УДК 340.113:004.056(477)

DOI: 10.26565/2075-1834-2020-29-22

# КІБЕРНЕТИЧНІ ЗАГРОЗИ У КОНТЕКСТІ СУЧАСНОГО СПРИЙНЯТТЯ ЇХ В УКРАЇНІ

**Веселова Л. Ю.,**
кандидат юридичних наук,
здобувач Одеського державного університету
внутрішніх справ,
м. Одеса, 65000, вулиця Успенська, 1
e-mail: cvet-Liliya@ukr.net
orcid: https://orcid.org/0000-0001-6665-0426

**АНОТАЦІЯ:** у статті зосереджується увага на дослідженні безпеки у сфері кіберпростору, зокрема у контексті кібернетичної загрози. Акцентується, що за сучасних умов низка стратегічно важливих об'єктів економічного, інфраструктурного та оборонного секторів, що використовують інформаційно-телекомунікаційні системи, є потенційно об'єктами високого ризику через наслідки та їх рівень уразливості від зовнішнього вторгнення.

Наголошується на певній дискусійності серед дослідників щодо видів внутрішніх загроз. Акцентується увага на переконанні, що враховуючи навіть загальні методологічні підходи до оцінювання ризиків поширення загроз, зазначені фактори внутрішніх загроз, перш за все, є не загрозами, а факторами внутрішнього характеру, що сприяють поширенню кібернетичних загроз і можуть характеризуватися як спроможність системи протидіяти поширенню цих загроз, або як вразливість суспільства.

Особливий акцент зроблено на кіберзлочинності, яка є характерною не лише для України, а й для всього світового соціуму. Вказано, що Конвенція про кіберзлочинність достатньо узагальнено підійшла до класифікації кіберзлочинності, певним чином поза її увагою залишились діяння у кіберпросторі, які вочевидь заподіюють в тій чи іншій мірі значні збитки суб'єктам інформаційних відносин.

Зауважено, що особливим видом кіберзагрози у сучасних умовах є поширення кібертероризму, глобальний характер технічної бази якого та її доступність визначили особливі риси цього виду тероризму. Наголошено, що кібертероризм від кіберзлочинності відрізняється характерною особливістю – його відкритістю, коли умови терориста широко висвітлюються мас-медіа. Вирішення проблеми протидії кібертероризму ґрунтується на комплексному підході та має правову, організаційну, психологічну та технічну складові. Разом з тим, ключовою проблемою залишається правова регламентація використання кіберпростору, а також правові колізії та прогалини в законодавстві, наслідком чого є несвоєчасне і неадекватне реагування правоохоронних органів на факти заподіяння шкоди інформації, інформаційно-телекомунікаційним мережам, репутації громадян тощо.

**КЛЮЧОВІ СЛОВА:** кібернетична безпека, інформаційна безпека, кіберзагрози, кіберзлочини, кібертероризм, кіберпростір, інформаційний простір, мережа Інтернет.

# КИБЕРНЕТИЧЕСКИЕ УГРОЗЫ В КОНТЕКСТЕ СОВРЕМЕННОГО ВОСПРИЯТИЯ ИХ В УКРАИНЕ

**Веселова Л. Ю.,**
кандидат юридических наук,
соискатель Одесского государственного университета
внутренних дел,
г. Одесса, 65000, улица Успенская, 1
e-mail: cvet-Liliya@ukr.net
orcid: https://orcid.org/0000-0001-6665-0426

**АННОТАЦИЯ:** в статье концентрируется внимание на исследовании безопасности в сфере киберпространства, в частности в контексте кибернетической угрозы. Акцентируется, что в современных условиях ряд стратегически важных объектов экономического, инфраструктурного и оборонного секторов, использующих информационно-телекоммуникационные системы, есть потенциально объектами высокого риска из-за последствий и их уровня уязвимости от внешнего вторжения.

Отмечается определенная дискуссионность среди исследователей по видам угроз. Акцентируется внимание на убеждении, что, учитывая также общие методологические подходы к оценке рисков распространения угроз, указанные факторы угроз, прежде всего, являются не угрозами, а факторами внутреннего характера, которые способствуют распространению кибернетических угроз и могут характеризоваться как способность системы противодействовать распространению этих угроз или уязвимости общества.

