ISSN 2072–8670 (Print)
НАУКА І ПРАВООХОРОНА
NAUKA I PRAVOOKHORONA
DOI (Issue): https: //doi.org/10.36486/np.2020.1(47)
Issue 1(47) 2020

ІНФОРМАЦІЙНЕ ПРАВО. ПРАВО ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

УДК 659.4:005.056

Веселова Лілія Юріївна,
кандидат юридичних наук,
доцент, здобувач Одеського державного
університету внутрішніх справ,
м. Одеса, Україна
ORCID ID 0000-0001-6665-0426

АКТУАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ГЛОБАЛЬНОЇ КІБЕРНЕТИЧНОЇ ЗАГРОЗИ

У статті досліджені актуальні питання кібернетичної безпеки як загрози у глобальному кіберпросторі. Акцентовано, що технічний прогрес призвів до виникнення низки абсолютно нових неврегульованих правом суспільних відносин. Проаналізовано інформацію щодо нових атак у кібернетичній сфері та визначено головні тенденції розвитку кібернетичних загроз. Зауважено, що за останні роки збільшились кібернетичні атаки, метою яких є злам провідних систем захисту і створення загрози національній інфраструктурі. Підсумовано, що кіберзлочини характеризуються високою латентністю; складністю виявлення, розслідування та доказування, мають транснаціональну складову та наносять великі збитки.

***Ключові слова**: кіберпростір, кіберзлочини, загрози, безпека, глобалізація, кібернетичні загрози, інформаційний простір.*

Провідне місце у сфері забезпечення державної безпеки займають питання її інформаційної складової. Тому забезпечення інформаційної безпеки в країні є вкрай актуальним та об'єктивно важливим, особливо щодо розуміння реалізації державної політики, спрямованої на протидію кібернетичним загрозам.

Метою цієї статті є дослідження проблематики інформаційної безпеки з акцентом на визначенні тенденцій поширення кібернетичних загроз.

Питання, пов'язані з інформаційною безпекою, а також протидією кібернетичним загрозам набули великої актуальності та перебувають у центрі суспільної уваги. Водночас вагомий науковий внесок у зазначеній сфері зробили відомі вчені: О.А. Баранов, В.М. Семенов, О.О. Гиркін М.М. Безкоровайний, В.М. Бутузов, О.Є. Користін, Д.Й. Никифорчук, Ю.Ю. Орлов, Ю.М. Оніщенко, А.Л. Татузов, О.О. Черноног та інші науковці. Разом з тим, напрацювання у сфері інформаційної безпеки нададуть можливість більш результативнішого та дієвого аналізу кібербезпеки, що, у свою чергу, згенерує масив знань для формування обґрунтованої та ефективної державної політики щодо протидії кібернетичним загрозам.

DOI (Article): https: //doi.org/10.36486/np.2020.1(47).35

Зростання сучасного суспільства нерозривно пов'язане із запобіганням різноманітним загрозам, які посилюються в період реформування будь-якої сфери життєдіяльності суспільства [1]. Професор Олександр Користін зазначає, що питання протидії гібридним загрозам, зокрема, інформаційним та кібернетичним, достатньо широко та комплексно охоплює проблеми національної безпеки. Зазначене, перш за все, потребує суттєвого аналізу ситуації, дослідження тих факторів, що спричинюють неспроможність ефективного реагування на протидію гібридним загрозам, зокрема у сферах громадської безпеки та цивільного захисту. Поряд з цим, об'єктивність та обґрунтованість результатів дослідження потребує відповідної методологічної бази, прийнятності даних, що використовуються в аналізі, та джерел, з яких вони надходять [2; 3].

