ISSN 2311-8040

УДК 342.9
DOI https://doi.org/10.32782/2311-8040/2023-1-4

Шопіна Ірина Миколаївна,
доктор юридичних наук, професор,
професор кафедри адміністративно-правових дисциплін
Інституту права,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: https://orcid.org/0000-0003-3334-7548

ІНФОРМАЦІЙНА БЕЗПЕКА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Анотація. *У статті визначено особливості інформаційної безпеки цифрової трансформації та її забезпечення. Сформульовано визначення цифрової трансформації і з'ясовано, що вона може розглядатися у двох аспектах: телеологічному (як мета органів публічного адміністрування) і в діяльнісному (як сукупність дій, спрямованих на реалізацію функцій, методів, заходів управлінської системи підприємства, установи, організації або органу публічної влади).*

Акцентовано увагу на тому, що активізація процесів цифрової трансформації потребує більш широкого застосування заходів інформаційної безпеки, що обумовлено зростанням кількості та інтенсивності інформаційних загроз у тих сферах суспільних відносин, в яких вказана трансформація здійснюється особливо швидкими темпами.

Визначено, що інформаційна безпека цифрової трансформації – це ідеальна модель позбавленого інформаційних загроз середовища, в якому динамічно відбувається впровадження інформаційних (цифрових) технологій у всі сфери функціонування та життєдіяльності фізичних та юридичних осіб з метою найбільш повної реалізації ними своїх інформаційних та інших прав, свобод та інтересів. Розуміння сутності цієї моделі можливо або через суб'єктивне сприйняття суб'єктів інформаційних правовідносин, або через систему кількісних критеріїв, які характеризують досягнення цілей цифрової трансформації.

Зроблено висновок, що від інформаційної безпеки цифрової трансформації слід відрізняти забезпечення цього явища. Забезпечення інформаційної безпеки цифрової трансформації – це сукупність дій органів публічного адміністрування, правоохоронних, правозахисних органів та військових формувань, судів, підприємств, установ, організацій всіх форм власності, інститутів громадянського суспільства та окремих громадян, спрямована на оптимізацію організації, управління, функцій та методів діяльності, підвищення рівня інформаційної культури та інформаційної свідомості суб'єктів правовідносин за рахунок використання ними інформаційних (цифрових) технологій.

Ключові слова: *інформаційна безпека, цифрова трансформація, забезпечення інформаційної безпеки, інформаційні правовідносини, інформаційні технологія, інформаційні права, інформаційна культура.*

Shopina Iryna. INFORMATION SECURITY OF DIGITAL TRANSFORMATION

Abstract. *The article defines the features of information security of digital transformation and its provision. The definition is formulated by digital transformation and it is found that it can be considered in two aspects: teleological (as the goal of public administration bodies), and in activity (as a set of actions aimed at implementing the functions, methods, measures of the management system of an enterprise, institution, organization or body of public authorities).*

Attention is focused on the fact that the activation of digital transformation processes requires a more active application of information security measures, which is due to the increase in the number and intensity of information threats in some areas of public relations.

The conclusion is made that the information security of digital transformation is an ideal model of an environment devoid of information threats, in which information (digital) technologies are dynamically introduced into all spheres of functioning and life of individuals and legal entities in order to fully realize their information and other rights, freedoms and interests. Understanding the essence of this model is possible either through the subjective perception of the subjects of information legal relations, or through a system of quantitative criteria that characterize the achievement of the goals of digital transformation.

Attention is focused on the fact that the provision of this phenomenon should be distinguished from the information security of digital transformation. Ensuring the information security of digital transformation is a set of actions of public administration bodies, law enforcement, human rights bodies and military formations, courts, enterprises,

institutions, organizations of all forms of ownership, civil society institutions and individual citizens, aimed at optimizing the organization, management, functions and methods of activity , raising the level of information culture and information consciousness of the subjects of legal relations through the use of information (digital) technologies.