Особый акцент сделан на киберпреступности, которая характерна не только для Украины, но и для всего мирового социума. Указано, что Конвенция о киберпреступности достаточно обобщенно подошла к классификации киберпреступности, определенным образом вне ее внимания остались действия в киберпространстве, которые явно причиняют в той или иной степени значительные убытки субъектам информационных отношений.

Обозначено, что особым видом киберугрозы в современных условиях является распространение кибертерроризма, глобальный характер технической базы которого и ее доступность определили особенные черты

этого вида терроризма. Отмечено, что кибертерроризм от киберпреступности отличается характерной особенностью – его открытостью, когда условия террориста широко освещаются СМИ. Решение проблемы противодействия кибертерроризма основывается на комплексном подходе и имеет правовую, организационную, психологическую и техническую составляющие. Вместе с тем, ключевой проблемой остается правовая регламентация использования киберпространства, а также правовые коллизии и пробелы в законодательстве, следствием чего является несвоевременное и неадекватное реагирование правоохранительных органов на факты причинения вреда информации, информационно-телекоммуникационным сетям, репутации граждан и др.

**КЛЮЧЕВЫЕ СЛОВА:** кибернетическая безопасность, информационная безопасность, киберугрозы, киберпреступления, кибертерроризм, киберпространство, информационное пространство, сеть Интернет.

## CYBER THREATS WITHIN THE CONTEXT OF CONTEMPORARY PERCEPTION OF THEM IN UKRAINE

**L. Veselova,**
PhD in Juridical Science,
Applicant for Odessa State University
of Internal Affairs,
Odessa, Assumption Street, 1
e-mail: cvet-Liliya@ukr.net
orcid: https://orcid.org/0000-0001-6665-0426

**ANNOTATION:** the article focuses on security research in cyberspace, in particular in the context of the cyber threat. It is emphasized that under current conditions a number of strategically important objects of economic, infrastructural and defense sectors using information and telecommunication systems are potentially objects of high risk due to consequences and their level of vulnerability to external invasion.

The article places emphasis on some discussion among researchers by type of threat. Attention is paid to the belief that, also taking into account the general methodological approaches to the assessment of risks of the proliferation of threats, these threat factors are primarily not threats, but internal factors that contribute to the spread of cyber threats and could be characterized as the ability of the system to counteract the proliferation of these threats or as vulnerability of society.

With this as a background of cybercrime, which is typical not only for Ukraine but for the whole world society. It has been pointed out that the Convention on Cybercrime has approached the classification of cybercrime in a rather generalized manner, and that certain actions in cyberspace which clearly cause significant losses to the subjects of information relations have been left out of its attention.

Under the contemporary conditions, a special type of cyber threat is the spread of cyberterrorism, the global nature of the technical base of which and its accessibility have determined the special features of this type of terrorism. It was noted that cyberterrorism from cybercrime differs by its openness, when the terrorist's demands are widely covered by the media. Solving the problem of combating cyberterrorism is based on a comprehensive approach and has legal, organizational, psychological and technical components. At the same time, the key problem remains the legal regulation of the use of cyberspace, as well as legal conflicts and gaps in legislation, resulting in an untimely and inadequate response by law enforcement agencies to damage to information, information and telecommunications networks, the reputation of citizens and so on.

**KEY WORDS:** cyber threats, cyberspace, cybercrime, cyberterrorism, cyberglobalization, national security, risk assessment.

---

**Постановка проблеми.** Сучасний еволюційний та прогресивний розвиток технологій дозволяє вирішувати широку низку завдань та проблем глобального світу. Поряд з цим, науково-технічний прогрес одночасно породжує й нові виклики та загрози в суспільстві, загалом, й у сфері кібернетичної безпеки, зокрема. У світі кібертероризм визнаний однією з першочергових проблем сьогодення. Кібертероризм є не тільки національною проблемою, він несе небезпеку для якісної роботи системи безпеки всіх країн світу.