Глобалізаційні та інтеграційні процеси, швидкі технологічні зміни дають можливість усвідомити, що сучасне інформаційне суспільство охоплює всі сфери життєдіяльності людини і держави, а кіберсфера стала важливим економічним, політичним і соціальним ресурсом [4, с. 28]. Проте, поставивши собі на службу сучасні надбання кіберсфери, суспільство не передбачало, які можливості для зловживання створюють ці технології. Саме з початку використання Інтернет-технологій виник особливий клас загроз національній безпеці. Однак, як зазначає О.А. Баранов, широких масштабів проблема кібербезпеки набула тоді, коли можлива шкода від реалізації загроз у сферах, де використовувались комп'ютерні системи та телекомунікаційні мережі, стала досягати великих обсягів [5, с. 133]. А отже, слід ураховувати, що процес глобалізації інформаційних процесів має зворотній негативний бік, який має пряме відношення до процесів зростання кіберзлочинності.

Зростання залежності людини, суспільства та національних інфраструктур (енергетичної, транспортної, телекомунікаційної) від належної роботи інформаційно-телекомунікаційних систем зумовлює їх уразливість від кібернетичних загроз, що, у свою чергу, підвищує ризик виникнення надзвичайних ситуацій, створює реальні загрози життєдіяльності людини, суспільства, держави, подальшому соціально-економічному розвитку та національній безпеці України [6, с. 299].

У Стратегії забезпечення кібернетичної безпеки України зазначено, що побудова інформаційного суспільства в різних країнах світу, глобалізація інформаційних процесів, суттєве зростання ролі інформаційної інфраструктури в різних сферах суспільного життя з одного боку створюють підґрунтя для ефективного соціально-економічного розвитку держав, задоволення конституційного права особи на інформацію, побудови ефективної системи державного управління. З іншого, – сучасні інформаційні технології, перетворюють інформаційні системи урядового, оборонного, виробничого, кредитно-банківського, комунального та інших секторів на надзвичайно вразливі для реалізації кібернетичних загроз об'єкти [7].

При цьому безпека тисячі користувачів може виявитися залежною від декількох злочинців. Простота, легкість, анонімність, доступність і заощадження часу – якості, що роблять інформаційні технології привабливими для людства, – не могли не притягнути до себе уваги осіб, що здійснюють протиправну діяльність. Зі зростанням використання інформаційних технологій у різних сферах діяльності людини зростає і використання їх з метою вчинення кіберзлочинів.

Як зазначають О.В. Орлов та Ю.М. Онищенко, кіберзлочинність є неминучим наслідком глобалізації інформаційних процесів. Жертвами кіберзлочинців можуть стати не лише окремі особи або підприємства, але й цілі держави, що, безперечно, є загрозою національній безпеці [8]. В.М. Семенов та О.О. Гиркіна слушно зауважують, що сучасні інформаційні технології перетворюють інформаційні системи урядового, оборонного, виробничого, кредитно-банківського, комунального та інших секторів на надзвичайно вразливі для реалізації кібернетичних загроз об'єкти [9, с. 235].

У сучасному світі прогрес неможливий без цифрового інфраструктурного базису – ключового компоненту економічного розвитку. Реальною є сучасна залежність людини та суспільства у цілому від кіберпростору, що охоплює прилади, обладнання, програмне забезпечення, комп'ютерну техніку, телефонію, які є невід'ємною складовою сучасної повсякденної життєдіяльності. Це телекомунікаційні мережі урядової, виробничої та соціальної сфер, секретні військові та розвідувальні мережі, відкритий Інтернет, локальні мережі окремих суб'єктів, інші масові мережі, які пов'язали людей, громади, підприємства та суспільства. Саме реальність кіберпростору і робить реальними ризики, які виникли разом із ним.

У цьому і є іронія інформаційного епохи – технології, що формують можливості для розвитку, створюють плацдарм для прояву негативних процесів, несанкціонованого втручання в інформаційні системи тощо. США як одна з найбільш інформаційно розвинених країн одна з перших зіткнулися з проблемою забезпечення недоторканості приватного життя та економічної безпеки держави й громадян. За даними дослідження, тільки за два роки кіберзлочинність вартувала американцям 8 млрд доларів [10, с. 16]. У серпні – жовтні 2008 року хакери отримали доступ до електронної пошти і низки файлів передвиборної кампанії Барака Обами, включаючи документи, що розкривають політичні позиції та плани поїздок [10, с. 16]. За оцінками фахівців, лише упродовж року, у глобальному вимірі, кіберзлочини завдають збитків на суму до $ 1 трлн власникам інтелектуальної власності [11]. Економічне процвітання будь-якого суспільства в XXI сторіччі залежатиме від кібербезпеки.

