sustainable development depend. At the same time, cyberattacks are becoming more and more unpredictable and sophisticated, which can cause damage to all segments of society at the national and international levels.
This article states that Brazil has a high rate of Internet use and is actively developing online services, although the level of cybersecurity leaves much to be desired. The current state and problems of development of Brazil cyberspace security are analyzed. Brazil‟s place in the global cybercrime scene has been studied, namely the types of crimes and their number, as well as their impact on economic, political and social stability in the country. The state of Brazilian cybersecurity legislation is described. The emphasis is on the problems of the industry. In particular, the concept of «fishing», which is the most common type of fraud in the Internet space in Brazil.
The article is based on the National Cyber Security Strategy of Brazil E-Cyber for the period 2020–2023, which was approved on February 5, 2020 by the President of the Republic Jair Messias Bolsonara. The emergence of this strategy is a significant step for Brazil towards creating a secure cyberspace and improving the information society. During the study, each item of the strategy was elaborated in detail and attention was paid to the steps proposed by the government of the republic for the development of the industry. Emphasis is placed on the need for a comprehensive vision and cooperation in the development of the industry by government agencies, business structures and society.
**Key words:** cybersecurity, information space, national security, cybersecurity strategy.

**REFERENCES**

1. Dobrozhanska, O. L., Demtsov A. A. (2011). Kiberbezpeka yak fenomen mizhnarodnykh vidnosyn na prykladi Federatyvnoi Respubliky Nimechchyny. *Aktualni problemy mizhnarodnykh vidnosyn,* 102, 111–116.
2. Vozniuk, E. (2017). Principles and features of Japan‟s information security system. *Політичне життя,* 4, 8–12.
3. Lukianchykova, V. Iu. (2013). Kiberprostir: zahrozy dlia mizhnarodnykh vidnosyn ta hlobalnoi bezpeky. *Hileia: naukovyi visnyk,* 72, 793–796.
4. 8 a cada 10 executivosjáenfrentaramfraudescibernéticas. URL: https://itforum365.com.br/8-cada-10-executivos-ja-enfrentaram-fraudes-ciberneticas/.
5. Internet organised crime threat assessment. *European Cyber crime Centre,* 2018. URL: https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf.
6. Relatórioda Segurança Digitalno Brasil. *DFNDR Lab.* 2018. URL: https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf.
7. Kovtun, L. Iu., Nechyporuk, I. V. (2015). Fishynh yak odna iz form shakhraistva v interneti. URL: http://www.legalactivity.com.ua/index.php?option=com_content&view=article&id=1075%3A2015-09-15-06-47-15&catid=131%3A5-0915&Itemid=161&lang=ru.
8. Estratégia Nacional de Segurança Cibernética. URL: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm.
9. CSO. UNITED STATES. URL: https://www.csoonline.com/article/3387981/stakes-of-security-especially-high-in-pharmaceutical-industry.html.

УДК 323.28:004](477:470+571)

**Вознюк Євгенія,**
кандидат політичних наук, доцент кафедри міжнародних відносин і регіональних студій
Східноєвропейського національного університету імені Лесі Українки, Луцьк, Україна.
Vozniukjane.vippo@gmail.com, Voznyuk.Yevhenija@eenu.edu.ua
https://orcid.org/0000-0002-7828-7430;
**Романцов Дмитро,**
студент факультету міжнародних відносин
Східноєвропейського національного університету імені Лесі Українки, Луцьк, Україна.
virtyalprofi@gmail.com, Romantsov.Dmytro@eenu.edu.ua;

**Рошко Іван,**
студент 4-го курсу факультету міжнародних відносин
Східноєвропейського національного університету імені Лесі Українки,
Луцьк,Україна.
Ivan.Roshko2016@eenu.edu.ua

# КІБЕРБЕЗПЕКА В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ

*Розглянуто втручання російських інформвійськ у внутрішню інформаційну систему не лише України, а й інших європейських держав. Висвітлено історичні та сучасні факти порушення російськими хакерами кіберпростору різних країн світу. Проаналізовано стан дотримання інформаційної безпеки на критичних об'єктах інфраструктури нашої держави, а також рівень розвитку законодавчого підгрунтя забезпечення кіберзахисту. Розкрито суть понять «кібербезпеки», «кіберзахисту», «кібератаки», «кібертероризму», «кіберзагрози».*

*Охарактеризовано діяльність Центру реагування на кіберзагрози України (CRC), а також запровадження зміни тактики сучасного кібірзахисту України проти російської агресії. Наголошено на частковій непристосованості та неефективній системі попередження й знешкодження кібератак.*

