Адміністративне право і процес

УДК 341:004+342.9

Тарасюк Анатолій Васильович
кандидат юридичних наук, головний науковий співробітник
Наукова лабораторія забезпечення інформаційної
та кібернетичної безпеки
НДІ інформатики і права НАПрН України
Тарасюк Анатолий Васильевич
кандидат юридических наук, главный научный сотрудник
Научная лаборатория обеспечения информационной
и кибернетической безопасности
НИИ информатики и права НАПрН Украины
Tarasyuk Anatoliy
Candidate of Law, Chief Scientist of the
Scientific Laboratory for Information and Cyber Security
Research Institute of Informatics and Law of the
National Academy of Science of Ukraine
ORCID: 0000-0002-0479-0666

МІСЦЕ ТА РОЛЬ УКРАЇНИ У ГЛОБАЛЬНИХ ІНФОРМАЦІЙНИХ ПРОЦЕСАХ: ПИТАННЯ КІБЕРБЕЗПЕКИ
МЕСТО И РОЛЬ УКРАИНЫ В ГЛОБАЛЬНЫХ ПРОЦЕССАХ: ВОПРОС КИБЕРБЕЗОПАСНОСТИ
THE PLACE AND ROLE OF UKRAINE IN GLOBAL INFORMATION PROCESSES: CYBER SECURITY ISSUES

Анотація. *Розглянуто загальні чинники актуалізації проблем кібербезпеки на глобальному рівні. Зроблено висновок, що відмінною рисою сучасного підходу до забезпечення кібербезпеки є його комплексний і*

фундаментальний характер, який включає цілу систему нормативних актів, планів і інститутів. Виявлено основні підходи й тенденції, пов'язані з виробленням на наднаціональному рівні ЄС єдиної стратегії в області кібербезпеки. Встановлено, що основна проблема ефективного забезпечення кібербезпеки полягає у створенні єдиного європейського політичного безпекового простору. Значна активність в цій сфері керівних органів ЄС стикається з нездатністю ряду країн в повному обсязі виконати всі директиви, розпорядження, регламенти та інші нормативні акти. Через складні процедури узгодження на національному і наднаціональному рівнях, що вимагає значного часу, а також через несформованість в ЄС єдиного політичного простору, держави і наднаціональні структури ЄС не завжди встигають вчасно реагувати на появу нових кіберзагроз.

У статті визначено основні стратегічні цілі національної інформаційної політики є: 1) забезпечення кібербезпеки й умов для підвищення ефективності державного управління; 2) створення сприятливих умов для забезпечення конституційних прав і свобод людини в інформаційній сфері, зміцнення та збереження моральних цінностей суспільства, традицій гуманізму і патріотизму, примноження наукового і культурного потенціалу та формування інформаційної культури населення; 3) перетворення регіональних інформаційних ресурсів на стратегічний ресурс стабільного та поступального розвитку і створення умов для гармонійної інтеграції в сучасну світову економіку на основі інформаційної відкритості та кооперації – входження в міжнародну систему поділу праці й обмінів в інформаційній сфері.

Ключові слова: *кібербезпека, глобалізація, загрози, кіберпростір, інформація, дані.*

Аннотация. *Рассмотрены общие факторы актуализации проблем*

кибербезопасности на глобальном уровне. Сделан вывод, что отличительной чертой современного подхода к обеспечению кибербезопасности является его комплексный и фундаментальный характер, включающий целую систему нормативных актов, планов и институтов. Выявлены основные подходы и тенденции, связанные с выработкой на наднациональном уровне ЕС единой стратегии в области кибербезопасности. Установлено, что основная проблема эффективного обеспечения кибербезопасности заключается в создании единого европейского политического пространства безопасности. Значительная активность в этой сфере руководящих органов ЕС сталкивается с неспособностью ряда стран в полном объеме выполнить все директивы, распоряжения, регламенты и другие нормативные акты. Через процедуры согласования на национальном и наднациональном уровнях, требует значительного времени, а также из-за несформированности в ЕС единого политического пространства, государства и наднациональные структуры ЕС не всегда успевают своевременно реагировать на появление новых киберугроз.