Сполучені Штати Америки, як і більшість країн Заходу, зіткнулися з необхідністю забезпечення інформаційної безпеки особи, суспільства та держави, зокрема, і за допомогою адміністративно-правових засобів, що спричинено технічним прогресом у сфері телекомунікацій та інформаційних технологій, який призвів до виникнення низки абсолютно нових неврегульованих правом суспільних відносин.

З метою інституційного забезпечення у травні 2009 року при федеральному уряді США була створена Єдина Рада з національної безпеки, однією з основних функцій якої є моніторинг реалізації політики кібербезпеки. У Білому Домі створено також новий відділ, яким керує Координатор з кібербезпеки, що підпорядковується безпосередньо Президенту [12]. У межах своїх повноважень Координатор є відповідальним за інтеграцію і злагоджену роботу усіх складових державного управління у сфері кібербезпеки, за співпрацю офісу адміністрації Президента та за координацію дій у випадку настання надзвичайної події або кібератаки.

У своїй доповіді від 29 травня 2009 року Обама визначив п'ять головних напрямів діяльності, зокрема: розробка нової стратегії забезпечення безпеки

інформаційно-телекомунікаційних мереж Америки; налагодження взаємодії державних та місцевих органів влади з метою забезпечення організованої відповіді на кібератаки; зміцнення співробітництва державного та приватного секторів, оскільки переважна кількість найважливіших інформаційних інфраструктур у США перебуває у власності або управляється приватним сектором; запровадження національної пропагандистської кампанії з метою поширення серед населення інформованості та грамотності у сфері цифрових технологій [13].

У січні 2010 року під час Всесвітнього економічного форуму в Давосі глава компанії-розробника антивірусних програм McAfee Дейв ді Велт сповістив учасників про початок епохи "гонки озброєнь" у кіберпросторі. За його словами, останнім часом спостерігається рух державних комп'ютерних структур від традиційних оборонних стратегій до наступальних. Інтернет стає полем міжнародних бойових дій. Півтора-два десятки країн, серед яких Росія, США та Китай, готуються до можливих операцій в Інтернеті. Експерти вже закликають до активного публічного обговорення проблеми віртуальних воєн [14, с. 58].

Фахівці McAfee виявили ознаки застосування "кіберзброї" принаймні в п'яти країнах − США, Китай, Росія, Ізраїль та Франція. І цей список розширюватиметься. Ці дані були представлені ще восени 2009 року в черговій доповіді McAfee "Звіт про віртуальну злочинність" [15]. Спостерігається різке збільшення кількості хакерських атак в усьому світі. За підрахунками McAfee, за рік кількість нових шкідливих програм зросла на 500 %. Спостерігається підвищена увага світової громадськості до кібернетичної сфери. Це наочно демонструє, на думку ді Велта, недавній випадок із компанією Google, яка після хакерської атаки на поштовий сервіс заявила про намір припинити роботу в Китаї. Але це був лише один із багатьох подібних нападів за останні роки, більшість же з них були непомічені. Тим часом експерти попереджають, що в майбутньому кібератаки проти ключових об'єктів життєзабезпечення, які в більшості розвинених країн недостатньо захищені, можуть обернутися величезним збитком. Уже зараз, як показало дослідження McAfee, атаки хакерів обходяться в середньому в $ 6,3 млн на добу, тобто в $ 1,75 млрд на рік у всьому світі [16, с. 45]. Найдорожчі − напади на мережеву інфраструктуру нафтогазового сектора. Антивірусна компанія McAfee спільно з Центром стратегічних і міжнародних досліджень (CSIS) представила на Всесвітньому економічному форумі в Давосі звіт про результати дослідження, проведеного серед шестисот керівників нафтових і газових об'єктів, електростанцій та іншої критично важливої інфраструктури.