*Доведено, що у 2007 р. Естонія також стала об'єктом безпрецедентних кібератак на комп'ютерні системи державних установ, банків, поліції й навіть уряду, операції яких були практично паралізовані протягом декількох днів під час загострення російсько-естонських відносин. На думку деяких спостерігачів, ця кібератака на Естонію була однією з найкраще організованих і популярних в історії Інтернету. Окрім кібератак, цілі загальної дезінформаційної кампанії, що Кремль подає фейкові новини, роками поширюються на інші країни Балтії. Більшість російських телеканалів ефективно використовує підроблену інформацію для спотворення історичних подій та розпалювання етнічної ненависті та війни.*

*Акцентовано на частковій дезадаптації та неефективній системі профілактики й нейтралізації кібератак.*

***Ключові слова:*** *кібербезпека, кіберпростір, Україна, Російська Федерація, кібератака, інформаційна безпека.*

## 1. ВСТУП

**Актуальність теми дослідження.** Сучасні процеси, що відбуваються в інформаційній сфері, суттєво впливають на прискорення руху до вищої фази розвитку людства – інформаційного суспільства, у якому інформація стає надзвичайно цінною складовою частиною національного надбання, важливим економічним, політичним і військовим ресурсом. Це, зі свого боку, призвело до виникнення в умовах глобальної інформатизації та розвитку Інтернету, нових викликів і загроз, з‟явилася можливість вирішувати міждержавні конфлікти не силовими методами, а застосовуючи найсучасніші інформаційні технології. Тому, як ніколи гостро, перед кожною країною сьогодні постало питання забезпечення інформаційної безпеки, що набуває стратегічного значення.

**Постановка проблеми.** Особливо важко захистити кіберпростір завдяки низці факторів, таких як здатність зловмисників працювати з будь-якої точки світу та взаємозв‟язок між кіберпростором і фізичними системами. Оскільки інформаційні технології стають усе більш інтегрованими до операцій фізичної інфраструктури, існує підвищений ризик для широкомасштабних або наслідкових подій, які можуть спричинити шкоду або завдати збитків послугам, від яких залежать економіка й повсякденне життя мільйонів жителів. Кількість кібератак зростає з кожним роком. Лише в період із 2006 р. по 2015 р. цифра збільшилася з 5503 до 77 183 нападів.

**Аналіз досліджень і публікацій.** Питаннями інформаційної та кібербезпеки займалися як вітчизняні, так і зарубіжні вчені: В. Л. Бурячок, Н. І. Бусленко, О. Ю. Колєсов, В. А. Ліпкан, А. М. Митко, Н. П. Карпчук, а також Конах В. К., а особливо аналізуючи загрози та виклики національним інтересам України в інформаційній сфері в умовах глобалізації [6] й ін.

Потрібно зауважити, що у монографії «Міжнародна інформаційна безпека: сучасні виклики та загрози» Є. А. Макаренко [9] висвітлив такі питання, як стан і тенденції розвитку міжнародної системи підтримання миру в інформаційну добу, планування й проведення спеціальних інформаційних операцій, сутність і методи протидії маніпулятивним технологіям, прикладні аспекти інформаційної безпеки в різних сферах суспільного життя.

**Мета** роботи – аналіз стрімкого та всесвітнього розповсюдження кібератак, а також особливостей розвитку українського кіберзахисту в умовах російської агресії.

## 2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Відразу після референдуму щодо незалежності в провінції Індонезії в Східному Тіморі (1999 р.) громадська організація «East Tymor campaign» провела з територій Іспанії, Португалії й Франції перші масштабні атаки на державні Інтернет-сайти Індонезії, «завдяки» чому виявлено безліч уражених урядових ВЕБ-сторінок. Ці інформаційні операції, проведені з території Європи, були прямим застосуванням інформаційної зброї для виконання конкретних внутрішньополітичних завдань [7, с. 83].

Знову ж таки Інтернет-сайти стали ще одним великим і невидимим полем бою за «незалежну Ічкерію» проти «російських пригноблювачів». Усьому світу відразу стали доступні матеріали про «реальну» ситуацію на Північному Кавказі.

Такий хід подій кардинально вплинув на зміну позицій більшості країн світу, що з‟ясувалося на семінарі з проблем інформаційної безпеки, який організовано Інститутом ООН із проблем роззброєння (ЮНІДІР) і Департаментом із питань роззброєння в серпні 1999 р. в Женеві. У семінарі взяли участь представники близько 50 країн, уключаючи всіх основних гравців тогочасного інформаційно-технологічного поля [8, с. 41]. На зустрічі визнано актуальність проблеми інформаційної й техногенної безпеки, незважаючи на те, що вироблявся підхід, який зводився до ігнорування проблеми як комплексної й виокремленню з неї лише кримінальної та терористичної складових частин. При цьому можливість створення інформаційної зброї й загроза виникнення інформаційних війн або взагалі не визнавалась, або визнавалася як гіпотетична та відводилася на задній план.