**Актуальність.** За сучасних умов низка стратегічно важливих об’єктів економічного, інфраструктурного та оборонного секторів, що використовують інформаційно-телекомунікаційні системи, є потенційно об’єктами високого ризику через наслідки та їх рівень уразливості від зовнішнього вторгнення. Тому питання дослідження кібернетичних загроз займає одне з головних місць у системі забезпечення безпеки у сфері кіберпростору та є на сьогодні актуальним для нашої держави.

**Мета даної статті**: дослідити особливості забезпечення безпеки у кіберпросторі з огляду на те, що триває гібридна війна з високою активністю кібератак.

**Завдання.** Дослідити безпеку у сфері кіберпростору, зокрема у контексті кібернетичної загрози; розглянути напрацювання дослідників щодо видів внутрішніх загроз; розглянути проблему та шляхи протидії кібертероризму.

**Огляд праць з даної проблематики.** Розглядом проблем боротьби з кіберзлочинністю та кібертероризмом займалися такі науковці, як Довгань О.Д., Доронін І.М., Дубов Д.В., Голубєв В.О., Ожеван М.А., Хлань В.Г. та багато інших.

**Виклад основного матеріалу.** Серед дослідників поширено підхід кібернетичні загрози долучати до сфери інформаційної безпеки. Однак, на нашу думку, доречним є відокремлення кібернетичної безпеки від інформаційної, не дивлячись на цілком логічне узагальнення.

Аналізуючи дослідження зарубіжних та вітчизняних науковців, достатньо обґрунтованим є висновок, що до змісту інформаційної безпеки долучаються і проблеми щодо стану інформаційної безпеки у мережі Інтернет. Зазначене, є важливим як в цілому для держави, у контексті боротьби з інформаційними загрозами, кіберзлочинами, в тому числі кібертероризмом, так і для кожної людини щодо проблем захисту персональних даних, фінансових інструментів тощо.

З цього приводу, доречним є виділення, достатньо вдалого, визначення кіберпростору: особливий інформаційний простір зі специфічними просторово-часовими характеристиками (транскордоність, екстериторіальність, децентралізованість, розгалуженість, багатоканальність, віртуальність, імітаційність тощо); виник і функціонує за допомогою комп'ютерних та інших електронних пристроїв (мобільних засобів зв'язку, ігрових консолей, телевізійних пристроїв, супутників тощо), на базі інформаційно-телекомунікаційних мереж, переважно мережі Інтернет, в зв'язку з чим, як правило, володіє параметрами глобального інформаційного обсягу, яке виконує функції комунікації, розміщення і використання інформації, надання інформаційних та інших соціально значущих послуг, взаємодії інститутів державної влади, громадянського суспільства і окремої особистості, що є моделюючим фактором впливу на індивідуальну, групову і масову свідомість, соціально-політичну, економічну, духовну (культурну, релігійну, ідеологічну, наукову, освітню) та інші сфери життєдіяльності соціуму [1]. Саме тому, кібернетичний простір можна оцінювати як об'єкт захисту інформаційних ресурсів, апаратних і програмних засобів, так і як джерела загроз щодо інших об'єктів у системі безпеки суспільства.

Традиційно загрози, що виникають в кібернетичному просторі класифікують за характером спрямованості: на внутрішні, джерелом походження яких є вітчизняний інформаційний простір, або національний сегмент глобальної інформаційно-телекомунікаційної мережі, та зовнішні, поширення яких, пов'язане з характером глобальності мережі Інтернет. Поряд з тим, екстериторіальність Інтернету, значно ускладнює визначення конкретного джерела загрози, так як може ідентифікуватися за доменом в одній країні, а поширювати інформацію в іншій, не розкриваючи його, за допомогою використання пошукової системи, посилання тощо.

За таких умов, достатньо складним є завдання встановлення суб'єкта поширення шкідливої інформації. Зокрема, цей фактор є надзвичайно важливим з огляду на те, що необхідним є врахування сучасного стану кібернетичної безпеки в Україні, який характеризується як справжній театр бойових дій [1].