В статье определены основные стратегические цели национальной информационной политики являются: 1) обеспечение кибербезопасности и условий для повышения эффективности государственного управления; 2) создание благоприятных условий для обеспечения конституционных прав и свобод человека в информационной сфере, укрепление и сохранение нравственных ценностей общества, традиций гуманизма и патриотизма, приумножение научного и культурного потенциала и формирование информационной культуры населения; 3) преобразования региональных информационных ресурсов на стратегический ресурс устойчивого и поступательного развития и создания условий для гармоничной интеграции в современную мировую экономику на основе информационной открытости и кооперации - вхождение в международную систему

разделения труда и обменов в информационной сфере.

Ключевые слова: *кибербезопасность, глобализация, угрозы, киберпространство, информация, данные.*

Summary. *The general factors of actualization of cybersecurity problems at the global level are considered. It is concluded that a distinctive feature of the modern approach to cybersecurity is its comprehensive and fundamental nature, which includes a whole system of regulations, plans and institutions. The main approaches and tendencies related to the development of a unified strategy in the field of cyber security at the supranational level of the EU are revealed. It is established that the main problem of effective cybersecurity is the creation of a single European political security space. Significant activity in this area of EU governing bodies is faced with the inability of a number of countries to fully comply with all directives, orders, regulations and other regulations. Due to complex coordination procedures at the national and supranational levels, which require considerable time, as well as due to the lack of a single political space in the EU, EU states and supranational structures do not always have time to respond to new cyber threats.*

The article identifies the main strategic goals of national information policy are: 1) ensuring cybersecurity and conditions for improving the efficiency of public administration; 2) creation of favorable conditions for ensuring constitutional human rights and freedoms in the information sphere, strengthening and preservation of moral values of society, traditions of humanism and patriotism, increase of scientific and cultural potential and formation of information culture of the population; 3) transformation of regional information resources into a strategic resource of stable and progressive development and creation of conditions for harmonious integration into the modern world economy on the basis of information openness and cooperation - entry into the international system of division of labor and

exchanges in the information sphere.

Key words: *cybersecurity, globalization, threats, cyberspace, information, data.*

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. У другому десятилітті XXI ст. завдяки небувалому прогресу техніки й інформаційно-телекомунікаційних технологій наші традиційні уявлення про відстані та часовий простір зазнали докорінних змін, внаслідок яких сформувався новий тип цивілізації – інформаційна. Сутність інформаційної цивілізації полягає у розвитку інтернет-технологій і розширенні супутникового зв'язку, у практично необмежених в обсязі взаєминах і спілкуванні поза просторовими рамками, у розробці та миттєвому поширенні інформації і новин, а також появі та розвитку цифрової дипломатії.

У зазначених умовах глобальний кіберпростір перетворюється на майданчик зіткнення економічних, політичних і культурних інтересів та центрів сили сучасного світу, у дієвий інструмент формування громадської думки та її спрямування в інтересах певних гравців. Слід визнати, що поряд із позитивними і конструктивними тенденціями, які забезпечують поінформованість про новітні досягнення людства у ході розвитку світового кіберпростору, можна помітити і негативні процеси, що містять ризики для кібербезпеки держав, зокрема й України.

У сучасній ситуації у світі простежується висока динаміка міжнародних політичних процесів як на глобальному, так і на регіональному рівнях. Для світового політичного розвитку, як зауважують фахівці, притаманні два основні тренди: упорядкування і хаотизація. Тренд упорядкування (структуризації, управління, регуляції) процесів світового політичного розвитку проявляється у створенні різних формальних і неформальних структур: міжнародних організацій; міждержавних коаліцій,

союзів, форумів, до складу яких входять державні і недержавні структури (наприклад, Давоський форум); різних міждержавних «клубів» (приміром, Група восьми, Група двадцяти) тощо. Хаотизація ж спостерігається в таких процесах, як розпад об'єднань і коаліцій, очевидне порушення міжнародних договорів, норм, виникнення нових явищ, сутність яких погано узгоджується з тим, що було раніше, тощо. Нині досить виразно проглядаються міжнародні політичні процеси, що відображають хаотизацію й ускладнюють бачення перспектив світового розвитку. Тренд хаотизації є індикатором деструктивних явищ, що здійснюють негативний вплив на підвалини політичної організації міжнародного співтовариства.

За таких умов зростає рівень невизначеності напрямів світового політичного розвитку, створюються передумови для значної трансформації всієї світової соціально-політичної структури і, відповідно, – засад забезпечення міжнародної безпеки.