На 54-й сесії Генеральної Асамблеї Організації Об‟єднаних Націй серед документів, котрі мають глибокі політичні наслідки, якщо думати про дипломатію й стратегічну стабільність XXI ст., відбулося прийняття резолюції 54/49 «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки». Світове Співтовариство визнало міжнародну інформаційну безпеку як глобальну проблему і як необхідну умову існування людського суспільства в пост‟ядерний вік[8].

Інформаційна безпека, як відомо, складається з двох рівноцінно важливих частин – власне інформаційної (тобто контенту) та кібербезпеки. По-новому оцінити стан кібербезпеки керівництво Української держави змусили кібератаки в грудні 2015 та 2016 рр., особливо остання – із використанням вірусу-здирника NotPetya, котрий у червні 2017 р. заразив сотні тисяч комп‟ютерів по всьому світу.

Після офіційних заяв із цього приводу українського Уряду, Служби безпеки України в лютому 2018 р. прозвучала низка гучних заяв урядів Сполучених Штатів Америки, Австралії, інших країн, у яких також відверто вказується, що власне військові хакери Росії здійснили кібератаку NotPetya проти України. Зокрема, заступник Міністра закордонних справ Великобританії Тарік Ахмад від імені уряду своєї країни заявив, що відповідальність за цю руйнівну кібератаку «несе російська влада, а саме російська армія» [1].

У Доктрині інформаційної безпеки Російської Федерації термін «інформаційна безпека» використовується в надто широкому змісті. Мається на увазі стан захищеності національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства й держави загалом [4]. І це не безпідставно. Як відомо, 22 лютого 2017 р. Міністерство оборони Російської Федерації оголосило про створення військ інформаційних операцій. Це, безумовно, аж ніяк не створення нових, а легалізація вже давно наявних підрозділів, які володіють достатнім досвідом проведення кібератак і ведення інформаційних війн. Це вони у квітні-травні 2007 р. таким чином атакували Естонію.

Ще на початку XXI ст. ця країна до пріоритетів державної політики віднесла амбітну ціль – стати флагманом Європи у сфері ІТ. А сьогодні серед країн Центрально-Східної Європи – членів ЄС вона по праву займає провідні позиції. Потрібно зазначити, що з перших днів утілення в життя цієї мети стало зрозуміло: навіть маючи певні напрацювання, очевидні здобутки, шлях до цілі буде нелегким і супроводжуватиметься додатковими ризиками. Адже державне управління, засоби масової інформації, приватні підприємства стають сьогодні все більш залежними від безпеки в Інтернет-середовищі.

У 2007 р. згадані ризики перетворились у реальну загрозу. Естонія стала тоді мішенню безпрецедентної кібератаки на комп‟ютерні системи державних установ, банків, поліції й навіть уряду, робота яких була практично паралізована впродовж кількох днів. Кібератаки продовжувалися з 28 квітня по 9 травня під час загострення російсько-естонських відносин, пов‟язаних із перенесенням із центру столиці на околицю так званого «бронзового солдата» – монумента полеглим у Другій світовій війні, а водночас і розміщеної поряд братської могили загиблих у ній радянських солдатів.

Росія діяла тоді відразу на двох фронтах: зуміла ще й вивести на вулиці Таллінна сотні демонстрантів, котрі піддалися її інформаційним атакам. Серед них були й такі, що навмисно приїхали з Росії допомагати місцевим, звинувачувати владу у «фашизмі» та «нарузі» над пам‟яттю жертв війни.

Ця кібератака на Естонію, на думку деяких оглядачів, була однією з найкраще організованих і масових в історії Інтернету. Але країна була готовою до захисту свого інформаційного простору, вибудувавши напередодні ефективну державну політику у сфері інформаційної безпеки, що звела до мінімуму фінансово-економічні збитки від цієї атаки.

Окрім кібератак, цілі кампанії дезінформації, фейкових новин із Кремлівської подачі роками поширюються і в інших Балтійських країнах. Яскравий приклад – Інтернет і його новинний портал Sputnik News, який від 2016 р. доступний, зокрема, і трьома балтійськими мовами. Він намагається порушувати теми, що випали з поля зору традиційних ЗМІ. І варто зазначити, інколи успішно знаходить своїх читачів, передусім із-поміж молодого покоління населення країн Балтії, зокрема й тих, хто не говорить російською.

Більшість російських телеканалів задля викривленого зображення історичних подій для підбурювання до міжнаціональної ненависті й війни ефективно використовують фейкову інформацію. Проте для боротьби з дезінформацією на телебаченні лише в Естонії створено телеканал, націлений на 330-тисячну російськомовну меншину.