За сучасних умов низка стратегічно важливих об'єктів економічного, інфраструктурного та оборонного секторів, зокрема, підприємства енергетичної й атомної галузі, транспортування газу та нафти, обслуговування ліній електромереж, що використовують інформаційно-телекомунікаційні системи, є потенційно об'єктами високого ризику через наслідки та їх рівень уразливості від зовнішнього вторгнення. Зазначене підтверджується проведеним працівниками Державного науково-дослідного інституту МВС України дослідженням, за яким рівень загрози атаки на об'єкти атомної енергетики оцінюється як надзвичайний, але, перш за все, не за рахунок ймовірності такої атаки, яка є середньою, а за рахунок катастрофічних наслідків, що спричинює катастрофа на цих об'єктах [2; 14; 15].

Як джерело загрози кібернетичної і в цілому національної безпеки України і інших країн слід розглядати і фактичне регулювання США мережі Інтернет. Це обумовлено розташуванням на її території організацій (зокрема, інтернет-корпорації ICANN), що забезпечують управління доменними іменами верхнього рівня, тобто практично всім адресним простором DNS (доменної системи імен) у мережі Інтернет, що дозволяє називати США генеральним «утримувачем» доступу в мережу Інтернет.

Щодо внутрішніх загроз потрібно акцентувати увагу на певній дискусійності серед дослідників. Зокрема, у дослідженні [3, с. 29-30] до внутрішніх загроз віднесено:

– технічна залежність інформаційної інфраструктури України від іноземних технологій, включаючи безпосередньо мережу Інтернет;

– низький рівень захищеності інформаційно-телекомунікаційних систем від несанкціонованого доступу (під цим мається на увазі і вразливість програмно-апаратного обладнання, і наявність людського фактора, що виражається у витоку важливої інформації про паролі та коди доступу);

– низька якість нормативно-правових актів, що розробляються та їх невідповідність нинішній ситуації в інформаційній сфері й в цілому відсутність послідовної державної політики в галузі забезпечення кібернетичної безпеки;

– низький рівень комп'ютерної грамотності у населення та знань у сфері інформаційно-комунікаційних технологій;

– відсутність кваліфікованих фахівців, що володіють необхідними професійними якостями, відповідних організаційно-функціональних структур, здатних на підставі ввірених державою

повноважень здійснювати ефективну протидію розміщенню в кібернетичному просторі незаконної і небажаної (шкідливої) інформації;

– відсутність механізмів контролю та відповідальності учасників медіаспівтовариства мережі Інтернет, реєстраторів доменних імен, провайдерів, що функціонують в Інтернеті засобів масової інформації.

На наше глибоке переконання, враховуючи навіть загальні методологічні підходи до оцінювання ризиків поширення загроз, зазначені фактори, перш за все, є не загрозами, а факторами внутрішнього характеру, що сприяють поширенню кібернетичних загроз і можуть характеризуватися як спроможність системи протидіяти поширенню цих загроз, або як вразливість суспільства.

Окремої уваги заслуговує кібернетична загроза, яка може містити як екстериторіальні, так і внутрішні характеристики – кіберзлочинність. Це явище є характерним не лише для України, а й для всього світового соціуму. У Європейській конвенції про кіберзлочинність зроблено спробу нормативно закріпити і систематизувати правопорушення в кібернетичному просторі за такими видами [4]:

- фальсифікація з використанням комп'ютерних технологій;
- шахрайство з використанням комп'ютерних технологій;
- правопорушення, пов'язані з дитячою порнографією;
- правопорушення, пов'язані з порушенням авторських та суміжних прав.

Враховуючи те, що Конвенція про кіберзлочинність достатньо узагальнено підійшла до класифікації кіберзлочинності, певним чином поза її увагою залишились діяння у кіберпросторі, які вочевидь заподіюють в тій чи іншій мірі значні збитки суб'єктам інформаційних відносин. До них відносять:

- кіберсквотерство (придбання доменних імен з метою їх подальшого перепродажу або розміщення реклами);

- розсилку спаму;

- створення спеціальних наборів та інструментів для проведення хакерських атак, пошуку і використання вразливостей в інформаційних системах (при цьому більшість таких засобів не є шкідливим програмним забезпеченням);

- кібердифамація (від латинського diffamatio – паплюжити), тобто поширення за допомогою засобів масової інформації в мережі Інтернет неправдивих відомостей, що ганьблять честь, гідність, ділову репутацію, добре ім'я [3, с. 31].