Аналіз останніх досліджень і публікацій. Питання забезпечення кібернетичної безпеки, в тому числі в контексті вивчення зарубіжного досвіду, були предметом наукової уваги багатьох вчених. Серед наукових праць, які слугували теоретичними орієнтирами для даної статті доцільно виокремити наступних дослідників О. Довгань [5], Т. Ткачук [8], С. Харченко [9], М. А. Носач [10], А. Благодарний [12]. Водночас, досвід забезпечення кібербезпеки у зарубіжних країнах, передусім з точки зору можливостей його використання у вітчизняних реаліях, лишається дослідженим недостатньо.

Формулювання цілей статті (постановка завдання). Проаналізувати найбільш складні та актуальні проблеми забезпечення кібербезпеки в Україні та формування державної політики у цій сфері.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Не викликає жодних сумнівів той факт, що виникнення нових засобів інформації і комунікації

та їхнє поширення у країнах сучасного світу є одним із найвагоміших чинників процесу глобалізації. Стрімке розширення інформаційної та комп'ютерної павутини зменшило відстань між людьми в різних регіонах нашої планети ще більше, ніж розвиток шляхів наземної, повітряної та водної комунікації. Щоб уявити всю глибину інформаційної трансформації, яка відбувається останнім часом, і зрозуміти динаміку, необхідно усвідомити: в умовах глобальної інформатизації зникає географія, стираються межі між зовнішньою та внутрішньою політикою, що неминуче деформує не лише «національну», але й «соціальну» ідентичності. Глобальна інформатизація розкриває багатопланові можливості для соціального інтегрування та транснаціональної взаємодії людей. Інтернет створює інші реалії для вільних контактів між людьми, які мешкають у різних країнах і є членами недержавних об'єднань.

Завдяки застосуванню сучасних інформаційно-комунікаційних технологій уявлення суб'єктів у реальному часі інтернаціоналізуються рідше, а їхню оцінку й відповідь на різні міжнародні події можна почути одразу ж після події. Усе це сприяє веденню дискусій на міжнародному рівні, створенню асоціацій між новими учасниками політичної інтерактивності.

Щоб розв’язати проблему «цифрового розриву», міжнародне співтовариство здійснює важливі кроки. На саміті «Великої вісімки», що проходив у липні 2000 р. в Японії (Окінава), наприклад, було ухвалено «Хартію глобального інформаційного співтовариства» [1]. У документі вперше у світовий контекст було введено поняття «цифровий розрив» й одним з основоположних принципів визначено імператив доступності інформаційних технологій для громадян усіх держав світу. Відповідно до основних положень Хартії було засновано міжнародну експертну раду «Група з можливостей цифрових технологій» (Digital Opportunity Task Force, G8DOT Force), головним завданням якої є пошук шляхів подолання

існуючої нерівності між різними державами у доступі до новин та інформації. Рада також розробила програму дій і представила її очільникам держав «вісімки» на саміті, що проходив улітку 2001 р. в Генуї. Результати саміту уможливили вироблення плану конкретних рекомендацій (т. зв. «Генуезька ініціатива») стосовно зазначеного питання [2]. Слід додати, що нині ініціатива з координації дій програми перейшла до Міжнародної експертної ради з інформаційно-комунікаційних технологій ООН, яку згодом було перетворено в Робочу (цільову) групу ООН з інформаційно-комунікаційних технологій (ІКТ). Виконання завдання подолання інформаційної нерівності в загальному контексті боротьби з бідністю нині покладено на ООН. Крім того, ООН у межах надання допомоги у впровадженні інформаційних технологій країнам, що розвиваються, ухвалила рішення про створення спеціального фонду обсягом 500 млн дол. Звісно, цього поки що явно недостатньо для врегулювання проблеми. З огляду на це можна зробити висновок, що нині розвиток і поширення інформаційно-комунікативних технологій у державах світу проходить дуже незбалансовано, щоб стати переконливою передумовою для соціальної інтеграції та рівності у масштабі всієї планети.

Отже, процес глобальної інформатизації, поряд із розмиванням традиційних основ національно-державної ідентичності, може сприяти актуалізації інших форм об'єднання людей. Наслідком нерівномірної та експансіоністської інформатизації може бути посилення релігійної та етнічної ідентичності людей і їхнє об'єднання за ідеологічними принципами. Це, зі свого боку, може створити передумови для появи так званих конфліктів «нового покоління».