Зазначене підтверджується й іншими дослідженнями. У межах експертного опитування 54 % респондентів, які займають вищі ланки менеджмента підприємств, сповістили про наявні збитки від великомасштабних кібератак, що були у минулому. Окрім того, 37 % респондентів повідомили про те, що через скорочення корпоративних бюджетів ситуація з кібербезпекою погіршилася. А 40 % опитаних очікують великого інциденту в сфері кібернетичної безпеки. Середня величина збитків, спровокованих втручанням у роботу IT-систем, прогнозується в межах 6,3 мільйона доларів на день. Відповідальність за запобігання таким атакам 45 % опитаних покладають на регіональні або місцеві органи влади [17, с. 27].

Дослідницькі установи ООН також активно займаються оцінюванням інформаційної безпеки у глобальному світі. Зокрема, наявні аналітичні ініціативи

щодо можливості створення наступальних озброєнь для атак на інформаційні системи й мережі. На 55-й і 56-й Генеральних Асамблеях ООН були прийняті резолюції 55/63 і 56/121, що спрямовувалися на боротьбу з кримінальним використанням інформаційної інфраструктури. Зазначалося, що вразливості інформаційної інфраструктури збільшують можливість кібернетичних атак, і суспільство має бути готовим до цих технологічних викликів, а також, що це питання як стратегічної важливості, так і політичної волі, економічної та соціальної відповідальності [18]. Запобігання цим загрозам потребує узгоджених дій між націями та міжнародними об'єднаннями, а також між державним і приватним секторами.

У грудні 2003 р. 57-ма Генеральна Асамблея ООН прийняла резолюцію 57/239 "Створення глобальної культури кібербезпеки", за якою культура безпеки має формуватися у взаємодії державних і приватних учасників, включаючи розробників і користувачів ІТ, регуляторні й наглядові органи. Зазначено, що необхідним є усвідомлення існуючих ризиків при впровадженні ІТ в індустріальну, економічну, соціальну сфери, ідентифікація джерел загроз і об'єктів критичної інфраструктури, розробка методології оцінювання загроз та адекватності заходів захисту з урахуванням етичних і демократичних принципів, формування системи управління безпекою [18].

У грудні 2003 року 58-ма Генеральна Асамблея ООН прийняла резолюцію 58/199 щодо створення глобальної культури інформаційної безпеки та захисту критичної інформаційної інфраструктури [19], в якій підкреслюється взаємозалежність країн у зв'язку зі зростанням загроз та вразливості, наголошується на важливості залучення менш розвинутих країн у процес захисту критичної інформаційної інфраструктури шляхом надання методологічної і технологічної підтримки, використання найкращих принципів у цій сфері, наприклад, узгоджених на паризькій зустрічі 2003 року.

Національна безпека України, її економічне процвітання та соціальне благополуччя все більше залежать від доступності, цілісності та конфіденційності інформаційних ресурсів, що забезпечуються інформаційними та комунікаційними технологіями, або в більш широкому розумінні − кіберпростором. Водночас зростання залежності від інформаційно-комунікаційних технологій робить сучасне українське суспільство більш уразливим перед можливими негативними наслідками протиправного використання кіберпростору [7]. Тому актуальним є питання адміністративно-правового регулювання забезпечення та організації кібербезпеки як структурного елемента національної безпеки України.

Можна констатувати, що в Україні в повному обсязі присутні всі ключові "класичні" кіберзлочини і щороку їх кількість зростає [20]. Дослідження відомого німецького оператора зв'язку Deutsche Telecom підтверджують високий рівень загроз у кіберпросторі, у результаті якого Україна займає четверте місце у світі серед країн-джерел кібернетичних атак. Тільки протягом лютого 2013 р. з території України їх було здійснено 566 тисяч [21].