Важливою обставиною, яка ускладнює проблему кіберзлочинності, обмежує спектр її поширення на протиправні діяння, є використання цього поняття лише стосовно сфери функціонування комп'ютерів і не враховування в якості кіберзлочину правопорушень, вчинених з використанням, наприклад, мобільних засобів зв'язку, зокрема, щодо поширення дитячої порнографії за допомогою стільникового зв'язку і шахрайства з оплатою послуг зв'язку. Більш обґрунтованим є підхід, який поділяє думку тих вчених та фахівців, які вважають, що кіберзлочини включають в себе «не тільки діяння, вчинені в глобальній мережі Інтернет, але і в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, техніка можуть виступати предметом злочинних посягань, середовищем, в якому вчинено правопорушення, і засобом або знаряддям злочину» [5].

Кіберзлочинність не обмежується межами злочинів, вчинених у глобальній мережі Інтернет. Вона поширюється на всі види злочинів, вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть бути предметом (метою) злочинних посягань, середовищем, в якому скоюються правопорушення, і засобом чи знаряддям злочину. Такий підхід є більш вдалим та більш обґрунтованим щодо сутності кібернетичного простору, що формується за рахунок усіх можливих локальних та глобальних інформаційно-телекомунікаційних мереж, хоча мережа Інтернет серед них є переважаючою.

Загалом, за певними характеристиками та ознаками щодо сфери поширення та впливу, кіберзлочини можуть характеризуватися як правопорушення економічного, політичного та дискримінаційного характеру, що проявляється у різних формах, зокрема, у формі незаконної політичної боротьби, вчинення шахрайства щодо фінансових операцій, тощо; у формі інформації, поширення якої потенційно є шкідливим так як стосується, наприклад, незаконної торгівлі зброєю, вибуховими речовинами, вибуховими пристроями, їх виготовлення, торгівлі людьми, людськими органами, наркотичними засобами, психотропними сильнодіючими речовинами, рецептами щодо їх виробництва тощо.

На нашу думку, особливим видом кіберзагрози у сучасних умовах є поширення кібертероризму. Одрі Курт Кронін [6] писав, що «ось уже років десять заколотники і терористи успішно використовують Інтернет для проведення своїх операцій. Засоби глобального зв'язку допомагають їм вирішувати завдання організації, набору нових членів, спілкування».

Президент США Обама зазначив, що «кіберзагрози можуть нашкодити навіть міжнародному миру і безпеці, оскільки традиційні форми конфлікту розширюються вже і на Інтернет» [7].

Відомі в минулому і сьогодні політики зазначили: - «соціальні мережі це найгірше зло в суспільстві» (Тайіп Ердоган), а екс-Президент США Обама сказав – Інтернет це «хребет, що підтримує процвітаючу

економіку, сильну армію, відкритий і демократичний уряд». Екс-Держсекретар США Керрі назвав кібератаки проти життєво важливої інфраструктури США «еквівалентом ядерної зброї 21-го століття» [3, с. 33].

Важливою особливістю сучасного тероризму є ієрархічна структурованість та сувора організаційна структура; жорстка конспірація; потужне технічне оснащення, що може конкурувати із забезпеченістю урядових підрозділів.

Кібертероризм не має державних кордонів, кібертерорист здатний однаковою мірою загрожувати інформаційним системам, розташованим практично у будь-якому місці світу. Виявити і нейтралізувати віртуального терориста дуже складно через занадто малу спроможність та складність фіксації слідів, на відміну від фізичного світу, де сліди є більш прагматичною та реальною можливістю для фіксації.

Різноманіття існуючих визначень ускладнює розроблення стратегії боротьби з тероризмом, пов'язаним із інформаційними технологіями [8]. Різноманіття наявних дефініцій ускладнює розроблення стратегії боротьби з кібертероризмом. Враховуючи думку відомих фахівців із питань забезпечення інформаційної безпеки, візьмемо як робочу версію таку: к*ібертероризм* – суспільно небезпечна діяльність, що здійснюється в кіберпросторі (або з використанням його технічних можливостей) із терористичною метою і полягає у свідомому, цілеспрямованому залякуванні населення та органів влади або вчиненні інших посягань на життя і здоров'я людей [9].

