КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.129139
УДК 32:004.056:061

Суський Георгій Валерійович
аспірант 2-го року навчання
Інститут програмних систем НАН України, Київ, Україна
ORCID ID: 0000-0001-8049-1687
nitaet@gmail.com

СУЧАСНИЙ ІНФОРМАЦІЙНИЙ ПРОСТІР ТА ПИТАННЯ КІБЕРБЕЗПЕКИ

Анотація. Стаття присвячена виявленню і уточненню поля взаємодії понять «інформаційний простір», «інформаційна безпека», «кібербезпека» в науковому дискурсі. Розгляд цієї інтерференції понять важливий з точки зору актуальної ситуації в інформаційному просторі України, яка склалася після повномасштабного вторгнення російських військ 24 лютого 2022 року. Зважаючи на те, що інструментом гібридної війни є також вплив на масову свідомість через інформаційний простір, питання інформаційної безпеки населення в цілому, а також кібербезпеки як сукупності інструментів технологічного забезпечення процесу безпечної роботи економічних, соціально-політичних та власне всієї системи державних інституцій України, постають сьогодні нагальним завданням не тільки відповідних структур і організацій, але й наукового середовища. У статті здійснена спроба проаналізувати притаманні українському інформаційному простору проблеми, зокрема, безпекові, технологічні, правові, адже під час російсько-української війни вони стали найбільш нагальними; крім цього, вони безпосередньо пов'язані з технологічними умовами розвитку ІКТ. Незаперечно важливими є зусилля міжнародних інституцій, зокрема НАТО, яке відіграє ключову та регулятивну роль у створенні ефективної системи протидії кіберконфліктам. Кібератаки, що стали особливо активними після повномасштабного вторгнення російських військ на територію України у 2022 році, спрямовані, насамперед, на підрив політичної стабільності в державі, особливо коли світові політичні лідери прагнуть до пошуку шляхів врегулювання і досягнення миру в російсько-українській війні. Вивчення проблем кібербезпеки в інформаційному просторі держави та визначення перспектив і можливостей їхнього вирішення в сучасних суспільних умовах постає актуальним питанням для сучасного кола фахівців з ІКТ та кібербезпеки.

Ключові слова: кібербезпека; гібридна війна; інформаційний простір; кіберінциденти.

ВСТУП

Проблеми кібербезпеки в українському інформаційному просторі набувають все більшої актуальності, адже сучасні тенденції зростання ролі та обсягів інформації розвиваються з небаченою раніше швидкістю. Особливий поштовх до загострення уваги саме на проблемах кібербезнеки надають кризові ситуації, зокрема, і період пандемії COVID-19, і особливо — російська агресія проти України, що поставила питання не тільки захисту демократичних засад нашого суспільства, але й загострила проблему існування української незалежної держави в цілому.

Саме інформаційний простір будь-якої держави відображає перспективи та рівень її демократичного розвитку. Категорія «інформаційний простір держави» включає всі ті явища та процеси, що відбуваються у просторі інформаційних ресурсів держави чи мають до нього стосунок, певну співвіднесеність та у своїй основі можуть бути визнаними «владою інформації», з усіма механізмами її впливу на суспільство. Розуміння інформаційного простору України як середовища, в якому здійснюється формування, збір, збереження та розповсюдження інформації регулюється правовими

засадами нашої країни, які відображені у певному контингенті правових актів інформаційного законодавства.

Крім цього, в середовищі сучасних комунікацій розрізняють: інформаційний простір інтерперсональної комунікації — як сукупність повідомлень (переважно у вигляді слів), що мають конкретне, а інколи й суто цілеспрямоване значення для учасників комунікації; а також інформаційний простір масової комунікації — як ареал словесних повідомлень, аудіовізуальних образів, інфографіки тощо, що створюють той величезний обсяг інформації, який забезпечується ІКТ та розповсюджується ЗМІ та соціальними мережами.

Постановка проблеми. Залученість до масового середовища сучасного інформаційного простору охоплює десятків мільйонів користувачів. Зважаючи на такі масштаби охоплення, постає питання про захист даних споживачів, який технологічно має забезпечувати розгалужена система кіберзахисту в мережі. Отже, проблеми безпеки транслювання інформації, даних (зокрема статистичних, даних реєстрів тощо) потребує постійної уваги, особливо під час воєнного стану.