Оскільки останнім часом інформація перетворилася в особливий ресурс будь-якої діяльності, отже вона, як і будь-який інший ресурс, потребує захисту в забезпеченні її безпеки, цілісності та збереження. Проведений аналіз доводить, що членство в регіональних організаціях

дозволяє Україні виконувати актуальні завдання у сферах політичної комунікації та кібербезпеки. Україна на цій основі має гостру потребу у спільних із розвиненими державами діях, що можуть гарантувати їй безпеку на регіональному та глобальному рівнях. З огляду на це вона здійснює політику «відкритих дверей» та активно співпрацює з міждержавними об'єднаннями, що не пред'являють попередніх вимог до рівня її військової могутності (ООН, НАТО, ОБСЄ та ін.) та соціально-економічного розвитку.

Проте, визначальним у міжнародному співробітництві нашої держави з іноземними партнерами є російський чинник. Даний чинник досить вдало визначив голова Парламентської асамблеї НАТО Паоло Алліу своєму виступі на урочистому засіданні Верховної Ради, присвяченому 20-ій річниці підписання Хартії про особливе партнерство між Україною та Організацією Північноатлантичного договору: «Агресія Росії проти України в 2014 році відкрила нову главу в міжнародних відносинах. Україна і Східна Європа на сьогоднішній день є лінією фронту із захисту європейської безпеки і захисту того світового порядку, який склався після Другої світової війни» [3].

Сьогодні беззаперечним пріоритетом державної політики у сфері забезпечення кібербезпеки є і має бути подальша інтеграція в НАТО. Серед останніх добутків нашої держави на цьому шляхи слід вважати надання у червні 2020 року Північноатлантичною радою статусу партнера з розширеними можливостями (Enhanced Opportunities Partner, EOP). EOP дозволяє країні-партнеру досягти т.зв. секторальної (оперативної) взаємосумісності з НАТО (на рівні системи логістики, зв’язку, управління військами, конкретних родів військ тощо). Крім того, EOP дає запрошеним до неї країнам-партнерам низку особливих можливостей взаємодії з НАТО [4]. До цього такий статус мали лише п'ять країн, зокрема Грузія, а також країни-члени ЄС Швеція та Фінляндія.

Варто зауважити, що на теперішньому етапі розвитку України стан її національної безпеки, насамперед, залежить від ефективності результатів процесу інформатизації та прогресу у впровадженні ІКТ у військовій сфері.

У сучасних умовах проникнення глобалізації в усі сторони суспільного життя забезпечення кібербезпеки вимагає від дослідників виконання завдання наукового осмислення та здійснення наукового аналізу проблем, що тісно пов'язані з гарантуванням кібербезпеки, як найважливішого компонента міжнародної та національної безпеки. Однак, на жаль, слід констатувати: нині майже всі підходи, що покликані забезпечити кібербезпеку України, орієнтовані на військово-політичні процеси. Безумовно, це пріоритетний напрям у забезпеченні національної безпеки. Та попри це, вони мають також акцентувати увагу на таких проблемах, як регіональна політична нестабільність, незаконний обіг наркотиків, злочинність, захист інформаційних прав людини тощо. Та й імідж держави залишається ще одним проблемним аспектом, що прямо залежить від її інформаційної політики. Нерідко нас сприймають як зручний полігон кіберзлочинності. Отже, глобалізація кіберпростору породила таке явище, як всеосяжний взаємообмін інформацією на загальносвітовому рівні.

В експертному середовищі останнім часом дедалі голосніше лунає така думка: щоб успішно втілювати в життя державну інформаційно-іміджеву політику, Україні слід створити інформаційну систему, яка б формувала та затверджувала позитивний образ нашої країни в російсько- та англомовному медіапросторах [5; 6]. У контексті зазначеного вище усе ж варто додати, що нині проблемі забезпечення кібернетичної безпеки приділяється достатня увага як на державному, так і на приватному рівнях. У зв'язку з проникненням технічних засобів обробки і передачі даних

практично в усі сфери людської діяльності особливої актуальності набуває протидія кіберзагрозам.

Аналіз актуальних загроз конфіденційній інформації, на основі якого формується система кібербезпеки і будується організація захисту інформації, розпочинається з усвідомлення та класифікації цих загроз. У зв'язку із цим підкреслимо, що теорія кібербезпеки оперує кількома формами класифікації інформаційних ризиків і загроз захисту інформації. Вважаємо за доцільне акцентувати на поділі загроз кібербезпеці, що бувають зовнішніми і внутрішніми.