Нова форма тероризму суттєво відрізняється від інших типів: вона діє в кіберпросторі і породжує новий різновид насильства. Саме тому глобальний характер технічної бази кібертероризму та її доступність визначили особливі риси цього виду тероризму: висока ефективність кібератак, наслідки яких можуть мати глобальний характер; невизначеність джерела кібератаки у просторі; тимчасова невизначеність у часі як самої кібератаки, так і процесу її підготовки; можливість організації складних кібератак одночасно на різні об'єкти із різних напрямів; анонімність злочинця (для здійснення терористичного акту зловмиснику немає необхідності перетинати межі держав і знаходитися безпосередньо на місці злочину); зниження рівня морально-психологічного тиску на суб'єкт кібератаки, пов'язане з просторово-часовою віддаленістю від об'єкта кібератаки (усі дії для суб'єктів кібератаки відбувається у віртуальному кіберпросторі) [10].

Характерною особливістю кібертероризму і його відмінністю від кіберзлочинності є його відкритість, коли умови терориста широко висвітлюються мас-медіа.

Спектр проявів кібертероризму досить широкий, від незаконного впливу на прийняття невиправданих рішень, поширення паніки і безладу, до проникнення в канали і системи супутникового зв'язку, навігації, управління енергетикою, транспортом, банківським сектором тощо. На відміну від звичайного терориста, який для досягнення своїх цілей використовує вибухівку або стрілецьку зброю, кібертерорист використовує для досягнення своїх цілей сучасні інформаційні технології, комп'ютерні системи і мережі, спеціальне програмне забезпечення, призначене для несанкціонованого проникнення в комп'ютерні системи й організації дистанційної атаки на інформаційні ресурси об'єкта нападу [3, с. 35].

Кібертерористи можуть діставатися доступу до різноманітної інформації та під загрозою є не доступ до закритих інформаційних ресурсів державних органів, а злам відкритих сайтів і комп'ютерних мереж. Кібертерористи можуть досягти цілі, отримавши доступ до чутливої інформації: даних щодо розташування підземних комунікацій, місць знаходження техногенно небезпечних об'єктів, можливої їх охорони тощо. Водночас злочинці можуть дістати доступ до особистих даних багатьох користувачів мережі, починаючи від адреси, номера телефону і завершуючи індивідуальною інформацією щодо особи, включаючи її хобі та розпорядок життя.

Наслідки терористичних посягань на об'єкти критичної інфраструктури можуть бути руйнівними в економічному й соціальному значенні. Низка об'єктів критичної інфраструктури перебуває у власності приватного капіталу, а не держави. Вкрай важливим елементом організації системи забезпечення кібербезпеки є створення відповідної системи координації, до складу якої б входили як урядові, так і громадські організації із залученням приватних учасників у ключових секторах критичної інфраструктури. Тісний взаємозв'язок між державним і приватним сектором країни є невід'ємною умовою безпеки держави. Ця взаємодія повинна ґрунтуватись на обізнаності щодо загроз критичній інфраструктурі держави; зосередженні уваги спецслужб і виробників програмного забезпечення на безпеці захищеності комп'ютерної техніки; своєчасному і швидкому реагуванні на інциденти, пов'язані з втручанням у роботу автоматизованих систем; наявності системи формального і неформального обміну інформацією щодо загроз комп'ютерної злочинності і кібертероризму [11].

Вирішення проблеми протидії кібертероризму ґрунтується на комплексному підході та має такі складові [3, с. 37]:

– *правову* – пов'язана з розробленням нормативно-правових актів, які регламентують відносини в інформаційній сфері, і нормативно-методичних документів із питань забезпечення інформаційної безпеки;

– *організаційну* – полягає в удосконаленні організаційної структури державних і комерційних підприємств, сертифікації і стандартизації засобів захисту інформації та ліцензуванні діяльності у сфері захисту інформації;

– *психологічну* – передбачає формування морально-етичних норм у співробітників, які працюють з інформаційними системами, що забезпечують критичну інфраструктуру держави;

– *технічну* – ґрунтується на створенні і постійному вдосконаленні системи забезпечення інформаційної безпеки на об'єктах інформатизації та попередження нападу.