Аналіз останніх досліджень і публікацій. Періодичність звертання до тих або інших джерел, які є носіями інформації в світі, все більш інтенсифікується. Активізується як процес самого обміну, так і продукування інформації, при цьому останнє відбувається у таких величезних масштабах, які, неможливо було уявити навіть ще півстоліття тому. Проте пропорційно активності користувачів інформаційного простору збільшується і потенційна небезпека втрати або ушкодження даних. Так, за оцінками Жиліна А. В. та ін. «для забезпечення рівня безпеки даних застосовуються наступні інструменти та методи мережевої безпеки: шифрування, контроль доступу, резервне копіювання, тестування на проникнення, аналіз вразливостей» [1, с.13]. З кожним роком актуальність протидії кібератакам зростає, адже зростають і стають все більш вишуканими способи зловмисного проникнення. В цьому сенсі особливо точною є думка Марка Ґантріпа (старшого директора із стратегій кібербезпеки Menlo Security), що у 2023 році «атаки програм-вимагачів зростатимуть. У сучасному ландшафті загроз жодна система не захищена, і немає жодних ознак того, що кіберзлочинці знижують темпи. Люди є найслабшою ланкою, коли йдеться про безпеку. Наше дослідження виявило, що працівники, які ігнорують поради щодо корпоративної безпеки, посідають перші місця у списку найбільших проблем тих, хто приймає рішення щодо ІЕ-безпеки. 39% занепокоєні атаками програм-вимагачів, які виходять за межі можливостей безпеки їхньої компанії. Не дивно, що кібер-зловмисники стають дедалі розумнішими, оскільки ми продовжуємо спостерігати появу методів, які допомагають уникнути типових засобів безпеки, наприклад, клас атак Highly Evasive Adaptive Threat (HEAT)» [2].

Дослідження медіаповедінки в інформаційному просторі демонструють все більшу активність споживачів інтернет-мережі — від повідомлень державних медіа до масового середовища реципієнтів, які обмінюються в мережах своїми дописами. Проте, набагато серйозніші загрози виникають при оцінці реальної шкоди, яку можуть завдати проникнення, наприклад, у держреєстри чи інші сховища інформації, важливі для життя країни [3]. Проблема посилюється тим, що більшість держреєстрів не можна вимикати. Отже, позиціонування вирішення проблеми має ще й часовий вимір й поділяється на те, чи стосується атакований держреєстр до такого типу, який можна вимикати на певний час, або ні.

Ще перед початком повномасштабного вторгнення російських військ на територію України, а саме, у січні 2022 року було зафіксоване суттєве зростання кількості кібератак. Так, 13 січня 2022 року компанією Microsoft було виявлено шкідливе

програмне забезпечення, націлене на уряд України та декілька некомерційних та IT-організацій, а 14 січня 2022 року під тимчасовим контролем хакерів опинилися 70 урядових сайтів, зокрема сайти Кабінету Міністрів України, Міністерства оборони та Міністерства закордонних справ, а також Міністерства освіти та науки. Відповідальність за цю атаку Міністерство цифрової трансформації України небезпідставно поклало на росію. В рамках протидії таким кібератакам, агрегувавши свої зусилля, незалежні хакери з усього світу виявили та оприлюднили російські урядові документи (в тому числі електронні листи), фінансові дані та інформацію про банківську діяльність, виробництво енергії та пропагандистські кампанії, а також дані про військовослужбовців та агентів російської ФСБ.

Становлення процесів продукування та тиражування інформації як частини суспільного виробництва є ґрунтівною ознакою сучасного інформаційного суспільства. Проте бурхливий розвиток цієї галузі як невід'ємної складової національних ресурсів держави, викликає й появу нових проблем. По-перше, це функціонування національного інформаційного простору в системі світового, глобалізованого медіапростору, де взаємовплив чи непередбачувана включеність одного простору в інший, або зловмисне втручання в інформаційний простір, яке викликає небажані наслідки (як це відбувалось з російськими каналами на тимчасово окупованих територіях українського Донбасу, або з протестами проти матеріалів каналу «Рашатудей» у Німеччині). По-друге, в сучасному світі з появою влади інформації народилося таке явище як інформаційні (гібридні) війни, які відбувались і в мирний час, але ще більшого масштабу досягли після повномасштабного вторгнення російських військ на територію незалежної України. Такі інформаційні війни можуть бути як частиною *гібридної війни*, так і відбуватися паралельно з «гарячою війною», з метою спрямувати свою силу впливу на маси у вигідному для агресора руслі. По-третє, всі ці колізії, що відбуваються навколо світу інформації не могли не викликати потребу в такій специфічній сфері, як *інформаційна безпека*, що тлумачиться як безпека людини, її інтелектуальної власності, різноманітних персональних даних тощо; «цифрова епоха інформаційного суспільства привнесла з собою не тільки позитивні трансформації. Основними недоліками стали ризики *кіберінцидентів*, які набувають все більших масштабів. Наявність кіберінцидентів в інформаційно-телекомунікаційній системі свідчить про розвиток кібератак або вже їх здійснення. Наслідки цих атак можуть призвести до несанкціонованого доступу до інформації, яка циркулює в мережі, або ж позбавлення її працездатності» [1, с. 5].