Упровадженням політики Естонії в галузі інформаційної безпеки займається Міністерство економіки та комунікацій, зокрема два його структурні підрозділи – Департамент державної інформаційної системи та Естонський центр інформатики.

В Естонії також досить успішно функціонує низка неурядових організацій, які роблять свій внесок у зміцнення інформаційної безпеки держави. Серед них – Фонд Look@World та Центр сертифікації.

Сьогодні Естонія напрацювала значний досвід у видачі сертифікатів на аудентифікацію й електронний підпис для ID-карток, якою займається єдина в країні установа – Центр сертифікації. Уже понад 10 років Інтернет-користувачі цієї держави мають змогу звертатися за послугами до Комп‟ютерної групи швидкого реагування, яка, за необхідності надає їм допомогу в здійснені превентивних заходів, котрі значно зменшують заподіяну шкоду при кіберзагрозі або відразу реагують на неї.

Чи не найбільше заслуговує на увагу тісна співпраця Естонії з НАТО в галузі кібербезпеки. У Таллінні розміщено об‟єднаний центр передових технологій із кібероборони НАТО, який, починаючи з 2010 р., щорічно проводить в Естонії найбільші у світі навчання з кіберзахисту LockedShields. У квітні 2017 р. в них узяли участь близько 800 учасників із 25 країн світу – це ІТ-фахівці, політичні та юридичні консультанти з держав-членів НАТО і країн-партнерів Альянсу. Згодом кібернавчання під назвою EU CYBRID 2017 проведено в Таллінні й для міністрів оборони країн-членів ЄС.

З огляду на недосконалу систему попередження кібератак, російські інформвійська зуміли завдати відчутного удару по репутації нашої держави – серйозно вплинули на громадську думку в Нідерландах напередодні проведення там референдуму щодо асоціації України і ЄС. Ефіри цієї держави заповнено тоді проросійськими експертами з економічних питань, політичними оглядачами, соцмережі – ботами, а Russia Today запопадливо відпрацьовувала виділені їй російською владою мільярди. Як результат, громадяни Нідерландів у квітні 2016 р. не підтримали угоду про Асоціацію України з ЄС. Потрібно зазначити, що уряд цієї країни офіційно визнав, що Росія впливала на громадську думку напередодні референдуму, і зробив цілком закономірні висновки.

У червні 2017 р. росіяни, порушивши кіберпростір десятків країн світу, переважно в Україні «шліфували» свої злочинні вміння й навички ведення одного з елементів гібридної війни. Кібератака була лише обставлена як вимагання, однак справжньою метою вірусу було не отримання викупу, а порушення роботи українських держустанов, фінансового й енергетичного секторів економіки.

Загалом наша держава зазнала величезних збитків (найбільше із шістдесяти чотирьох країн, які піддавалися цій кібератаці), недоотримавши 0,4 % ВВП, що становило близько 10 млрд грн.

До таких утрат, як стверджують окремі вітчизняні аналітики, Україну призвела відсутність на той час дієвої системи кіберзахисту, зокрема її законодавчого підґрунтя. Так, на думку колишнього голови парламентського комітету із питань інформатизації та зв‟язку Олександра Івановича Данченка, «країна виявилась неготовою до нападу, причому не готова вже втретє чи вчетверте. Координація між службами відсутня, приватний бізнес взагалі не долучений до системи захисту і ніяк не співпрацює із державними органами» [12].

Певною мірою з політиком можна погодитися. Наприклад, базовий для цієї сфери Закон України «Про основні засади забезпечення кібербезпеки України» готувався, розглядався та вдосконалювався роками. Ще у 2015 р. група народних депутатів із комітету інформатизації та зв‟язку подала в Секретаріат Верховної Ради підготовлений нею законопроект. Коли ж лише в червні 2017 р. він був переведений на повторне друге читання, у цілому ж цей Закон 257-а голосами «за» був ухвалений лише 5 жовтня 2017 р., а чинності він набирає 9 травня 2018 р. [11].

Закон започаткував формування належної нормативної бази і є надзвичайно важливим із погляду створення системи кібербезпеки Української держави. До того часу це питання в країні регулювали лише три Укази Президента, одним із яких 15 березня 2016 р. була затверджена Стратегія кібербезпеки України, а також окремі рішення Ради національної безпеки і оборони (РНБО).