У разі зовнішніх атак супротивник відшукує слабкі місця в інформаційній структурі, що уможливлять доступ до ключових вузлів внутрішньої мережі, сховищ даних, локальних комп'ютерів співробітників. При цьому зловмисник використовує широкий набір інструментів і шкідливе програмне забезпечення для виведення з ладу систем захисту, шпигунства, фальсифікації або знищення даних, копіювання, завдання шкоди об'єктам власності тощо. З огляду на це не дивно, що у доповіді Всесвітнього економічного форуму «Глобальні ризики 2012» («Global Risks 2012») [7] кібератаки визначені як одна з основних загроз світовій економіці. За ймовірністю настання кібератаки входять до п'ятірки найбільших потенційних глобальних загроз. Зазначений висновок Всесвітнього економічного форуму доводить значну актуальність і велику небезпеку електронної злочинності. Спектр загроз кібербезпеці, викликаних застосуванням шкідливого програмного забезпечення, дуже широкий. Нині, наприклад, фахівці виокремлюють такі види загроз захисту інформації [8-10]:

- упровадження вірусів та застосування інших руйнівних програмних впливів;
- упровадження програм-шпигунів з метою аналізу мережевого трафіку й отримання даних про систему та стан мережевих з'єднань;

- аналіз і модифікація / знищення встановленого програмного забезпечення;
- розкриття, розкрадання та перехоплення секретних паролів і кодів;
- використання вразливостей ПЗ для виведення з ладу програмного захисту з метою отримання несанкціонованих прав читання, копіювання, модифікації або знищення інформаційних ресурсів, а також порушення їхньої доступності;
- блокування роботи користувачів системи програмними засобами тощо.

Варто відмітити, що нами наведено базовий склад загроз кібербезпеці держави, у зв'язку з тим, що вичерпний перелік таких загроз зробити не можливо. Адже вони, у значній мірі, залежать від динаміки розвитку суспільно-політичної та міжнародної обстановки. З огляду на це стали реальними загрози: а) створенню і розвитку національної індустрії інформації, зокрема й індустрії засобів інформатизації, зв'язку та телекомунікації, задоволенню потреб внутрішнього ринку в її продукції, а також забезпеченню накопичення, ефективного використання та збереження вітчизняних і зарубіжних інформаційних ресурсів; б) безпеці інформаційних і телекомунікаційних засобів та систем, як створюваних на території України, так і вже розгорнутих й упроваджуваних.

Уже цілком очевидно, що інформаційна сфера є самостійною галуззю національної безпеки, де необхідно гарантувати охорону інформаційних ресурсів, механізми їхнього створення, застосування та поширення, комунікаційну інфраструктуру, реалізацію прав на інформацію держави, суспільства і громадян тощо.

На сучасному етапі перед Україною постало завдання здійснення переходу до якісно нового рівня управління шляхом забезпечення всіх учасників інформаційних правовідносин достовірною, своєчасною та повною інформацією. Це можливо виконати лише завдяки послідовному

реформуванню інформаційного впровадження в системі органів державної влади й управління та правильній реалізації інформаційної політики. Інформаційна політика – це здатність і можливість суб'єктів політики впливати на свідомість та психіку людей, їхню діяльність і поведінку за допомогою інформації в інтересах держави та громадянського суспільства [11]. Нині вже ні в кого не викликає сумнівів той факт, що доступність і якість інформаційних ресурсів багато в чому визначають рівень розвитку країни, її статус у світовому співтоваристві і, безперечно, стануть базовим показником статусу в перші десятиліття XXI ст. Зважаючи на це, стратегічними напрямами національної політики забезпечення кібербезпеки мають бути:

– захист національних інформаційних інтересів, забезпечення кібербезпеки, захист від інформаційних експансій, кіберзагроз та інших недружніх акцій, їхнє усунення;
– створення, розвиток і забезпечення безпеки національних інформаційних ресурсів;
– входження у світове інформаційне співтовариство.

