікації.

Спільним для досліджуваних держав є вагомість теоретичного, методологічного, міжгалузевого удосконалення міжнародної діяльності, внутрішньо-політичної активності в контексті пануючих кібервикликів. Україна та Польща повинні регулярно вживати заходів, які гарантуватимуть необхідний рівень інформаційної захищеності, вірно конфігуруючи елементи безпекової структури – сервери, робочі станції, сенсори та аплікації. Окремої уваги (як на державному, так і на національному рівні) варті спеціалізовані комп'ютерні програми, що спроможні протидіяти невиправній діяльності хакерів. Вдосконалення: антивірусного програмного забезпечення, криптографічного кодування, аналізаторів мережевої активності, систем виявлення інформаційних зломів, постійне сканування слабких місць в оперативній пам'яті електронно-обчислювальних машин – ось мінімальний перелік необхідних дій провладних структур. Для інформаційної протидії ризикам і викликам кібербезпеки України та Польської Республіки, важливо також вводити в дію засоби автоматичного збереження даних, системи повторного копіювання контенту на надійні сервери. Захищене програмне забезпечення, внесення доцільних змін в організаційну, юридичну та фінансову сторону Інтернет-технологій, вдосконалення технічної

спроможності держави не лише зменшуватимуть потенційні кіберзагрози, але й підвищать довіру громадян до національної комунікаційної діяльності.

Список використаних джерел

1. Кочан І. Слова з компонентом кібер- у сучасній українській мові / І.Кочан // Вісник Львівського університету. – Серія філологічна. – Випуск 63, 2016. С. 277–285. – Режим доступу: nbuv.gov.ua/j-pdf/Vlnu_fil_2016_63_32.pdf.
2. Магда Є. В. Виклики гібридної війни: інформаційний вимір [Електронний ресурс] / Є.В.Магда. — 2014. — 5 с. — Режим доступу: irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Nzizvru_2014_5_29.pdf.
3. Про Стратегію кібербезпеки України : Рішення Ради Національної Безпеки і Оборони України від 27.01.16 р. – Електронний ресурс. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/n0003525-16/paran2#n2.
4. Указ Президента України № 242/2016 «Про Національний координаційний центр кібербезпеки». – Київ, 07.06.16 р. – Верховна Рада України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/242/2016.
5. Указ Президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». – Київ, 15.03.16 р. – Верховна Рада України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/96/2016#n11.
6. Biuletyn analityczny nr 2, Rządowe Centrum Bezpieczeństwa, http://rcb.gov.pl/wp-content/uploads/biuletyn/2.pdf, s. 7.

7. Cyber Security Strategy, Cyber Security Strategy Committee, Ministry od Defence, Estonia 2008.

8. Deterring hybrid warfare: a chance for NATO and the EU to work together? – Режим доступу: http://www.nato.int/docu/review/2014/also-in-2014/Deterring-hybrid-warfare/EN/index.htm.

9. Doktryna Cyberbezpieczeństwa RP.

10. Eco U., Środki masowego przekazu a przyszłość książki, [w:] Nowe media w komunikacji społecznej XX wieku, pod red. Maryli Hopfinger, Warszawa 2002, s. 531-532.

11. Głowacki A., Cyberprzestrzeń, „dePRESSJA" 2008, nr 1, s. 14.

12. Lichocki E., Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy, s. 2.

13. Majewski A., DDoS nasz powszedni, Atak i obrona 2013. Raport: Ataki i metody obrony w Internecie w Polsce, s. 24.

14. Melnitzky A., Defening America against Chinese cyber espionage trough the use of active defenses, „Cardozo Journal of International and Comparative Law", Vol. 20.2, Winter 2012, s. 554-556 [w:] red. A. Podraza, P. Potakowski, K. Wiak, Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, Difin, Warszawa 2013, s. 45.

15. Pikulicka-Wilczewska A., Sakwa R. Ukraine ana Russia: People, Politics, Propaganda and Perspectives, E-International Relations Publishing.

16. Pokruszyński W., Polityka a strategia bezpieczeństwa, Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi, Józefów 2011, s. 19-25.

17. Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016, http://bip.mswia.gov.pl.

18. Strategia Bezpieczeństwa Narodowego 2014, http://www.bbn.gov.pl/ftp/SBN%20RP.pdf, s. 17-18.

19. Terlikowski M., Bezpieczeństwo teleinformatyczne państwa, Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 107-108.

20. William Gibson (pisarz science fiction). – Wikipedia. https://pl.wikipedia.org/wiki/William_Gibson_(pisarz_science_fiction)

21. Włodarczyk T. Wojny w cyberprzestrzeni / T. Włodarczyk // Elektroniczny magazyn Computerworld. – 19.06.2012. – Режим доступу: http://www.computerworld.pl/news/383495/Wojny.w.cyberprzestrzeni.html.