Key words: *information security, digital transformation, information security, information legal relations, information technology, information rights, information culture.*

Вступ. Проблеми забезпечення інформаційної безпеки в Україні набули особливої актуальності ще у 2014 році, із початком збройної агресії Російської Федерації проти нашої держави. Постійне проведення противником інформаційно-психологічних операцій продовжується і після набуття збройною агресією держави-терориста повномасштабного характеру. Нині ціна помилки в інформаційній сфері є надзвичайно високою – будь-які відомості та дані активно використовуються Російською Федерацією для розвідування позицій підрозділів Збройних Сил України та інших військових формувань, проведення шантажу на основі компрометуючої інформації, здійснення терористичних актів проти цивільного населення та об'єктів критичної інфраструктури.

Перед початком повномасштабної збройної агресії Російської Федерації наша держава знаходилася на піку розвитку цифровізації процесів взаємодії громадянина і держави, а також діяльності органів публічної влади. Незважаючи на певні недоліки системи «Дія», а також єдиних та державних реєстрів (переважно пов'язаних із їх вразливістю до витоку персональних та інших даних), можна констатувати, що Україна вийшла на одне з перших місць в Європі у сфері цифрової трансформації органів публічного адміністрування. Єдина судова інформаційно-телекомунікаційна система, яка включає у тому числі й підсистему «Електронний суд», дозволила зробити великий крок уперед на шляху підвищення доступності правосуддя. Цифровізація сфери публічних послуг підвищила зручність та інклюзивність користування ними для громадян, а також сприяла зниженню корупційних ризиків у найбільш чутливих сферах правовідносин.

У теперішній час об'єкти енергетичної інфраструктури України зазнали значних руйнувань, що негативно позначилося на рівні доступу до низки публічних послуг. Разом з тим, враховуючи, що відмова від здобутків цифровізації означала б суттєвий крок назад, перед Україною постало складне завдання продовження цифрової трансформації в умовах правового режиму воєнного стану, з урахуванням вимог інформаційної безпеки, що і обумовлює актуальність цієї статті.

Питання правового забезпечення інформаційної безпеки та цифрової трансформації розглядали у своїх роботах І. Арістова, О. Баранов, К. Бєляков, І. Бондар, В. Гавловський, М. Гаврильців, О. Дзьобань, О. Довгань, О. Золотар, Р. Калюжний, М. Ковалів, Б. Кормич, І. Кушнір, А. Марущак, В. Пилипчук, С. Онопрієнко, В.Фурашев, В. Цимбалюк та інші автори. Однак системний зв'язок між інформаційною безпекою та цифровою трансформацією в умовах правового режиму воєнного стану досліджено нині ще недостатньо, що обумовлює спрямованість наукових пошуків.

Мета статті – визначення сутності інформаційної безпеки цифрової трансформації та діяльності з її забезпечення.

Матеріали та методи. Для досягнення мети статті використовувалися загальнонаукові та спеціально-правові методи наукового пізнання. Методи аналізу та синтезу застосовувалися під час з'ясування сутності підходів до вивчення феноменів інформаційної безпеки та цифрової трансформації. Компаративно-правовий метод надав змогу визначити особливості формулювання цілей цифрової трансформації та основі кількісних критеріїв, а також виокремити тенденції зростання інформаційних ризиків, які супроводжують процеси цифрової трансформації. Структурно-правовий та формально-логічний методи дозволили проаналізувати підходи до явища інформаційної безпеки. Метод

ISSN 2311-8040

моделювання дав змогу сформулювати визначення понять інформаційної безпеки цифрової трансформації та її забезпечення.