Продовжуючи аналіз, варто додати, що стан формування інформаційних ресурсів в Україні нині, на жаль, перебуває на низькому рівні. Однією з найважливіших умов розвитку єдиного кіберпростору України є всеохопна (домашня) комп'ютеризація, що дозволила б розширити кіберпростір і відкрити широкий доступ до інформаційних ресурсів, готуючи ґрунт для діалогу влади із населенням. Заслуговує на увагу те, що в Україні поступово формується ринок інформаційно-комунікаційних технологій, продуктів і послуг, зростає мережа абонентів відкритих світових мереж, збільшується кількість персональних комп'ютерів. Прискореними темпами здійснюється забезпечення населення мобільними засобами зв'язку, розширюються національна мережа зв'язку та супутникова мережа. Триває інформатизація органів державної влади,

галузей економіки, банківської сфери, зв'язку, транспорту, освіти та культури тощо.

Інша проблема, яка потребує теоретичного осмислення та практичного вирішення це рівень інформаційно-просвітницької, ідеологічної й освітньої роботи із протидії радикальній ідеології та екстремізму. Така робота потребує значного посилення. Серед найбільших проблем можемо виокремити, зокрема такі:

– брак фахівців у галузі інформаційної протидії екстремізму і тероризму;
– недостатня кількість інформаційної та довідкової літератури стосовно екстремістських і терористичних організацій;
– спостерігається відсутність пропаганди та наочної агітації;
– слабка роль засобів масової інформації у запобіганні та профілактиці екстремізму, а також у висвітленні антитерористичної й антиекстремістської діяльності державних органів.

У розрізі зазначеного ми підтримуємо думку М. Стрельбицького та А. Благодарного, що запобігти екстремізм можна лише спільними зусиллями державних органів та громадськості, спрямованими на підвищення правової і загальної культури населення, поліпшення соціально-економічних умов життя людей, формування позитивного іміджу держави [12, с. 43].

Висновки та перспективи подальших досліджень у даному напрямку. Проведене дослідження дає можливість зробити ряд важливих висновків, зокрема в частині визначення загроз безпеці в сучасній Україні в кіберсфері належать:

– наявність зовнішніх і внутрішніх центрів політичної, релігійної, міжнаціональної та іншої напруженості у прикордонних районах суміжних Україні країн;

– збільшення на державному кордоні та прикордонній території масштабів розвідувально-підривної діяльності іноземних спецслужб;
– здійснення бандформуваннями бойових дій і терористичних акцій у прикордонній смузі та прикордонних територіях, зокрема проти військ й органів Державної прикордонної служби України;

З огляду на зазначене вище варто підкреслити, що державним органам необхідно вдосконалювати нормативно-правові акти, які регулюють питання протидії використанню Інтернету в терористичних й екстремістських цілях, а також забезпечують національні інтереси суверенної України в інформаційній сфері.

Проблема забезпечення глобальної кібербезпеки стала зворотною стороною глобальної інформатизації людської спільноти. В усіх основних групах учасників глобального інформаційного суспільства Україна представлена досить активно. Зважаючи на це, забезпечення національної безпеки нашої країни безпосередньо залежить від рівня підтримки глобальної кібербезпеки.

Література

1. Окинавская хартия глобального информационного общества (Окинава, 22 июля 2000 года). URL: https://zakon.rada.gov.ua/laws/show/998_163#Text
2. Jeffrey A. Hart The Digital Opportunities Task Force: The G8's Effort to Bridge the Global Digital Divide. 26 p. URL: https://www.researchgate.net/publication/228852360_The_Digital_Opportunities_Task_Force_The_G8's_Effort_to_Bridge_the_Global_Digital_Divide
3. Урочисте засідання, присвячене 20-ій річниці підписання Хартії про особливе партнерство між Україною та Організацією Північно-Атлантичного договору // Прес-служба Апарату Верховної Ради