Враховуючи актуальність то нові виклики, що постають перед спеціалістами з кібербезпеки, все більш активно розвивається сфера наукових досліджень у цьому напрямку. Серед вітчизняних фахівців з кібербезпеки незаперечний внесок А. Жиліна, Д. Костельнюка, І. Огірка, О. Успенського, О. Шаповала, Ю. Щавінського, ін.; правовими аспектами захисту інформаційного простору займались В. Брижко, А. Грубінко, О. Кузнєцов, В. Фурашев, ін., зокрема, питання ролі НАТО у захисті кіберпростору аналізують А. Балашов, В. Бутримас, В. Гвоздь, Ю. Завгородня, О. Звоздецька, С. Кавин, А. Ковальов, О. Суходоля.

Велику увагу удосконаленню і розвитку кібербезпеки приділяє НАТО, яке здійснює «інтеграцію наступальних кіберзасобів при плануванні місій і операцій за допомогою SCEPVA — структури суверенних кіберефектів, наданих союзниками на добровільній основі. Але у мирний час НАТО не вдається до кібероперацій поза межами свого оборонного простору» [4]. Досвід НАТО з питань кібербезпеки вивчається й вітчизняними спеціалістами, зокрема, згідно з думкою Ю. Завгородньої, «питання трансформації НАТО залишається досліджуваним та продовжується пошук наукових

висновків в різних аспектах, однак в сучасних політичних процесах важливо звернути увагу на ефективну систему протидії кіберконфліктів, в яких НАТО може відіграти ключову регулятивну роль, стабілізувати хаотичні процеси взаємодії суб'єктів політиків та сформувати принципи доброчесної діяльності» [5, с. 63].

Про стратегічну важливість убезпечення від кіберзагроз країн Європи (зокрема, країн-членів НАТО), свідчать і такі документи, як «The French White Paper on defence and national security», де зафіксовано, що «ми повинні гарантувати захист громадян Франції, в тому числі від кіберзагроз, зберегти довіру до нашого ядерного стримування та чітко підтвердити наше право проявляти ініціативу в діях, які відстоюють наші інтереси та міжнародної спільноти. Наша мета — гарантувати безпеку Франції шляхом мобілізації всіх сил у загальнонаціональних зусиллях, які самі повинні бути закріплені у ширших рамках побудови ефективної європейської оборонної політики» [6, с. 7–8].

НАТО не має власної кіберзброї, проте очолюваний США альянс створив оперативний центр у Бельгії — новий центр кібероперацій (CYOC) у Монсі. Великобританія, США, Естонія та інші союзники з того часу запропонували свої безпекові кіберпрограми [7]. Так, Сполучені Штати Америки, наприклад, через свою доктрину постійних дій наголошують на необхідності переносити боротьбу з ворогом на операції поза межами своєї «зони відповідальності» в конкурентному цифровому просторі, і цю думку загалом поділяє Великобританія. Ціль програми полягає в тому, щоб формувати поведінку супротивника, а також норми «узгоджених змагань» в кіберпросторі, «замість того, щоб сидіти і чекати доки дипломати домовляться про глобальні умови поведінки держав, які, швидше за все, будуть проігноровані» [8].

Можна запропонувати тезу, що функціонування інформаційного простору можливе лише за умови існування засад кібербезпеки (або інформаційної безпеки цифрової доби). З розвитком та поширенням засобів акумулювання, збереження та обміну інформаційними ресурсами ця теза набуває нових, більш складних рис та важливого значення у комунікаційних процесах.

Під час кіберконференції НАТО у 2023 році генерал-майор Вольфганг Реннер, командувач ВПС Німеччини, який керує новим центром кібероперацій (CYOC) у Монсі, сказав: «Це нова сфера, і загроза зростає… Ми повинні бути готові, щоб мати можливість виконувати операції в кіберпросторі. Ми вже вийшли за рамки захисту та запобігання» [8].