Результати. Значущість категорії інформаційної безпеки настільки загальновизнана й деталізована у наукових дослідженнях, що деякі вчені вважають цей феномен навіть не інститутом, а підгалуззю інформаційного права [1]. Не вдаючись до дискусій з приводу відмінностей між підгалузями та інститутами права, які точаться багато десятиліть, зауважимо, що важливість інформаційної безпеки як правового феномену підтверджується, на нашу думку, двома основними факторами: її практичною роллю для підтримання життєдіяльності держави (саме прогалини у сфері інформаційної безпеки сприяли швидкому і безперешкодному відновленню влади Талібана в Афганістані), а також її ґрунтовним теоретичним осмисленням у багатьох науках (інформаційному, адміністративному, кримінальному, фінансовому, цивільному праві, праві національної безпеки та воєнному праві тощо).

Враховуючи, що метою статті є пошук співвідношення між цифровою трансформацією та інформаційною безпекою, спробуємо спочатку розглянути структуру останньої, щоб знайти в ній місце для поєднання з іншими правовими категоріями.

Існує декілька підходів до структури інформаційної безпеки. Так, її розглядають як відносини, що складаються в інформаційній сфері і включають: суспільні відносини, що забезпечують реалізацію права на інформацію і на охорону інформації від незаконного втручання; суспільні відносини, що забезпечують безпеку інформаційних ресурсів; суспільні відносини, що забезпечують безпеку використання інформаційно-телекомунікаційних технологій [2]. Безумовно, будь-яке правове явище пов'язано із суспільними відносинами, оскільки право виступає їх універсальним регулятором, водночас це лише один із аспектів, в якому можна розглядати інформаційну безпеку. Багатогранність цього феномену обумовлює необхідність його розгляду з використанням широкого арсеналу методів наукового пізнання, як правових, так і запозичених в інших галузях наукових знань.

У діяльнісному аспекті інформаційна безпека розглядається як феномен, що включає до себе: інформаційне забезпечення діяльності; захист інформаційного ресурсу; протидію негативному інформаційному впливу [3, с. 31]. Діяльнісний підхід, запозичений правовими науками у методологічному апараті загальної психології, дуже ефективно використовується у правничих дослідженнях. Разом з тим не зовсім зрозуміло, як співвідносять між собою захист і протидія, адже ці терміни є близькими за змістом, на наш погляд, захист включає у тому числі протидію, втім, ці питання потребують окремих досліджень.

Адміністративно-правовий підхід до структури інформаційної безпеки передбачає наділення цього феномену адміністративно-правовими властивостями та включення його до всіх рівнів структури адміністративно-правового регулювання. Відповідно до вказаного підходу структуру інформаційної безпеки ототожнюють з її адміністративно-правовим регулюванням і розглядають як сукупність таких елементів: 1) фізичні та юридичні особи, суспільство, держава, які є формальними носіями прав, свобод і законних інтересів у сфері інформаційної безпеки та охороняються адміністративно-правовими засобами і способами; 2) охоронювані адміністративно-правовими засобами, формально визначеними у Конституції України та інших нормативно-правових актах інформаційні права, свободи і законні інтереси громадян (об'єктами безпеки у сфері адміністративно-правового регулювання); 3) формально позначені типізовані умови (ситуації), що виникають та стають шкідливими і небезпечними у сфері адміністративно-правового регулювання інформаційних відносин та їх забезпечення (адміністративно дозволені дії (діяльність) фізичних та юридичних осіб; адміністративно заборонені дії (бездіяльність); адміністративно-правові казуси). При цьому критерієм, що визначає структуру адміністративно-правового регулювання відносин у сфері інформаційної безпеки особи,