Насамперед, важливим у законі є те, що в ньому тлумачаться самі поняття «кібербезпеки», «кіберзахисту», «кібератаки», «кібертероризму» тощо, які під час оцінки вчинених у мережі злочинів уже десятиліттями використовуються в юридичній практиці, політиками та державними чиновниками, але досі так і не були закріплені в жодному офіційному документі:

«Кібератака» – спрямовані (навмисні) дії в кіберпросторі, які реалізовуються за допомогою засобів електронних комунікацій (уключаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби й обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) у комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного й штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів і засобів електронних комунікацій для здійснення кібератак на інші об‟єкти кіберзахисту;

– «кібербезпека» – захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національній безпеці України в кіберпросторі;

– «кіберзагроза» – наявні й потенційно можливі явища та чинники, що створюють небезпеку життєво важливим національним інтересам України в кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку й кіберзахист її об‟єктів;

– «кіберзахист» – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення й захист від кібератак, ліквідацію їх наслідків, відновлення сталості та надійності функціонування комунікаційних, технологічних систем;

– «кібертероризм» – терористична діяльність, що реалізовується в кіберпросторі або з його використанням [5].

Новий закон запроваджує ще й таке поняття, як Національна система кібербезпеки. Основними її суб‟єктами, що відповідають за гарантування кібербезпеки, визначені Держспецзв‟язок, нацполіція, СБУ, Міністерство оборони, генштаб ЗСУ, розвідка та НБУ. Первинне реагування на кіберінциденти закон покладає на створену ще у 2007 р. урядову команду реагування на комп‟ютерні надзвичайні події України CERT-UA. Ця структура, як відомо, діє при Державній службі спеціального зв‟язку та захисту.

CERT – центр реагування на кібератаки. Команда реагування на інциденти здійснює управління інцидентами інформаційної безпеки в межах своєї організації або в мережі. Її завдання – запобігати

нападам і підвищувати рівень обізнаності громадян, виявляти потенційні інциденти до фактичного відстеження й вирішувати вже наявні [14, с. 35].

Стабільність мережевих і інформаційних систем, а також безперервність основних послуг є важливими для належного функціонування внутрішнього ринку організації, до якої ми прагнемо вступити, зокрема, для подальшого розвитку єдиного цифрового ринку ЄС. Ця директива вимагає від усіх держав-членів Європейського Союзу створити «Комп‟ютерні групи реагування на надзвичайні ситуації» (CERT) і прийняти національні стратегії та плани співпраці. Запропонована директива як головне нововведення вимагає обов‟язкового повідомлення операторами ринку про інциденти, що мають істотний вплив на безпеку ключових послуг [10].

Поряд із відповідальними за гарантування кібербезпеки закон чітко визначає й об‟єкти захисту від кібератак. Під захист потрапляють комунікаційні системи, якими, зокрема, користуються органи влади та правопорядку, ресурси у сферах електронного урядування й комерції. Крім того, згідно із законом, захищеними мають бути «критично важливі об‟єкти інфраструктури» – це низка установ і підприємств у галузі енергетики, інфраструктури, банківського сектору, стратегічних підприємств, перелік яких затверджують Уряд та Національний банк.

Перевірка дотримання інформаційної безпеки на критичних об‟єктах інфраструктури здійснюватиметься за допомогою незалежного аудиту, що має проходити за стандартами ЄС і НАТО, котрі володіють сьогодні багаторічним досвідом його проведення. Це, безумовно, сприятиме тісній міжнародній співпраці України в інформаційній сфері.

У законі йдеться також про так звану «державно-приватну взаємодію» у сфері кібербезпеки. Документ зобов‟язує держустанови, підприємства й навіть окремих громадян сприяти органами держбезпеки, повідомляючи, наприклад, про кіберзагрози. Важливим у цьому законі є й те, що він запроваджує відповідальність, у тому числі й кримінальну, за злочин, учинений саме в кіберпросторі.

Закон України «Про основні засади забезпечення кібербезпеки», з одного боку, став законодавчим базисом для розробки та розгляду інших документів забезпечення як національної, так і інформаційної безпеки, а з іншого – сприяв створенню в умовах гібридної війни реальних механізмів інформаційного та кіберзахисту в дуже стислі терміни.

Останнім часом значно активізувалася Служба безпеки України у сфері боротьби з кібератаками та кіберзагрозами. У 2017 р. її фахівці відбили близько 50 кібератак різного ступеня ураження, а окремі з них могли бути небезпечнішими за «NotPetya». Основний напрям хакерських кібератак, які, без сумніву, мали російське походження, спрямовано на системи та об‟єкти критичної інфраструктури нашої країни, урядові й банківські установи. Однією з найбільших кібератак була WannaCry (також відома як WCry, WCrypt, WannaCrypt, WNCRY і WanaCrypt0r) – комп‟ютерний вірус, який уражає операційну систему Microsoft Windows за допомогою шифрування файлів. Вірус атакував урядові та бізнес-структури 12 травня 2017 р. Одним із перших зазнали нападу комп‟ютери Іспанії, пізніше вірус поширився й на інші країни. Станом на 17 червня 2017 р. заражено комп‟ютери в 150 державах світу і їх кількість невпинно зростала й перевищила 500 000 одиниць. Вимога переказувати гроші зловмисникам перекладена 28 мовами світу [14, с. 37]. Усе це є яскравим прикладом того, як треба створювати умови для фахівців, котрі, за необхідності, можуть захистити державу, зокрема її інформаційний простір.