Метою статті є висвітлення питань кібербезпеки інформаційного простору держави, що набули особливої актуальності після початку повномасштабного вторгнення російських військ на територію України 24 лютого 2022 року.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На сучасному етапі розвитку глобальних цифрових технологій все частіше вживається такий термін, як «кібервійна», що розуміється як крайня форма кіберконфліктів. Ситуація в інформаційному просторі складається іноді більш напружено, ніж можна було уявити ще років десять назад; наприклад, «комунікаційні та комп'ютерні мережі НАТО стикаються з сотнями значних спроб злому щомісяця, за даними Агентства зв'язку та інформації НАТО, тоді як експерти кажуть, що Росія, Північна Корея та Китай постійно розгортають складну комп'ютерну хакерську зброю та програмне забезпечення для спостереження» [8].

Крім цього безпека інформаційного простору охоплює процеси, формування громадської думки, виховання, освіти, спричиняє лояльність (або нелояльність) до

держави, громадськості, окремих груп і спільнот, тощо. Звідси й витікає її величезне значення, особливо в суспільствах перехідного або кризового періоду.

В сучасних умовах затяжного військового конфлікту, яким є російсько-українська війна, особливо стає відчутною сутність гібридної війни, що полягає у стратегічній координації агресивних дій з метою досягнення своїх цілей та приховуванні відповідальності за конфлікт. Однією з перших одразу після початку повномасштабного вторгнення російських військ на територію України 25 лютого 2022 р. відбулась кібератака на пункт прикордонного контролю з метою перешкоджання виїзду біженців до Румунії. Також в перші дні від початку російської агресії відбулись атаки на цифрову інфраструктуру України, що призвело до блокування доступу до фінансових послуг та енергетичних ресурсів (зокрема, 28 лютого 2022 р.) [9]. Агресор використовує можливість заперечувати і саме провокування конфлікту, і свою безпосередню участь у ньому, створюючи ускладнення як для противника, так і для міжнародного співтовариства щодо оперативного, чіткого та ефективного реагування на нього. Безперечно потребують уваги й так звані «конспірологічні теорії», про які йдеться у праці Аарона Джона Гуліаса «Теорії змови: коріння, теми та розповсюдження параноїдальних політичних і культурних наративів», який пише, що «незалежно від того, чи закликають вони (конспірологічні дослідники та автори) своїх читачів протестувати проти втручання Америки в ООН чи виступають за підтримку та компенсацію жертвам урядових медичних і психологічних експериментів, часто виникає бажання політичних змін, які виходять за межі жанру змови, та ілюструє широке застосування до позаконспірологічної політики» [10, с. 9–10].

Кібератаки, спрямовані, насамперед, на підрив політичної стабільності в державі, особливо коли світові політичні лідери прагнуть до пошуку шляхів врегулювання і досягнення миру в російсько-українській війні, але російська пропаганда намагається використати їх для маніпулювання громадською думкою або дискредитації мирних ініціатив (як це було під час Швейцарського саммиту у червні 2024 року). Це може призвести до загострення політичних конфліктів, спотворення та погіршення якості прийнятих політичних рішень.

Енді Грінберг, який є старшим автором журналу WIRED, розповідає про хакерство, кібербезпеку та стеження, у своїх працях: «Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency» та «Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers» — наголошує на тому, що наступає «нова ера кібервійни та полювання на найнебезпечніших хакерів Кремля» [11]. Необхідно також підтримувати розвиток незалежних органів інформаційної безпеки та медійного нагляду, які мають на меті забезпечення принципів кібербезпеки. Ці органи можуть відігравати ключову роль у виявленні та припиненні поширення маніпулятивних матеріалів та вирішенні питань захисту інформації в ІКС та навіть віртуальних приватних мережах.

Розуміння та використання передових інформаційних технологій у сфері кібербезпеки може значно зменшити вплив і характер небезпеки маніпулятивно-пропагандистських матеріалів у ЗМІ та соціальних мережах. За даними КМІС щодо використання Інтернету «89% респондентів віком 18–29 років у 2023 році користувалися принаймні однією послугою, серед респондентів віком 70 років та більше таких користувачів лише 30%. Крім того, минулого року державними електронними послугами частіше користувалися чоловіки, з вищою освітою та з високим рівнем достатку. Люди старшого віку найрідше користуються як державними цифровими послугами (35%), так і інтернетом (50% роблять це щодня, тоді як 30% узагалі не користуються). Разом з тим,

саме ця вікова категорія — одна з тих, де найбільше зросла кількість регулярних користувачів інтернету. Їх частка збільшилася до 50% порівняно з 32% у 2022 році» [12].