До головних тенденцій розвитку кібернетичних загроз відносять:

− зростання кількості кібернетичних атак, багато з яких призводять до великих втрат;

– зростання складності кібернетичних атак, які можуть включати кілька етапів і застосовувати спеціальні методи захисту від можливих методів протидії;

– вплив практично на всі електронні (цифрові) пристрої, серед яких останнім часом все більшого значення набувають мобільні пристрої, а вони найбільшою мірою схильні до ризиків у сфері кібербезпеки;

– усе частіші випадки нападу на інформаційну інфраструктуру великих корпорацій, найважливіших промислових об'єктів і навіть державних структур;

– застосування найбільш розвиненими у сфері комп'ютерних технологій країнами засобів і методів кібернетичних нападів на інші держави [22].

Це підтверджується практично щоденними зведеннями новин, у яких повідомляється про нові атаки в кібернетичній сфері. Так, наприклад, за останні роки збільшились кібернетичні атаки, метою яких є злам провідних систем захисту і створення загрози національній інфраструктурі (ймовірне джерело – Китай) [23]. У 2013 р. представниками Лабораторії Касперського було опубліковано інформацію про розкриття шпигунської мережі Red October, яка протягом п'яти років займалася розкраданням державних секретів. Це складний комплекс шкідливих програм (близько 1000 шкідливих файлів, що належать до 30 різних груп модулів) [24]. Аналогічні методи вже активно застосовуються і для мобільних пристроїв на платформі Android [25].

На початку 2014 р. було здійснено серію атак на найбільші американські ЗМІ, що змусило уряд США ще раз серйозно задуматися про посилення кібербезпеки у країні [26].

За оцінками Інтерполу, кількість кіберзлочинів зростає пропорційно кількості комп'ютерних мереж, а темпи зростання правопорушень та злочинів у кіберпросторі є найшвидшими на планеті. А отже, проблема правового та організаційного забезпечення кібербезпеки має безпосереднє відношення до обігу інформації, також і щодо забезпечення суб'єктів інформаційних відносин своєчасною, повною та достовірною інформацією, а крім того, до недопущення несанкціонованого використання і поширення інформації, порушення її цілісності та конфіденційності. Кіберзлочини характеризуються такими особливостями: високою латентністю; складністю їх виявлення та розслідування; складністю доказування за матеріалами кримінальних проваджень; транснаціональною складовою в основному з використанням інформаційної мережі Інтернет; високим збитком навіть від одиничного злочину.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Протидія відмиванню коштів: міжнародні стандарти, зарубіжний досвід, адміністративно-правові, кримінологічні, кримінально-правові, криміналістичні засади та система фінансового моніторингу в Україні: підручник. / за ред. О.Є. Користіна. Київ: Скіф, 2015. 984 с.

2. *Ковальчук Т.І., Користін О.Є., Свиридюк Н.П.* Гібридні загрози у секторі цивільної безпеки в Україні. *Наука і правоохорона*. 2019. № 3(45). С. 69–79.

3. *Kovalchuk T.I., Korystin O.Y., Sviridyuk N.P.* Hybrid threats in the civil security sector in Ukraine. Проблеми законності. 2019. Вип. 147. С. 163–175.

4. *Данильчук Л.О.* Сутність дефініції "інформація". Педагогіка і психологія професійної освіти. 2012. № 5. С. 28–32.

5. *Баранов О.А.* Про тлумачення та визначення поняття "кібербезпека". Правова інформатика. 2014. № 2(42). С. 132–138.

6. *Шеломенцев В.П.* Сутність організаційного забезпечення системи кібербезпеки України та напрями його удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. № 2(28). С. 299–309.

7. Стратегія забезпечення кібербезпеки України. Офіційний текст: проєкт Закону України. URL: w1.c1.rada.gov.ua/pls/.../webproc34?id (дата звернення: 20.12.2019).

8. *Орлов О.В.* Попередження кіберзлочинності – складова частина державної політики в Україні. Теорія та практика державного управління. Вип. 1(44). URL: www.irbis-nbuv.gov.ua/.../cgiirbis_64.exe*?* (дата звернення: 20.12.2019).