Із врахуванням предмету нашого дослідження, ключовою проблемою залишається правова регламентація використання кіберпростору. Правовим регулюванням держава має сприяти підвищенню відповідальності провайдерів і власників сайтів щодо розміщення недостовірної та завідомо шкідливої інформації, а також закріплювати механізм впливу на недобросовісних суб'єктів інформаційних правовідносин в кібернетичному просторі. Крім того, необхідною умовою також є уникнення правових колізій та прогалин в законодавстві, наслідком чого є несвоєчасне і неадекватне реагування правоохоронних органів на факти заподіяння шкоди інформації, інформаційно-телекомунікаційним мережам, репутації громадян тощо.

Таким чином, забезпечення кібербезпеки все частіше розглядається, у якості стратегічного завдання держави, що охоплює увесь спектр суб'єктно-об'єктного складу. Не виключенням є і нинішній стан цієї проблеми в Україні, який характеризується процесами глобалізації та особливим станом України.

Кіберзагрози в Україні мають додаткову характеристику, так як використовуються у якості складової гібридної агресії Російською Федерацією проти нашої держави. У зазначеному контексті набуло широкого розповсюдження використання цілої низки споріднених термінів, зокрема: гібридна війна, гібридна агресія, гібридні виклики, гібридні загрози тощо. Гібридна агресія Росії проти України переросла в активну фазу на початку 2014 року, хоча підривну діяльність проти України вона стала вести одразу після проголошення Україною незалежності у 1991 році. Такої думки дотримується більшість (51,4%) з 37 українських експертів, які взяли участь в опитуванні, що здійснювалось у 2017 році Центром глобалістики «Стратегія XXI» за підтримки ЄС і Міжнародного фонду «Відродження» [12].

Використання кіберпростору як виміру гібридної агресії є явищем порівняно новим і менш опрацьованим з точки зору розуміння рівня загроз та можливої протидії. Як відзначає Д. Дубов, начальник відділу інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень, дискусія щодо сприйняття природи кібератак та відповідей на них почалася в 2010-2011 роках. У 2011 році був прийнятий документ «Талліннське керівництво із застосування міжнародного законодавства у кіберсфері», а в 2012 році НАТО визнало кіберпростір новим театром воєнних дій. Однак у практичній площині реагування є досить проблематичним, оскільки важко довести причетність конкретних країни чи груп до здійснення атак [13].

**Висновок.** Забезпечення безпеки у кіберпросторі є на сьогодні актуальним для нашої держави з огляду на те, що проти неї ведеться гібридна війна, одним з проявів якої є кібератаки на українські державні органи та установи, а також об'єкти критичної інфраструктури. З огляду на це, державі слід приділяти питанню кібербезпеки максимальну увагу.

## ЛІТЕРАТУРА

1. Тонконогов А.В. Кибернетическая безопасность: понятие и сущность феномена. Правовой Центр – «Правый Берег». URL: http://www.center-bereg.ru/h69.html
2. Аналітичний звіт щодо аналізу гібридних загроз у секторі громадської безпеки та цивільного захисту. Державний науково-дослідний інститут МВС України. Київ. 2019. 13 стор.
3. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту. Монографія. Київ: Видавничий дім «АртЕк». 2017. 107 с.
4. Конвенція про кіберзлочинність. URL: http://zakon0.rada. gov.ua/laws/show/994_575
5. Щетилов А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом. *Информатизация и информационная безопасность правоохранительных органов:* XI межд. конф. Москва, 2002. С. 186-188.
6. How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns. URL: https://www.amazon.com/How-Terrorism-Ends-Understanding-Terrorist/dp/069115239X
7. International Strategy for Cyberspace, 2011. URL: https: // obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
8. Голубєв В.О. Кібертероризм, як нова форма тероризму. URL: http://www.crimeresearch.org/library/Gol_tem3.ht.– 10.04.0.
9. Дубов Д.В., Ожеван М.А. Кібербезпека: світові тенденції та виклики для України. Київ: НІСД, 2011. 30 с.
10. Іксар В.К. Комп'ютерні злочини. URL: http:// www.comprice.ru/pravo/.2001–20_2.phtml.
11. Довгань О.Д., Хлань В.Г. Кібертероризм як загроза інформаційному суверенітету держави. *Інформаційна безпека людини, суспільства, держави*. 2011. №3(7). С.49 – 53.
12. Сприяння розбудові можливостей України гарантувати безпеку суспільства в умовах гібридних загроз. Результати експертного опитування. URL: https:// geostrategy.org.ua/images/%D0%94%D0%BE%D1%81%D0%BB%D1%96%D0%B4%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F_%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%BE%D1%8E.pdf.
13. Військова відповідь на кібератаки Кремля? І так, і ні. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-technology/2251563-vijskova-vidpovid-nakiberataki-kremla-i-tak-i-ni.html