суспільства і держави, виступають формально закріплені у нормативно-правових актах носії адміністративно охоронюваних законних інтересів, на підставі чого існує потреба у виокремленні таких видів інформаційної безпеки: безпека особи, суспільна/національна безпека і державна безпека [4, с. 173]. Погоджуючись з наведеним науковцями критеріями поділу елементів інформаційної безпеки на три категорії залежно від їх носіїв, зауважимо, однак, що повне ототожнення структури інформаційної безпеки зі структурою адміністративно-правового регулювання уявляється нам не зовсім можливим з огляду на поєднання у структурі інформаційної безпеки приватноправових та публічно-правових відносин. При цьому в наукових дослідженнях, присвячених проблемам інформаційної безпеки, і у програмах інвестицій, спрямованих на безпосереднє забезпечення інформаційної безпеки, найбільша увага приділяється саме приватним аспектам досліджуваного явища (це цілком логічно, адже провідну роль серед замовників наукових досліджень та технологічних рішень у сфері інформаційної безпеки займають великі міжнародні корпорації, бюджети яких перевищують розміри бюджетів багатьох держав світу).

Найбільш розгалужений підхід до структури інформаційної безпеки включає низку її різнопланових критеріїв. Так, у широкому аспекті інформаційна безпека класифікується: а) за джерелом походження повноважень щодо здійснення заходів із забезпечення інформаційної безпеки (природні права і свободи людини, Конституція України, закони України, підзаконні правові акти); б) за видами суб'єктів, які забезпечують інформаційну безпеку (людина і громадянин, інститути громадянського суспільства, органи державної влади, органи місцевого самоврядування, військові формування, підприємства, установи та організації всіх форм власності); в) за ступенем обов'язковості здійснення заходів із забезпечення інформаційної безпеки: основна (для спеціально уповноважених органів публічної влади та військових формувань); факультативна (для інших органів публічної влади); делегована (для підприємств, установ та організацій, яким повноваження щодо здійснення заходів інформаційної безпеки делеговано відповідними правовими актами; необов'язкова (для громадян і суб'єктів громадянського суспільства). У вузькому аспекті інформаційна безпека включає такі види: а) за критерієм суб'єктів, охоплених заходами інформаційної безпеки (інформаційна безпека людини, корпорацій, органів державної влади та місцевого самоврядування, громадянського суспільства і держави в цілому); б) за критерієм інформаційних загроз (політична інформаційна безпека, воєнна інформаційна безпека, економічна інформаційна безпека, екологічна інформаційна безпека тощо); в) за критерієм досягнутих результатів (досконала і недосконала інформаційна безпека) [5, с. 61–62]. Цей підхід вбачається нам таким, що враховує максимальну кількість аспектів досліджуваного явища, разом з тим хотілося б згадати про позицію О. Золотар, яка наголошує на некоректності ототожнення інформаційної безпеки людини з її забезпеченням. Це, на думку дослідниці, є методологічною помилкою, оскільки забезпечення (щодо інформаційної безпеки людини) стосується більшою мірою заходів (технічних, організаційних, правових, кадрових тощо), а сама безпека – суб'єктивного переживання людиною, що відображає активний зміст її свідомості, яка здатна прогнозувати, передбачити і уявити небезпеки, а також своєчасно і адекватно на них відреагувати. Наступною дилемою, що має місце в правових (і не лише) дослідженнях інформаційної безпеки, вчена називає протиставлення її як стану і процесу. На її думку, у самому загальному вигляді під інформаційною безпекою людини можна розуміти її здатність зберігати свої істотні властивості і забезпечувати власне існування і розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Тобто не слід обмежуватись розумінням її як «стану», а найбільш відповідним, на нашу думку, є комплексний підхід, згідно з яким інформаційна безпека визначається через її істотні риси, найбільш важливі основні функції, беручи

ISSN 2311-8040

до уваги постійну динаміку інформаційних і соціальних систем [6, с. 71]. Отже, розгляд інформаційної безпеки у динаміці дозволяє не лише з'ясувати притаманні їй закономірності та ризики, а й визначити ступінь впливу на неї кожного з них. Тому структура інформаційної безпеки має включати й розмежування залежно від перманентності або дискретності впливу на неї зовнішніх та внутрішніх факторів, а також залежно від того, статичні чи динамічні особливості узяті дослідником, законотворцем або представником публічної адміністрації як основоположні.