9. *Семенов В.М., Гиркіна О.О.* Сучасні аспекти забезпечення інформаційної безпеки України. Науковий вісник Херсонського державного університету: Серія "Юридичні науки". Вип. 5. Т. 2. С. 234–240.

10. AIG Technology Report 2007–2008: Readiness for the Networked World Center for International Development at Harvard University. March 2009. P. 14–18.

11. WIPO 2008 Report. WIPO Site. URL: http://www.wipo.int/meetings/en/archive.jsp (дата звернення: 20.12.2019).

12. Barack Obama Speech, March, 13, 2009. Barack Obama Site. URL: http://my.barackobama.com/ page/ content/ofasplashbsignon/ (дата звернення: 20.12.2019).

13. Remarks by the President on Securing our Nation's Cyber Infrastructure. White House Official Site. URL: http://www.whitehouse.gov/the_pressoffice/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (дата звернення: 20.12.2019).

14. *Тумарец В.* Новые угрозы для информационного общества. Москва: ЭКСМО, 2008. 288 с.

15. United Nations "Global E-Government Survey-2008". UN PAN Site. URL: http://www.unpan.org/egovkb/ global_reports/08report.htm (дата звернення: 20.12.2019).

16. *Прохожев А.А., Турко Н.И.* Основы информационной войны. Анализ систем на пороге XXI века: теория и практика. Москва, 1996. 388 с.

17. *Даниелова А.* Основные направления информатизации американского общества. США–Канада. 2009. № 5. С. 25–29.

18. Резолюция, принятая Генеральной Ассамблеей [по докладу Второго комитета (A/57/529/Add.3)] 57/239. Создание глобальной культуры кибербезопасности. URL: http://www.ifap.ru/ofdocs/un/57239.pdf (дата звернення: 20.12.2019).

19. UN General Assembly Resolution 58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures. 30 January 2004.

20. *Черноног О.О.* Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління. URL: http://mino.esrae.ru/178-1484 (дата звернення: 20.12.2019).

21. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2013 рік. URL: http://www. dknii. gov. ua/s ites/default/files/stan_informatyzacii_20132.pdf (дата звернення: 20.12.2019).

22. *Безкоровайний М.М., Татузов А.Л.* Кибербезопасность – подходы к определению понятия. URL: cyberleninka.ru/.../kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya (дата звернення: 20.12.2019).

23. Cyber Security news. URL: http://www.cybersecurity.ru/crypto/171331 .html (дата звернення: 20.12.2019).

24. Технология разоблачения Red October. URL: http://habrahabr.ru/company/kaspersky/blog/169839/ (дата звернення: 20.12.2019).

25. Киберопасность. URL: http://www.itsec.ru/keywords.php?keyword =15845&from=40#sthash.qnxYXcOZ. dpuf (дата звернення: 20.12.2019).

26. Cyber danger. URL: http://www.nytimes.com/2013/01/28/us/pentagon-to- beef-up-cybersecurity-force-to-counter-attacks.html (дата звернення: 20.12.2019).

REFERENCES

1. Protydiia vidmyvanniu koshtiv: mizhnarodni standarty, zarubizhnyi dosvid, administratyvno-pravovi, kryminolohichni, kryminalno-pravovi, kryminalistychni zasady ta systema finansovoho monitorynhu v Ukraini. "Anti-money laundering: international standards, foreign experience, administrative law, criminology, criminal law, forensic principles and the system of financial monitoring in Ukraine": a textbook / for ed. O.Ye. Korystin. Kyiv: Skif. 984 p. [in Ukrainian].

2. *Kovalchuk T.I., Koristin O.Ye., Sviridiuk N.P.* (2019). Hibridni zahrozy u sektory tsyvilnoi bezpeky v Ukrainy. "Hybrid threats in the civil security sector in Ukraine". Nauka I Pravookhorona. No. 3(45). P. 69–79 [in Ukrainian].