У нашому сьогоденні, особливо в умовах воєнного стану, говорячи про український інформаційний простір акцентуються, насамперед, територіальний (охоплення) та змістовий аспекти. Власний інформаційний простір незалежної України формувався спонтанно, поступово, виходячи від кардинальної перебудови суспільства. Протягом перших десятиліть розбудови Української незалежної держави національний інформаційний простір отримав відповідну частку належної уваги з боку різних соціально-політичних груп та державних органів; зокрема, було створене інформаційне законодавство України [13], що забезпечило функціонування незалежних медіа та їх демократизацію, а у 2023 році був прийнятий Закон України «Про медіа», який регламентував не тільки традиційні, але й нові інтернет-медіа.

Технологічні проблеми інформаційного простору України, пов’язані з питаннями кібербезпеки, можна структурувати таким чином: соціо-політичні, правові, економічно-фінансові, технологічні, власне безпекові, психологічні, освітні та культурні. І хоч всі окреслені проблеми стосуються різних сфер життя, проте тісно пов’язані між собою саме гостротою вирішення питань кібербезпеки. Всі згадані вище проблеми не можуть сьогодні розглядатися виокремлено, тому що їхньому вирішенню притаманний системний характер та чітке дотримання технологій кібербезпеки. У свою чергу, наявність невирішених актуальних завдань і викликів, як в науковому так і в суто професійному плані, спричиняє появу все нових і нових груп проблем.

Аналізуючи притаманні українському інформаційному простору проблеми, почнемо з безпекових, адже під час російсько-української війни вони стали найбільш нагальними; крім цього, вони безпосередньо пов’язані з технологічними, що дозволяє визначити перспективи і можливості їх вирішення у сучасних умовах технологічного розвитку суспільства. В колі проблем безпекового характеру перше і головне місце посідає саме політична проблематика, зокрема, підтримка більшістю країн Європи і США боротьби України проти російської агресії. Тут необхідно підкреслити увагу до дій кіберспільноти, яка виступає на боці України і розгорнула низку заходів, які є актуальними щодо протидії злочинним кібератакам Росії. За повідомленням ДСЄП (Дослідницької служби Європарламенту), наприклад, збирається конфіденційна інформація, яка потім передається міжнародним активістам, щоб покарати росію за її злочини в Україні. Вторинним ефектом таких дій хакерів є їхній успіх стосовно створення хаосу в російських кіберсистемах і руйнування переконань про неприступність кібероборони росії. Позиція Європарламенту є непохитною: у резолюції від 1 березня 2022 року Парламент закликав до негайного та повного впровадження всіх рішень, які посилять внесок ЄС у зміцнення оборонних спроможностей України, у тому числі й у сфері кібербезпеки. Крім того, Парламент закликав ЄС, НАТО та інших зацікавлених партнерів посилити допомогу Україні у сфері кібербезпеки [14].

Впродовж посилення російської агресії та атак на об’єкти критичної інфраструктури стає зрозумілим, що «кібербезпека стає все більшою загрозою для секторів критичної інфраструктури ЄС, оскільки кількість кібератак значно зросла за останні роки. Лише у 2023 році було зареєстровано понад 200 кіберінцидентів, спрямованих на енергетичний сектор, і більше половини з них були спрямовані саме на Європу. Значна роль, яку цей сектор відіграє для європейської економіки, робить енергетичну галузь особливо сприйнятливою до кіберзагроз і атак» [15], йдеться у повідомленні European Union Agency for Cybersecurity (ENISA).

Розуміння цієї досить складної сфери суспільних відносин, коли інформаційний

простір трактується переважно з технологічної точки зору, як-то сукупність наявних ЗМІ, комп'ютерів, новітніх комунікацій, що охоплюють територію нашої країни. Негативні наслідки кібератак потребують їх негайного вирішення, іноді це стає неможливим без зовнішнього втручання або допомоги, або без досить великих втрат для всього суспільства. Безпека інформаційного простору України пов'язана із зосередженням уваги ІТ-спеціалістів на питаннях розвитку інформаційного простору в контексті міжнародних кроків і глобалізаційних устремлінь України (зокрема, в рамках вектору майбутнього вступу до ЄС). З'являються відповідні публікації, законодавчі акти, розгортаються дискусії з приводу функціонування та розвитку комп'ютерних технологій, піднімаються проблеми функціонування національного інформаційного простору та його включення до глобальних систем інформаційного обміну.

В політичному плані слід також зазначити, що інформаційний простір, якщо він існує у демократичній країні, просто не може бути в світлі глобалізаційних тенденцій суто національним, оскільки поява та розповсюдження новітніх засобів комунікації та поширення інформації все швидше стирають міждержавні та міжцивілізаційні кордони. В реаліях Української держави присутня ще одна специфічна риса — це її поліетнічний характер. Помилково забувати про цей чинник у розбудові українського інформаційного простору, який повинен враховувати потреби всіх своїх суб'єктів та об'єктів й узгоджувати їх з державною політикою, особливо під час війни.