України. URL: https://www.rada.gov.ua/preview/anons_acred/146596.html

4. 12 червня 2020 року Україна отримала статус члена Програми розширених можливостей НАТО (NATO's Enhanced Opportunities Program – EOP). Урядовий портал: URL: https://www.kmu.gov.ua/news/ukrayina-otrimala-status-chlena-programi-rozshirenih-mozhlivostej-nato
5. Ткачук Т.Ю., Довгань О.Д. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс // Інформація і право. 2018. № 2 (25). С. 73-85.
6. Баровська А.В. Понятійно-категоріальний апарат інформаційної сфери: правовий аспект // Аналітична записка. Національний інститут стратегічних досліджень. URL: http://old2.niss.gov.ua/articles/532/
7. Global Risks 2012 Seventh Edition. Insight Report. URL: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf
8. Ткачук Т. Ю. Механізми протидії інформаційним загрозам зовнішніх джерел // Вісник НТУ України «Київський політехнічний інститут». Політологія. Соціологія. Право. 2017. № 1-2. С. 242-246.
9. Харченко С.О. Наукові підходи до класифікації загроз інформаційній безпеці. Серія: Державне управління, 2019. № 2 (66). С. 191-197.
10. Носач А.В. Загрози національній безпеці як обов'язкова ознака злочинності, що посягає на державний суверенітет і територіальну цілісність України // Право і суспільство. 2019. №3. С. 50-56.
11. Литвин Н. А. Наукові підходи щодо визначення поняття державної інформаційної політики в Україні // Наука і правоохорона. 2019. № 1(43). С. 253-261.
12. Стрельбицький М.П., Благодарний А.М. Превентивна протидія екстремістським проявам в Україні: правові та організаційні аспекти //

Information Security of the Person, Society and State. 2019. № 1 (25). C. 37-45.

References

1. Okynavskaja khartyja ghlobaljnogho ynformacyonnogho obshhestva (Okynava, 22 yjulja 2000 ghoda). URL: https://zakon.rada.gov.ua/laws/show/998_163#Text
2. Jeffrey A. Hart The Digital Opportunities Task Force: The G8's Effort to Bridge the Global Digital Divide. 26 r. URL: https://www.researchgate.net/publication/228852360_The_Digital_Opportunities_Task_Force_The_G8's_Effort_to_Bridge_the_Global_Digital_Divide
3. Urochyste zasidannja, prysvjachene 20-ij richnyci pidpysannja Khartiji pro osoblyve partnerstvo mizh Ukrajinoju ta Orghanizacijeju Pivnichno-Atlantychnogho doghovoru // Pres-sluzhba Aparatu Verkhovnoji Rady Ukrajiny. URL: https://www.rada.gov.ua/preview/anons_acred/146596.html
4. 12 chervnja 2020 roku Ukrajina otrymala status chlena Proghramy rozshyrenykh mozhlyvostej NATO (NATO's Enhanced Opportunities Program – EOP) // Urjadovyj portal: URL: https://www.kmu.gov.ua/news/ukrayina-otrimala-status-chlena-programi-rozshirenih-mozhlivostej-nato
5. Tkachuk T.Ju., Dovghanj O.D. Pravove zabezpechennja informacijnoji bezpeky derzhavy jak pidghaluzj informacijnogho prava: teoretychnyj dyskurs // Informacija i pravo. 2018. # 2 (25). S. 73-85.
6. Barovsjka A.V. Ponjatijno-kateghorialjnyj aparat informacijnoji sfery: pravovyj aspect // Analitychna zapyska. Nacionaljnyj instytut strateghichnykh doslidzhenj. URL: http://old2.niss.gov.ua/articles/532/

7. Global Risks 2012 Seventh Edition. Insight Report. URL: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf
8. Tkachuk T. Ju. Mekhanizmy protydiji informacijnym zaghrozam zovnishnikh dzherel // Visnyk NTU Ukrajiny «Kyjivsjkyj politekhnichnyj instytut». Politologhija. Sociologhija. Pravo. 2017. # 1-2. S. 242-246.
9. Kharchenko S.O. Naukovi pidkhody do klasyfikaciji zaghroz informacijnij bezpeci // Serija: Derzhavne upravlinnja, 2019. # 2 (66). S. 191-197.
10. Nosach A.V. Zaghrozy nacionaljnij bezpeci jak obov'jazkova oznaka zlochynnosti, shho posjaghaje na derzhavnyj suverenitet i terytorialjnu cilisnistj Ukrajiny // Pravo i suspiljstvo. 2019. #3. S. 50-56.
11. Lytvyn N. A. Naukovi pidkhody shhodo vyznachennja ponjattja derzhavnoji informacijnoji polityky v Ukrajini // Nauka i pravookhorona. 2019. # 1(43). S. 253-261.
12. Streljbycjkyj M.P., Blaghodarnyj A.M. Preventyvna protydija ekstremistsjkym projavam v Ukrajini: pravovi ta orghanizacijni aspekty // Information Security of the Person, Society and State. 2019. # 1 (25). S. 37-45.