3. *Kovalchuk T.I., Korystin O.Ye., Sviridiuk N.P.* (2019) Hybrid threats in the civil security sector in Ukraine. Problemy zakonnosti. Iss. 147. P. 163–175 [in English].
4. *Danilchuk L.O.* (2012). Sutnist definitsii "informatsiia". "The essence of the definition of "information"". Pedahohika i psiholohiia profesiinoi osvity. No. 5. P. 28–32. [in Ukrainian].
5. *Baranov O.A.* (2014). Pro tlumachennia ta viznachennia poniattia "kiberbezpeka". "On the interpretation and definition of "cybersecurity"". Pravova informatika. No. 2(42). P. 132–138 [in Ukrainian].
6. *ShelomentsIev V.P.* (2012). Sutnist orhanizatsiinoho zabezpechennia sistemi kiberbezpeky Ukrainy ta napriami yoho udoskonalennia. "The essence of organizational support of the cybersecurity system of Ukraine and directions of its improvement". Borotba z orhanizovanoiu zlochinnistiu i koruptsiieiu (teoriia i praktyka). No. 2(28). P. 299–309 [in Ukrainian].
7. Stratehiia zabezpechennia kiberbezpeky Ukrainy. Ofitsiinyi tekst: proekt Zakonu Ukrainy. "Cybersecurity strategy of Ukraine". Official text: draft Law of Ukraine. URL: w1.c1.rada.gov.ua/pls/.../webproc34?id (date of application: 20.12.2019) [in Ukrainian].
8. *Orlov O.V.* Poperedzhennia kiberzlochynnosti – skladova chastyna derzhavnoi politiky v Ukraini. "Cybercrime prevention is an integral part of public policy in Ukraine." Teoriia ta praktyka derzhavnoho upravlinnia. Iss. 1 (44). URL: www.irbis-nbuv.gov.ua/.../cgiirbis_64.exe? (date of application: 20.12.2019) [in Ukrainian].
9. *Semenov V.M., Hirkina O.O.* Suchasni aspekty zabezpechennia Informatsiinoi bezpeky Ukrainy. "Modern aspects of information security of Ukraine". Scientific Bulletin of Kherson State University: Series: Yuridichni nauky. Iss. 5., Vol. 2. P. 234–240 [in Ukrainian].
10. AIG Technology Report 2007–2008: Readiness for the Networked World Center for International Development at Harvard University. March 2009. P. 14–18 [in English].
11. WIPO 2008 Report. WIPO Site. URL: http://www.wipo.int/meetings/en/archive.jsp (date of application: 20.12.2019) [in English].
12. Barack Obama Speech, March, 13, 2009. Barack Obama Site. URL: http://my.barackobama.com/ page/ content/ofasplashbsignon/ (date of application: 20.12.2019) [in English].
13. Remarks by the President on Securing our Nation's Cyber Infrastructure. White House Official Site. URL: http://www.whitehouse.gov/the_pressoffice/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (date of application: 20.12.2019) [in English].
14. *Tumarets V.* (2008). Novyie ugrozy dlia informatsionnogo obschestva. "New threats to the information society". Moscow: EKSMO. 288 p. [in Russian].
15. United Nations "Global E-Government Survey-2008". UN PAN Site. URL: http://www.unpan.org/egovkb/ global_reports/08report.htm (date of application: 20.12.2019) [in English].
16. *Prohozhev A.A., Turko N.I.* (1996). Osnovy informatsionnoi voiny. "The basics of information warfare". Analysis of systems on the threshold of the 21st century: theory and practice. Moskow. 388 p. [in Russian].
17. *Danielova A.* (2009). Osnovnyie napravleniia informatizatsii amerikanskogo obschestva. "The main directions of informatization of American society". USA – Canada. No. 5. P. 25–29 [in Russian].
18. Rezoliutsiia, priniataia Generalnoi Assambleei [po dokladu Vtorogo komitieta (A/57/529/Add.3)] 57/239. "Resolution adopted by the General Assembly [on the report of the Second Committee (A/57/529/Add. 3)] 57/239". Creating a global cybersecurity culture. URL: http://www.ifap.ru/ofdocs/un/57239.pdf (date of application: 20.12.2019) [in Russian].
19. UN General Assembly Resolution 58/199 (30 January 2004). Creation of a global culture of cybersecurity and the protection of critical information infrastructures [in English].
20. *Chernonoh O.O.* Napriamy pidvischennia efektivnosti zabezpechennia kiberbezpeky informatsiinykh tehnolohii v sistemi publichnoho upravlinnia. "Directions for improving the efficiency of cybersecurity of information technologies in the system of public administration". URL: http://mino.esrae.ru/178-1484 (date of application: 20.12.2019) [in Ukrainian].
21. Dopovid pro stan informatyzatsii ta rozvitok informatsiinoho suspilstva v Ukraini za 2013 rik. "Report on the state of informatization and development of the information society in Ukraine for 2013". URL: http://www. dknii. gov. ua/s ites/default/files/stan_informatyzacii_20132.pdf (date of application: 20.12.2019) [in Ukrainian].
22. *Bezkorovainyi M.M., Tatuzov A.L.* Kiberbezopasnost – podhody k opredeleniiu poniatiia. "Cybersecurity – approaches to the definition of a concept". URL: cyberleninka.ru/.../kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya (date of application: 20.12.2019) [in Russian].
23. Cyber Security news. URL: http://www.cybersecurity.ru/crypto/171331.html (date of application: 20.12.2019) [in English].