Структура інформаційної безпеки відображує сучасні особливості розвитку науки інформаційного права, а також завдання, які постають перед дослідником у кожному конкретному випадку. Крім того, заслуговує на увагу розмежування між інформаційною безпекою як ідеальним конструктом, що відображується у свідомості суб'єкта та має суб'єктивний характер, інформаційною безпекою як метою, рівень досягнення якої вимірюється за допомогою конкретних (кількісних) показників, і інформаційною безпекою як діяльністю або процесом (у даному випадку доречним є використання терміну «забезпечення інформаційної безпеки»). Це не означає відмову від розмежування між видами інформаційної безпеки за суб'єктами, змістом, джерелами повноважень чи загроз, однак ці критерії, на нашу думку, носять вторинний характер. Методологічно вірним було б, на нашу думку, спочатку визначити, який саме (моделюючий, телеологічний чи діяльнісний) підхід буде найбільше відповідати цілям дослідника, а вже потім розгалужувати один з вказаних підходів, будуючи власну класифікацію.

Цифрова трансформація, яку ми розуміємо як оптимізацію організації, управління, функцій та методів діяльності, інформаційної культури та інформаційної свідомості суб'єктів правовідносин за рахунок використання ними інформаційних технологій, може розглядатися у двох аспектах: телеологічному, як мета органів публічного адміністрування, і в діяльнісному, як сукупність дій, спрямованих на реалізацію функцій, методів, заходів, що є частиною управлінської системи підприємства, установи, організації або органу публічної влади. Прикладом телеологічного розуміння може бути відображення у проєкті Рішення Європейського Парламенту та Ради 2021/0293 про запровадження Політичної програми до 2030 року «Шлях до цифрового десятиліття цілей цифрового розвитку до 2030 року, до яких віднесено: 1) населення з цифровими навичками та висококваліфіковані професіонали з цифрових технологій: принаймні 80% осіб у віці 16-74 років мають принаймні базові цифрові навички; щонайменше 20 мільйонів зайнятих у сфері інформації та зв'язку працюють як спеціалісти з технологій із конвергенцією між жінками і чоловіками; 2) безпечні, продуктивні та стійкі цифрові інфраструктури: усі європейські домогосподарства охоплені гігабітною мережею з усіма населеними пунктами, охопленими 5G; виробництво передових та стійких напівпровідників у Європейському Союзі становить не менше 20% світового виробництва у вартісному вираженні; розгорнуто принаймні 10000 кліматично нейтральних високозахищених «граничних вузлів» в Європейському Союзі, розповсюджених у спосіб, який гарантує доступ до послуг даних з низькою затримкою (кілька мілісекунд) незалежно від того, де розташовані підприємства; до 2025 року в Європейському Союзі з'явиться перший комп'ютер із квантовим прискоренням, прокладаючи шлях до того, щоб Європейський Союз був на передньому краї квантових технологічних можливості до 2030 року; 3) цифрова трансформація бізнесу: принаймні 75% підприємств Європейського Союзу взяли на себе: послуги хмарних обчислень; великі дані; штучний інтелект; охоплення понад 90% малих і середніх підприємств Союзу принаймні базовим рівнем цифрової інтенсивності; Європейський Союз нарощує коло своїх інноваційних масштабів і вдосконалюється доступ до фінансування, що призведе до принаймні подвоєння кількості підприємств з високим рівнем капіталізації активів; 4) цифровізація державних послуг: 100% доступне онлайн

надання ключових державних послуг для громадян та підприємств Європейського Союзу; 100% громадян Союзу мають доступ до своїх медичних записів (електронні медичні картки (EHR)); принаймні 80% громадян Союзу використовують рішення цифрової ідентифікації (ID)» [7]. Діяльнісне розуміння цифрової трансформації базується на здобутках теорії управління та соціальної психології і передбачає структурування дій суб'єктів суспільних відносин, дотичних до впровадження інформаційних технологій у процеси функціонування та життєдіяльності фізичних та юридичних осіб.