26 січня 2018 р. в Києві відкрито Ситуаційний центр забезпечення кібернетичної безпеки, створений на базі Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ. Для організації роботи Центру в рамках виконання першого етапу Угоди про реалізацію Трастового фонду Україна-НАТО з питань кібербезпеки Служба отримала необхідне сучасне технічне обладнання й програмне забезпечення. Ключовими можливостями центру стануть система виявлення та реагування на кіберінциденти й лабораторія з комп‟ютерної криміналістики. Вони уможливлять ефективні превентивні заходи попередження та знешкодження потенційних кібератак, установлення розробників і їх походження, аналізу для вдосконалення майбутньої протидії та захисту тощо [3].

У лютому 2018 р. відкрито Центр реагування на кіберзагрози Держспецзв‟язку (Cyber Treat Response Centre, CRC). Його створено як центральний цілісний компонент і ядро національної системи кіберзахисту України. CRC організовано на основі останніх досягнень у сфері кібербезпеки як

вітчизняних, так і провідних ІТ-компаній світу, сучасні технологічні й аналітичні системи Центру розроблено на рівні найкращих світових аналогів й уже закономірно є одними з найбільш потужних у європейському співтоваристві.

CRC – це технічна платформа чіткої взаємодії основних суб"єктів забезпечення кібербезпеки (Держспецзв"язку, СБУ, Нацполіції), що на порядок підвищує ефективність та оперативність діяльності правоохоронних структур із протидії й розслідування кіберзлочинів. Це ефективний механізм координації зусиль усіх учасників кіберзахисту як державного, так і приватного секторів, що є однією з ключових ланок прийняття оперативних рішень Національним центром кібербезпеки РНБО України [2].

Завдяки унікальним технологічним рішенням цього Центру Держспецзв"язок здатен із великою вірогідністю й точністю здійснювати в режимі «24/7» попереднє виявлення аномальних атак та потенційно небезпечних дій у системах і мережах, підключених до Інтернету в державі.

## 3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, у нашій країні почала кардинально змінюватися тактика кіберзахисту: від реакції на заподіяну від кібератак шкоду – до ефективних дій на випередження та максимальної локалізації можливих уражень. Роблячи сьогодні перші кроки в цьому напрямі держава має вивчити кращий досвід країн, які зуміли вийти переможцями в інформаційному протистоянні. Серед них чільне місце по праву займає Естонія.

Підсумовуючи, зазначимо, що в умовах відкритої російської агресії, нових військово-інформаційних викликів Україна, як ніколи, повинна бути готовою в законодавчому, науковому, технічному та військовому плані до забезпечення своєї інформаційної й кібербезпеки. Як свідчить практика, вони можуть бути реалізовані лише за умови узгодження та чіткої координації діяльності в цьому напрямі всіх силових відомств, інших органів і структур.

Володіючи значним внутрішнім потенціалом в особі фахівців інформаційної галузі, Україні потрібно вдосконалювати систему контролю за використанням власного інформаційного простору та поширювати розповсюдження українського контенту у світі, кардинально збільшуючи фінансові й матеріально-технічні можливості для цього.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Британія виділить Україні £9 млн на підтримку незалежних медіа URL: https://hromadske.ua/posts/ britaniya-vidi lit-ukrayini-pound9-mln-na-pidtrimku-nezalezhnih-media. 2019.18.09.
2. Відкриття Центру реагування на кіберзагрози. URL: https://cert.gov.ua/ news/25. 2019.04.09.
3. Голова СБУ відкрив Ситуаційний центр забезпечення кібернетичної безпеки. URL: https://ssu.gov.ua/ua/ news/1/category/21/view/4318.O4n8C7Vl.dpbs. 2019.13.08.
4. Доктрина информационной безопасности Российской Федерации. URL: www.russianenterpricesolutions. com/help/dib.html. 2019.18.09.
5. ЗАКОН УКРАЇНИ «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov. ua/laws/show/en/2163-19.
6. Конах В. К. Загрози та виклики національним інтересам України в інформаційній сфері в умовах глобалізації. *Стратегічні пріоритети.* 2014. № 2. С.73–78.
7. Крутских А. Информационный вызов безопасности на рубеже XXI века: [информационное оружие]. *Международная жизнь*. 1999. № 2. С. 82–84.
8. Крутских А., Федоров А. О международной информационной безопасности. *Международная жизнь*. 2000. № 2. С. 37–48.
9. Макаренко Є. А. Міжнародна інформаційна безпека: сучасні виклики та загрози. Київ: Центр вільної преси, 2006. 916 с.
10. Німецька кіберзлочинність. URL: http://www.dw.com/uk/%D1%838C/a-38555191. 2019.10.09.
11. Основні засади забезпечення кібербезпеки України. URL: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-osnovnye-principy-obespecheniya-kiberbezopasnosti-ukrainy.
12. Система кіберзахисту в нас відсутня». URL: https://hromadske.ua/posts/kaberataka-v-ukraini. 2019.10.09.

13. Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». URL: http://www.president.gov.ua/documents/962016-19836.
14. Voznyuk Yevhenija, Vetrov Kyrylo. Information Terrorism as a Modern Threat for Information Security of European States. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2019. №1(5). 152 с.

*Матеріал надійшов до редакції 04.10.2019 р.*

## CYBER SECURITY IN THE CONDITIONS OF THE RUSSIAN AGGRESSION

The interference of Russian information troops in the internal information system not only of Ukraine but also of other European states is considered. The historical and modern facts of cyber space violation of different countries of the world by Russian hackers are covered. The peculiarities of the adoption and implementation of the Law of Ukraine «On the Fundamental Principles of Cyber Security of Ukraine» are revealed.

The state of compliance with information security on critical infrastructure of our country is analyzed, as well as the level of legal basis for cyber defense development. The essence of the concepts of «cyber security», «cyber defense», «cyber attacks», «cyber terrorism», «cyber threat» are given.

It was emphasized that the cyber-attacks in December 2015 and 2016 made the Ukrainian government to assess the state of cyber security in a new way, especially the last one – with the use of the NotPetya virus. As a result – the creation of a government computer emergency response team of Ukraine – CERT-UA, which operates with the State Special Communications and Protection Service.

The activity of the Cyber Threat Response Center (CRC) is described, as well as the introduction of changes in the tactics of modern cyber defense of Ukraine against Russian aggression.

It is proved that in 2007 Estonia also became the target of unprecedented cyber-attacks on computer systems of state institutions, banks, police and even the government, which operations were practically paralyzed for several days during the aggravation of Russian-Estonian relations. According to some observers, this cyber attack on Estonia was one of the best organized and popular in the history of the Internet. In addition to cyber attacks, the goals of the general misinformation campaign, the Kremlin feed fake news, have spread to other Baltic countries for years. The vast majority of Russian TV channels make effective use of fake information to distort historical events and to incite ethnic hatred and war.

Emphasis is placed on the partial maladaptation and ineffective system of prevention and neutralization of cyber attacks.

**Key words:** cyber security, cyberspace, Ukraine, Russian Federation, cyber attack, information security.

### REFERENCES

1. Brytaniia vydilyt Ukraini £9 mln na pidtrymku nezalezhnykh media [Elektronnyi resurs]. Rezhym dostupu: https://hromadske.ua/posts/britaniya-vidi lit-ukrayini-pound9-mln-na-pidtrimku-nezalezhnih-media. 2019.18.09.
2. Vidkryttia Tsentru reahuvannia na kiberzahrozy. URL: https://cert.gov.ua/ news/25. 2019.04.09.
3. Holova SBU vidkryv Sytuatsiinyi tsentr zabezpechennia kibernetychnoi bezpeky. URL: https://ssu.gov.ua/ua/news/ 1/category/21/view/4318.O4n8C7Vl.dpbs. 2019.13.08.
4. Doktryna ynformatsyonnoi bezopasnosty Rossyiskoi Federatsyy. URL: www.russianenterpricesolutions.com/help/dib.html. 2019.18.09.
5. ZAKON UKRAINY «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy». URL: https://zakon.rada.gov.ua/ laws/show/en/2163-19.
6. Konakh, V. K. (2014). Zahrozy ta vyklyky natsionalnym interesam Ukrainy v informatsiinii sferi v umovakh hlobalizatsii. *Stratehichni priorytety,* 2, 73–78.
7. Krutskykh, A. (1999). Ynformatsyonnyi vyzov bezopasnosty na rubezhe XXI veka: [Ynformatsyonnoe oruzhye]. *Mezhdunarodnaia zhyzn,* 2. 82–84.
8. Krutskykh, A., Fedorov, A. (2000). O mezhdunarodnoi ynformatsyonnoi bezopasnosty. *Mezhdunarodnaia zhyzn,* 2, 37–48.
9. Makarenko, Ye. A. (2006). Mizhnarodna informatsiina bezpeka: suchasni vyklyky ta zahrozy. Kyiv: Tsentr vilnoi presy, 916 p.
10. Nimetska kiberzlochynnist. URL: http://www.dw.com/uk/%D1%838C/a-38555191. 2019.10.09.
11. Osnovni zasady zabezpechennia kiberbezpeky Ukrainy. URL: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-osnovnye-principy-obespecheniya-kiberbezopasnosti-ukrainy.
12. Systema kiberzakhystu v nas vidsutnia». URL: https://hromadske.ua/posts/kaberataka-v-ukraini. 2019.10.09.