14. Ковальчук Т.І., Користін О.Є., Свиридюк Н.П. Гібридні загрози у секторі цивільної безпеки в Україні. *Наука і правоохоронна*. 2019. № 3 (45). С. 69-79.
15. 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.

## REFERENCES

1. Tonkonogov A.V. Kiberneticheskaya bezopasnost: ponyatie i suschnost fenomena. Pravovoy Tsentr – «Pravyiy Bereg». URL: http://www.center-bereg.ru/h69.html
2. Analitichniy zvit schodo analizu gibridnih zagroz u sektori gromadskoyi bezpeki ta tsivilnogo zahistu. Derzhavniy naukovo-doslidniy institut MVS Ukrayini. Kiyiv. 2019. 13 stor.
3. Dovgan O.D., DoronIn I.M. Eskalatsiya kiberzagroz natsionalnim interesam Ukrayini ta pravovi aspekti kiberzahistu. Monografiya. Kiyiv: Vidavnichiy dim «ArtEk». 2017. 107 s.
4. Konventsiya pro kiberzlochinnist. URL: http://zakon0.rada. gov.ua/laws/show/994_575
5. Schetilov A. Nekotoryie problemyi borbyi s kiberprestupnostyu i kiberterrorizmom. Informatizatsiya i informatsionnaya bezopasnost pravoohranitelnyih organov: XI mezhd. konf. Moskva, 2002. S. 186-188.
6. How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns. URL: https://www.amazon.com/How-Terrorism-Ends-Understanding-Terrorist/dp/069115239X
7. International Strategy for Cyberspace, 2011. URL: https:// obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
8. Golubev V.O. Kiberterorizm, yak nova forma terorizmu. URL: http://www.crimeresearch.org/library/Gol_tem3.ht.– 10.04.0.
9. Dubov D.V., Ozhevan M.A. (2011) Kiberbezpeka: svitovi tendentsiyi ta vikliki dlya Ukrayini. Kiyiv: NISD. 30 s.
10. Iksar V.K. Komp'yuterni zlochini. URL: http:// www.comprice.ru/pravo/.2001–20_2.phtml.
11. Dovgan O.D., Hlan V.G. (2011) Kiberterorizm yak zagroza informatsiynomu suverenitetu derzhavi. *Informatsiyna bezpeka lyudini, suspilstva, derzhavi.* № 3(7). S.49 – 53.
12. Spriyannya rozbudovi mozhlivostey Ukrayini garantuvati bezpeku suspilstva v umovah gibridnih zagroz. Rezultati ekspertnogo opituvannya. URL: https:// geostrategy.org.ua/images/%D0%94%D0%BE%D1%81%D0%BB%D1%96%D0%B4%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F_%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%BE%D1%8E.pdf.
13. Viyskova vidpovid na kiberataki Kremlya? I tak, I ni. *Ukrinform*. URL: https://www.ukrinform.ua/rubric-technology/2251563-vijskova-vidpovid-nakiberataki-kremla-i-tak-i-ni.html
14. Kovalchuk T.I., KoristIn O.Ye., Sviridyuk N.P. Gibridni zagrozi u sektori tsivilnoyi bezpeki v Ukrayini. *Nauka i pravoohoronna*. 2019. № 3 (45). S. 69-79.
15. Kovalchuk T. I., Korystin O. Ye., Sviridyuk N. P. Hybrid threats in the civil security sector in Ukraine. *problemi zakonnosti*. 2019. Vip. 147. S. 163-175.