Забезпечення прозорості державних органів є однією з передумов формування демократичного суспільства, а обов'язок держави щодо надання правдивої та неупередженої інформації громадянам лежить в основі побудови громадянського суспільства та зростання ступеня взаємної відповідальності влади та суспільства.

Україна перебуває сьогодні в динамічному розвитку, тож навіть найпрогресивніше законодавство потребує внесення відповідних змін і доповнень, зокрема, це стосується і сфери кібербезпеки [16]. Зволікання і нерозуміння цього призводить до того, що український інформаційний простір виявився вразливим і недостатньо незахищеним від зовнішніх інформаційних впливів, що створює поле потенційних загроз національній безпеці та суверенітету.

В межах реальних потреб у розвиткові та прогресі суспільства і держави є недопустимим розкриття певних фактів, важливої для держави та її інституцій інформації (особливо під час воєнного стану). Такі засади втілює Закон України «Про основні засади забезпечення кібербезпеки України», який визначає: «кібербезпека — захищеність життєво важливих інтересів людини і 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 і потенційних загроз національній безпеці України у кіберпросторі» [17], проте в майбутньому з розвитком технологій нас чекає ще багато аспектів кібербезпеки, які ще треба буде визначати на законодавчому рівні.

Економічні чинники справляють величезний вплив на інформаційний простір спричиняють розробку і розвиток нових технологій. Для ефективної реалізації державної політики у сфері кібербезпеки необхідна відповідна підтримка суб'єктів інформаційного простору, допомога в становленні й розвитку вітчизняних технологічних ресурсів. Наявна експансія протягом більш ніж двох десятиліть щодо українського інформаційного простору з боку неукраїнських політичних й фінансових кіл (зокрема російських), що використовували його у власних інтересах, інколи, навіть, з метою дестабілізації української економіки та дискредитування суспільно-політичних інститутів нашої країни, була фактично припинена лише у перші місяці

широкомасштабної російської агресії.

Наступним колом проблем є технологічне забезпечення діяльності суб'єктів інформаційного простору, що знаходиться в прямій залежності від економіко-фінансових питань. Сьогодні маємо визначити два головних суперечних аспекти цієї проблеми. Перший стосується того, що об'єктивно можливості для використання нових технологічних розробок в інформаційно-телекомунікаційній сфері не тільки існують, але й з розвитком та вдосконаленням відповідних засобів, вони стають все ширшими. Другий аспект полягає у тому, що їхньому використанню заважають, з одного боку, недостатність у більшості аґентів інформаційного простору коштів на використання відповідних засобів, а з іншого, у певному консерватизмі, причому, як зі сторони самих суб'єктів, так й зі сторони соціальних інституцій. Технологічна політика як складова інформаційної політики в Україні потребує вдосконалення. Як результат — маємо подолати все ще відчутну технологічну відсталість та набути спроможності максимальної оперативності інформації, яку подають суб'єкти інформаційного простору.