13. Ukaz Prezydenta Ukrainy №96/2016 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy». URL: http://www.president.gov.ua/ documents/962016-19836.
14. Voznyuk, Yevhenija, Vetrov, Kyrylo (2019). Information Terrorism as a Modern Threat for Information Security of European States. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii*, 1(5), 152 p.

УДК 811

**Гулай Василь,**
професор, доктор політичних наук, завідувач кафедри міжнародної інформації,
Національний університет «Львівська політехніка»,
79013, Україна, Львів, пл. Св. Юра, 3, каб. 126;
e-mail: Vasyl.V.Hulai@LPNU.UA
http://orcid.org/0000-0002-7609-7967;
**Воробець Юлія,**
студентка 2 курсу магістратури ОНП «Міжнародна інформація»,
Національний університет «Львівська політехніка»,
79013, Україна, Львів, пл. Св. Юра, 3, каб. 126;
e-mail: Yuliia.Vorobets.MnMV.2018@lpnu.ua
https://orcid.org/0000-0002-5100-3848

# TELEGRAM-КАНАЛИ ЯК ІНСТРУМЕНТ МАНІПУЛЯТИВНОГО ВПЛИВУ НА ФОРМУВАННЯ ГРОМАДСЬКОЇ ДУМКИ (НА ПРИКЛАДІ УКРАЇНИ ТА РОСІЇ)

*У вступі розкрито актуальність теми дослідження та сформульовано наукову проблему. Проаналізовано основні дослідження й публікації. Сформульовано мету та поставлено дослідницькі завдання роботи. Описано методику міждисциплінарного дослідження такого новітнього вища інформаційно-комунікативного простору, як Telegram-канали. Основну частину статті становлять результати власних досліджень авторів. Описано феномен Телеграм у Росії. Анонімність каналів Telegram серйозно ускладнює адміністративне та/або кримінальне переслідування проти їхніх авторів. Telegram став важливою платформою для трансляції різноманітної інформації, починаючи від чуток і відвертих міркувань щодо цілком достовірної інсайдерської інформації, уключаючи компрометуючі матеріали. Із появою каналів Telegram стали залучати специфічну аудиторію споживачів медіа-контенту, здебільшого зосереджуючись на постійному споживанні інформації в легкодоступній та стислій формі. Основну увагу звернуто на те, що для російської правлячої еліти Telegram – це ресурс, який дає їм змогу охопити важку, але дуже важливу частину населення, чого майже неможливо досягти, застосовуючи традиційні засоби масової інформації. ЗМІ, які посилаються на повідомлення в каналах Telegram, здебільшого є опозиційними або критично ставляться до правлячої влади в Росії (наприклад «Ехо Москви», «Медуза», «Нова газета»), меншою мірою використовують як альтернативне джерело отримання новин. На окрему увагу заслуговує український сегмент Telegram. Сформульовано такі висновки: по-перше, Telegram використовується як інформаційний канал для представлення офіційних думок; по-друге, українські ЗМІ застосовують Telegram як джерело інформації й ефективний засіб впливу на громадську думку шляхом маніпулювання через новини, витік інсайдерської інформації, чуток тощо; по-третє, Telegram використовується як канал вертикальної комунікації всередині самої політичної еліти, що має особливе значення у вертикалі влади та зважаючи на відсутність зворотного зв'язку, між політиками й громадянами; по-четверте, дослідження відомих анонімних каналів, які діють в Україні, підтвердили зв'язок із російською владою, що свідчить про задіяння російської пропаганди в Україні, здійснено задля дестабілізації суспільства, яке й так перебуває в стані війни з Росією. Отже, Telegram та його канали зберігатимуть важливу роль як найважливіший засіб політичної комунікації в найближчі роки, що здебільшого залишатиметься маніпулятивним інструментом, негативний вплив чого доведеться мінімізувати, бо остаточне виключення його видається нереальним.*

***Ключові слова:*** *Telegram, Telegram-канали, Україна, Росія, формування громадської думки.*