24. Tehnologiya razoblacheniya Red October. “Red October exposure technology”. URL: http://habrahabr.ru/company/kaspersky/blog/169839/ (date of application: 20.12.2019) [in Russian].
25. Kiberopasnost. “Cyberhazard”. URL: http://www.itsec.ru/keywords.php?keyword =15845&from= 40#sthash.qnxYXcOZ. dpuf (date of application: 20.12.2019) [in Russian].
26. Cyber danger. URL: http://www.nytimes.com/2013/01/28/us/pentagon-to- beef-up-cybersecurity-force-to-counter-attacks.html (date of application: 20.12.2019) [in English].

UDC 659.4:005.056

Veselova Liliia,
Candidate of Political Sciences, Associate Professor,
Applicant at the Odessa State University of Internal Affairs, Odesa, Ukraine
ORCID ID 0000-0001-6665-0426

APDATING OF INFORMATION SECURITY AND THE GLOBAL CYBERNETIC THREAT

The article focuses on research regarding cyber security as a threat in global cyberspace. It is emphasized that technological progress in telecommunications and information technologies has led to the emergence of a number of completely new unregulated social relations. According to this aspect, most States faced the need of ensuring information security of the individual, society and the State, primarily through administrative and legal means.

The questions of countering hybrid threats, in particular information and cyber threats, cover national security issues in a broad and comprehensive manner. Therefore, there is a need for a significant analysis of the situation, investigating the factors that cause failure to respond effectively and counter hybrid threats, in particular in the areas of public security and protection. However, the objectivity and validity of the research results requires an appropriate methodological basis, the acceptability of the data used in the analysis and the sources from which they are coming.

Analyzing information on new attacks in the area of cybernetics, the main trends in the development of cyber threats have been identified, and it has also been noted that in recent years there has been an increase in cyber attacks aimed at disrupting advanced systems of protection and threatening national infrastructure.

Particular emphasis is placed on the fact that today there is a pressing problem of legal and organizational cybersecurity. In this context, this is directly related to the circulation of information, ensuring that subjects of information relations are provided with timely, complete and accurate information, to prevent unauthorized use and dissemination of information, violating its integrity and confidentiality.

The article concludes that cybercrime is characterized by high latency; difficulty of detection and investigation; difficulty of proving from the materials of criminal proceedings; transnational component mainly using the Internet information network; high damage even from a single crime.

Keywords: cyberspace, cybercrime, threats, security, globalization, cyber threats, information space.

Отримано 18.02.2020