Питання безпеки в інформаційному просторі діяльності державних органів влади відображає стан кібербезпеки держреєстрів (як це зазначалось вище). Також ця проблема поглибилась з розвитком національної складової мережі Інтернет. Наприклад, в українському сегменті Інтернет, на думку багатьох спеціалістів, лише кілька державних Web-сайтів є «повнофункціональними», тобто тут представлена більш-менш вичерпна інформація про даний орган управління, функції, які ним виконуються, законодавчу базу, на якій заснована його діяльність, ін. Представницький характер мають також Web-сайти різних наукових інституцій. Так, наприклад, сайт (портал) НАН України містить інформацію про склад Президії НАНУ, біографічні дані про видатних вчених минулих років та сьогодення, дійсних членів-кореспондентів та академіків, повний науковий склад НАН України на теперішній час і молодих вчених. Офіційний сайт НАНУ потребує також пильних заходів кібербезпеки, які здійснюються за допомогою інноваційних сучасних систем захисту мереж та даних для забезпечення кіберстійкості. Останнє надає можливість надання своєчасної і достовірної інформації про діяльність НАН України для користувачів в Україні та за кордоном.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Очевидно, кіберзлочинність та присутність кібератак стають тим самим «другим тлом», на якому відбуваються процеси інформатизації. Й хоч вони нібито «відсторонені» від реальності або спрямовані на її деформацію, проте використання їх проти певної країни або етнічної групи, осіб чи подій свідчить про розгортання інформаційної агресії, яка має бути ідентифікована та знайдені способи протидії. Кібератаки все частіше стають узвичаєною тактикою гібридних воєн, що поєднують військові дії та інформаційну війну, політичний тиск та маніпуляцію свідомістю мас. Дослідження основних напрямів і підходів розвитку інструментів і політики кібербезпеки взагалі мають велику потенційну перспективу. Очевидно, вивчення стратегій і тактик гібридних воєн є абсолютно актуальним у сучасний момент активізації воєнних конфліктів і загострень у різних частинах світу, а також вимагає нових підходів до питань інформаційної безпеки (зокрема, кібербезпеки) та захисту національних інтересів у глобальному медіакомунікативному просторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Жилін, А. В., Шаповал, О. М., & Успенський, О. А. (2021). *Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посібн.* Київ: КПІ ім.Ігоря Сікорського. Видавництво «Політехніка».
2. *Кіберексперти про головні тенденції кібербезпеки 2023, до яких варто підготуватися.* (2023). https://10guards.com/ua/articles/cisos-top-cybersecurity-trends-2023-to-prepare-for/
3. Суський, Г. В. (2024). Питання кібербезпеки в організаціях (на прикладі кіберзахисту держреєстрів). *Розвиток основних напрямів соціогуманітарних наук: проблеми та перспективи*: *збірник матеріалів XI Всеукраїнської науково-практичної конференції з міжнародною участю,* 131–136.
4. *НАТО і стратегічна конкуренція в кіберпросторі.* (2023). NATO REVIEW. https://www.nato.int/docu/review/uk/articles/2023/06/06/nato-strategchna- konkurentsya-v-kberprostor/index.html
5. Завгородня, Ю. В. (2022). Роль НАТО у боротьбі з кіберконфліктами: політико-правовий аспект. *Регіональні студії, 30,* 62–65. https://doi.org/10.32782/2663-6170/2022.30.10
6. *The French White Paper on defence and national security*. (2013). https://ccdcoe.org/uploads/2018/10/White-paper-on-defense-2013-1.pdf
7. *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space.* (n. d.). https://assets.publishing.service.gov.uk/media/5a7c69fb40f0b62aff6c17fc/7642.pdf
8. *NATO cyber command to be fully operational in 2023.* (2023). REUTERS. https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9/
9. *A Strategic Compass for Security and Defence, EEAS.* (2022). https://www.iiea.com/blog/the-cost-of-passivity-can-the-strategic-compass-guide-the-eu-in-an-era-of-insecurity?gad_source=1&gclid=CjwKCAjwhIS0BhBqEiwADAUhcw7zJLSrySjGW1LvMbYx6qCUpC4IPAS1KQNy42S151dkj7kyio-Q4RoCIrUQAvD_BwE
10. Gulyas, A. J. (2016). *Conspiracy Theories: The Roots, Themes and Propagation of Paranoid Political and Cultural Narratives.* McFraland&Company.Inc., Publishers Jefferson, North Carolina.
11. Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.
12. КМІС. (2023). *Результати досліджень.* https://www.undp.org/uk/ukraine/press-releases/ukrayintsi-staly-chastishe-korystuvatysya-internetom-80-onlayn-shchodnya-sotsopytuvannya#:~:text
13. Брижко, В. М., & Фурашев, В. М. (2020). *Інформаційне право та інформаційне законодавство: наукове видання. (НДІІП НАПрН України).* Київ: Видавничий дім «АртЕК».
14. Пшетачник, Я., & Тарпова, С. (2022). *Війна Росії проти України: хронологія кібератак. Огляд.* ДСЄП: Дослідницька служба Європейського парламенту. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf
15. *European Union Agency for Cybersecurity (ENISA).* (2024). https: //www.enisa.europa.eu/news/cyber-europe-tests-the-eu-cyber-preparedness-in-the-energy-sector
16. Фурашев, В. (2012). Питання законодавчого визначення понятійно-категоріального апарату у сфері інформаційної безпеки. *Інформація і право, 1(4),* 46–55.
17. *Закон України «Про основні засади забезпечення кібербезпеки України».* https://zakon.rada.gov.ua/laws/show/2163-19#Text

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Heorhii Suskiy
Postgraduate student of the 2nd year of study
Institute of Software Systems of the National Academy of Sciences, Kyiv, Ukraine
ORCID ID: 0000-0001-8049-1687
nitaet@gmail.com