Хронологічно вироблення телеологічного підґрунтя цифрової трансформації має передувати розробці її діяльнісних аспектів: за відсутності цілей, формалізованих і доведених до відома всіх суб'єктів, планування їх конкретних дій уявляється марним. Втім, в національній практиці таке спостерігалося неодноразово: як приклад можна навести таке декларативне завдання Національної програми інформатизації, як «застосування та розвиток сучасних інформаційних технологій у відповідних сферах суспільного життя України» [8], простежити ступінь реалізації якого не уявляється можливим.

Отже, можливість досягнення поставленої мети залежить від коректності її формулювання, що, у випадку з інформаційною безпекою цифрової трансформації, потребує використання кількісних критеріїв, які дозволяють порівнювати між собою різні сфери суспільних відносин, різні проміжки часу тощо.

Успішна діяльність з цифрової трансформації залежить також від правильного вибору тих сфер суспільних відносин, стосовно яких можна прогнозувати зростання інформаційних ризиків. Однією з таких сфер в Україні є сфера освіти, цифрова трансформація якої протягом трьох років (з моменту встановлення карантинних обмежень внаслідок пандемії коронавірусної хвороби COVID-19) розвивалася надзвичайно швидкими темпами. Як свідчить досвід США і держав-членів Європейського Союзу, спостерігається посилення трьох основних типів кіберзагроз для сфери вищої освіти. По-перше, це значні фінансові втрати, спричинені програмами-вимагачами або знищеними даними. Хоча кібератаки університетів за допомогою програм-вимагачів не є новим явищем, однак протягом останніх кількох років їх стрімко зросла, причому швидше, ніж в інших секторах, особливо після пандемії COVID-19 [9, с. 141]. Наприклад, кількість атак програм-вимагачів на заклади освіти зросла з 6% у 2019 році до 15% у 2020 році, тоді як у сфері охорони здоров'я за цей же час кількість таких атак зросла з 21% до 23% [10]. Серед найбільш значущих прикладів – Маастрихтський університет у Нідерландах заплатив 220 000 доларів як викуп у 2019 році [11]; Університет Юти заплатив 457 000 доларів [12]. Той факт, що вища освіта стає прибутковою мішенню для кіберзлочинців, викликає особливу тривогу, враховуючи внесок сектора у ВВП, на який уже вплинули пандемічний фінансовий стрес [9, с. 141].

Другим ключовим впливом кіберзагроз на освіту є порушення процесів навчання. Оскільки все більше навчальних закладів переходять на дистанційне навчання, кібербезпека постає серйозною проблемою. За оцінками, кількість атак розподіленої відмови в обслуговуванні (DDOS) на онлайн-ресурси навчальних закладів зросла на 350 відсотків у період із січня по червень 2020 року порівняно з аналогічним періодом 2019 р. Під час таких атак студенти та викладачі не мали доступу до навчальних матеріалів протягом періоду від декількох днів до декількох тижнів. По-третє, залучення багатьох університетів до досліджень, які є стратегічно чи економічно значущими, робить їх привабливими мішенями для крадіжки інтелектуальної власності. Наприклад, у 2018 році Міністерство юстиції США звинуватило дев'ятьох осіб, пов'язаних із Революційною гвардією Ірану, у хакерських атаках на 144 університети США та 176 інших університетів по всьому світу та викрадення 31 терабайта даних, включаючи дослідницькі, академічні та приватні дані та інтелектуальну власність [9, с. 142].

Отже, активізація процесів цифрової трансформації потребує більш активного

ISSN 2311-8040

застосування заходів інформаційної безпеки, що обумовлено зростанням кількості та інтенсивності інформаційних загроз у тих сферах суспільних відносин, в яких вказана трансформація здійснюється особливо швидкими темпами. Ці процеси перебувають у нерозривному взаємозв'язку: ефективність інформаційної безпеки обумовлює досягнення цілей цифрової трансформації, тоді як активізація процесів цифрової трансформації викликає необхідність застосування, розвитку та вдосконалення засобів забезпечення інформаційної безпеки.