MODERN INFORMATION SPACE AND ISSUES OF CYBER SECURITY

Abstract. The article is devoted to identifying and clarifying the field of interaction of the concepts "information space", "information security", "cyber security" in the scientific discourse. Consideration of this interference of concepts is important from the point of view of the current situation in the Ukrainian information space, which developed after the full-scale invasion of Russian troops on February 24, 2022. Taking into account the fact that the instrument of hybrid war is also the influence on the mass consciousness through the information space, the issue of information security of the population as a whole, as well as cyber security as a set of tools for technological support in accordance the process of safe work of economic, socio-political and actually the entire system of state institutions of Ukraine, appear today, it is an urgent task not only for the relevant structures and organizations, but also for the scientific environment. The article attempts to analyze the problems inherent in the Ukrainian information space, in particular, security, technological, and legal problems, because during the Russian-Ukrainian war they became the most urgent; in addition, they are directly related to the technological conditions of ICT development. The efforts of international institutions, in particular NATO, which plays a key and regulatory role in creating an effective system for countering cyber conflicts, are undeniably important. Cyberattacks, which became especially active after the full-scale invasion of Russian troops on the territory of Ukraine in 2022, are aimed, first of all, at undermining political stability in the state, especially when world political leaders strive to find ways to settle and achieve peace in the Russian-Ukrainian war. The study of cyber security problems in the information space of the state and the determination of prospects and opportunities for their solution in modern social conditions is an urgent issue for the modern circle of ICT and cyber security specialists.

Keywords: cyber security; hybrid warfare; information space; cyber incidents.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Zhilin, A.V., Shapoval, O.M., & Uspenskyi, O.A. (2021). *Information protection technologies in information and telecommunication systems: training*. Kyiv: KPI named after Igor Sikorskyi, "Polytechnic" Publishing House.
2. *Cyber experts on the top 2023 cybersecurity trends to prepare for*. (2023). https://10guards.com/ua/articles/cisos-top-cybersecurity-trends-2023-to-prepare-for/
3. Suskiy, G. V. (2024). Issues of cyber security in organizations (on the example of cyber protection of state registers). *Development of the main directions of social and humanitarian sciences: problems and prospects*: *a collection of materials of the 11th All-Ukrainian scientific and practical conference with international participation,* 131–136.
4. *NATO and strategic competition in cyberspace.* (2023). NATO REVIEW. https://www.nato.int/docu/review/uk/articles/2023/06/06/nato-strategchna-konkurentsya-v-kberprostor/index.html
5. Zavhorodnya, Yu. V. (2022). The role of NATO in the fight against cyber conflicts: political and legal aspect. *Regional studies*, *30*, 62–65. https://doi.org/10.32782/2663-6170/2022.30.10
6. *The French White Paper on defence and national security.* (2013). https://ccdcoe.org/uploads/2018/10/White-paper-on-defense-2013-1.pdf
7. *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*. (n. d.). https://assets.publishing.service.gov.uk/media/5a7c69fb40f0b62aff6c17fc/7642.pdf
8. 8.*NATO cyber command to be fully operational in 2023*. (2023). REUTERS. https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9/

9. *A Strategic Compass for Security and Defence*, EEAS, March 2022. https://www.iiea.com/blog/the-cost-of-passivity-can-the-strategic-compass-guide-the-eu-in-an-era-of-insecurity?gad_source=1&gclid=CjwKCAjwhIS0BhBqEiwADAUhcw7zJLSrySjGW1LvMbYx6qCUpC4IPAS1KQNy42S151dkj7kyio-Q4RoCIrUQAvD_BwE
10. Gulyas, A. J. (2016). *Conspiracy Theories: The Roots, Themes and Propagation of Paranoid Political and Cultural Narratives.* McFraland&Company.Inc., Publishers Jefferson, North Carolina.
11. Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.
12. KMIS. (2023). *Research results.* https://www.undp.org/uk/ukraine/press-releases/ukrayintsi-staly-chastishe-korystuvatysya-internetom-80-onlayn-shchodnya-sotsopytuvannya#:~:text
13. Bryzhko, V. M., & Furashev, V. M. (2020). *Information law and information legislation*: *scientific edition. NDIIP NAPRN of Ukraine.* Kyiv: ArtEK Publishing House.
14. Pshetachnik J., & Tarpova S. (2022). Russia's war against Ukraine: a chronology of cyberattacks. Review. DSEP: *Research Service of the European Parliament*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf
15. *European Union Agency for Cybersecurity (ENISA).* (2024). https://www.enisa.europa.eu/news/cyber-europe-tests-the-eu-cyber-preparedness-in-the-energy-sector
16. Furashev, V. (2012). The question of the legislative definition of the conceptual and categorical apparatus in the field of information security. *Information and law, 1(4),* 46–55.
17. *The Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine".* (n. d.). https://zakon.rada.gov.ua/laws/show/2163-19#Text