Висновки. Інформаційна безпека цифрової трансформації – це ідеальна модель позбавленого інформаційних загроз середовища, в якому динамічно відбувається впровадження інформаційних (цифрових) технологій у всі сфери функціонування та життєдіяльності фізичних та юридичних осіб з метою найбільш повної реалізації ними своїх інформаційних та інших прав, свобод та інтересів. Розуміння сутності цієї моделі можливо або через суб'єктивне сприйняття суб'єктів інформаційних правовідносин, або через систему кількісних критеріїв, які характеризують досягнення цілей цифрової трансформації.

Від інформаційної безпеки цифрової трансформації слід відрізняти забезпечення цього явища. Забезпечення інформаційної безпеки цифрової трансформації – це сукупність дій органів публічного адміністрування, правоохоронних, правозахисних органів та військових формувань, судів, підприємств, установ, організацій всіх форм власності, інститутів громадянського суспільства та окремих громадян, спрямована на оптимізацію організації, управління, функцій та методів діяльності, підвищення рівня інформаційної культури та інформаційної свідомості суб'єктів правовідносин за рахунок використання ними інформаційних (цифрових) технологій.

Список використаних джерел:

1. Довгань О.Д., Ткачук Т.Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. Інформація і право. 2018. № 2(25). С. 73–85. URL: http://ippi.org.ua/sites/default/files/9_8.pdf.

2. Малашко О.Є., Ковалів М.В. Теоретична конструкція поняття «інформаційна безпека». Інтернаука. Серія: «Юридичні науки». 2020. № 10. С. 20–33. URL: https://doi.org/10.25313/2520-2308-2020-10-6350.

3. Мохнюк А.М., Скорук О.В. Організація та управління інформаційною безпекою на підприємстві: конспект лекцій. Луцьк : ПП «Поліграфія», 2017. 99 с.

4. Остапенко О., Баїк О. Адміністративно-правова природа інформаційної безпеки. Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки». 2021. № 3(31). С. 167 179. URL: http: //doi.org/10.23939/law2021.31.167.

5. Онопрієнко С. Класифікація видів інформаційної безпеки як правової категорії. Вісник Київського національного університету імені Тараса Шевченка. Серія: «Військово-спеціальні науки». 2022. № 1(49). С. 60–62. URL: https://miljournals.knu.ua/index.php/visnuk/article/view/898/841.

6. Золотар О.О. Правові основи інформаційної безпеки людини : дис. …докт. юрид. наук : 12.00.07. Київ, 2018. 479 с.

7. Proposal for a Decision of the European Parliament and of the Council Establishing the 2030 Policy Programme "Path to the Digital Decade" (Text with EEA relevance). URL: https://data.consilium.europa.eu/doc/document/ST-11900-2021-INIT/en/pdf.

8. Про Національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР. Відомості Верховної Ради України. 1998. № 27-28. Ст. 181.

9. Fouad N. S. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy. 2021. № 6(2). P. 137–154. URL: https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1973526.

10. Education Technology. Ransomware Attacks on Education Sector More Than Doubled Since 2019. URL: https://edtechnology.co.uk/cybersecurity/ransomware-attackseducation-sector-doubled-since-2019 /. Цит. за: Fouad N. S. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy. 2021. № 6(2). P. 137–154. URL: https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1973526.

11. Reuters. University of Maastricht Says It Paid Hackers 200,000-Euro Ransom (2020). URL: https://uk.reuters.com/article/us-cybercrime-netherlands-university-idUKKBN1ZZ2HH. Цит. за: Fouad N. S. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy. 2021. № 6(2). P. 137–154. URL: https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1973526.

12. University of Utah Update on Data Security Incident (2020). URL: https://attheu.utah.edu/facultystaff/university-of-utah-update-on-data-security-incident /. Цит. за: Fouad N. S. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy. 2021. № 6(2). P. 137–154. URL: https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1973526.

References:

1. Dovhan, O.D., Tkachuk, T.Iu. (2018). Pravove zabezpechennia informatsiinoi bezpeky derzhavy yak pidhaluz informatsiinoho prava: teoretychnyi dyskurs [Legal provision of information security of the state as a sub-branch of information law: theoretical discourse]. Informatsiia i pravo, 2(25), 73-85. Retrieved from. http://ippi.org.ua/sites/default/files/9_8.pdf [in Ukrainian].

2. Malashko, O. Ye., Kovaliv, M. V. (2020). Teoretychna konstruktsiia poniattia «informatsiina bezpeka» [Theoretical construction of the concept of "information security"]. Internauka. Seriia: «Yurydychni nauky», 10, 20-33. Retrieved from. https://doi.org/10.25313/2520-2308-2020-10-6350. [in Ukrainian].

3. Mokhniuk, A. M., Skoruk, O. V. (2017). Orhanizatsiia ta upravlinnia informatsiinoiu bezpekoiu na pidpryiemstvi: konspekt lektsii [Organization and management of information security at the enterprise: lecture notes]. Lutsk, 99. [in Ukrainian].

4. Ostapenko, O., Baik, O. (2021). Administratyvno-pravova pryroda informatsiinoi bezpeky [Administrative and legal nature of information security]. Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Seriia: «Yurydychni nauky», 3 (31), 167-179. Retrieved from. http: //doi.org/10.23939/law2021.31.167. [in Ukrainian].

5. Onopriienko, S. (2022). Klasyfikatsiia vydiv informatsiinoi bezpeky yak pravovoi katehorii [Classification of types of information security as a legal category]. Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Seriia: «Viiskovo-spetsialni nauky», 1 (49), 60-62. Retrieved from. https://miljournals.knu.ua/index.php/visnuk/article/view/898/841. [in Ukrainian].

6. Zolotar, O.O. Pravovi osnovy informatsiinoi bezpeky liudyny: dys. …dokt. yuryd. nauk: 12.00.07 [Legal foundations of human information security: Doctoral thesis: 12.00.07]. Kyiv, 2018. [in Ukrainian].

7. Proposal for a Decision of the European Parliament and of the Council Establishing the 2030 Policy Programme “Path to the Digital Decade” (Text with EEA relevance). Retrieved from. https://data.consilium.europa.eu/doc/document/ST-11900-2021-INIT/en/pdf [in English].

8. Pro Natsionalnu prohramu informatyzatsii: Zakon Ukrainy vid 4.02.1998 № 74/98-VR [On the National Informatization Program: Law of Ukraine No. 2073-IX of February 4, 1998]. Vidomosti Verkhovnoi Rady Ukrainy, 27-28, 181.9. [in Ukrainian].

9. Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(2), 137-154. Retrieved from. https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1973526. [in English].

10. Education Technology. 2020b. “Ransomware Attacks on Education Sector More Than Doubled Since 2019.” Education Technology. Retrieved from. https://edtechnology.co.uk/cybersecurity/ransomware-attackseducation-sector-doubled-since-2019/, as cited in: . Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(2), 137-154. https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1973526 [in English].

11. Reuters. 2020. “University of Maastricht Says It Paid Hackers 200,000-Euro Ransom.” Retrieved from. https://uk. reuters.com/article/us-cybercrime-netherlands-university-idUKKBN1ZZ2HH. as cited in: Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. [in English].

12. University of Utah Communications. 2020. “University of Utah Update on Data Security Incident.” Retrieved from. https://attheu.utah.edu/facultystaff/university-of-utah-update-on-data-security-incident/. as cited in: Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. [in English].