

13. Zakon Ukrainy Pro zapobihannia koruptsii : pryiniaty 14 zhovtnia 2014 r. № 1700-VII. [Law of Ukraine On Prevention of Corruption from October 14, 2014 No. 1700-VII.] *Vidomosti Verkhovnoi Rady Ukrainy - Information from the Verkhovna Rada of Ukraine*. 2014. № 49. Art. 2056 [in Ukrainian].
14. Kodeks Ukrainy pro administratyvni pravoporushennia : pryiniaty 07.12.1984 r. № 8073-Kh. [Code of Ukraine on Administrative Offenses from 07.12.1984 No. 8073-X] Kyiv: Parlamentske vyd-vo [in Ukrainian].
15. Shemshuchenko, Yu.S. & (Ed.). (2018). *Velyka ukrainska yurydychna entsyklopediia : u 20 t. T.14 : Ekolohichne pravo* [The Great Ukrainian Law Encyclopedia: 20 tons. Kharkiv: Law, 2016. T.14: Environmental Law] Nats. akad. prav. nauk Ukrainy ; In-t derzhavy i prava im. V.M. Koretskoho NAN Ukrainy ; Nats. yuryd. un-t im. Yaroslava Mudroho [in Ukrainian].
16. Kryminalnyi kodeks Ukrainy [The Criminal Code of Ukraine] (2001, April 5). *Vidomosti Verkhovnoi Rady Ukrainy - Information from the Verkhovna Rada of Ukraine*. 2001. № 25-26. Art. 131 [in Ukrainian].

Інформація про автора

ОВЕРКОВСЬКА Тетяна Костянтинівна – кандидат юридичних наук, доцент, доцент кафедри права, Вінницький національний аграрний університет (21008, м. Вінниця, вул. Сонячна, 3, e-mail:otk@vsau.vin.ua)

OVERKOVSKA Tetiana - PhD, Associate Professor, Associate Professor of Law Faculty of Management and Law, Vinnitsa National Agrarian University (21008, Vinnytsia, 3, Sonyachna str, e-mail:otk@vsau.vin.ua)

ОВЕРКОВСКАЯ Татьяна Константиновна - кандидат юридических наук, доцент, доцент кафедры права, Винницкий национальный аграрный университет (21008, г. Винница, ул. Солнечная, 3, e-mail:otk@vsau.vin.ua)



УДК: 342.9

DOI: 10.37128/2411-4413-2019-9-19

**КОНСТИТУЦІЙНО- ПРАВОВІ ЗАСАДИ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ ©**

ПРАВДЮК А.Л.,
кандидат юридичних наук,
доцент кафедри права
Вінницький національний
аграрний університет
(м. Вінниця)

У статті розглядаються пріоритети удосконалення інформаційної безпеки України на основі аналізу внутрішніх та зовнішніх чинників, європейських тенденцій та сучасної ситуації в країні. Обґрунтовується, що інформаційна безпека посідає одне з ключових місць у системі забезпечення життєво важливих інтересів усіх без винятку суспільств. Це передусім обумовлено нагальною потребою створення розвинутого інформаційного середовища суспільства. Але саме через інформаційне середовище найчастіше здійснюються загрози національній безпеці в різних сферах діяльності особистості, суспільства й держави. Досліджено проблему інформаційної безпеки України та захисту національного інформаційного простору від негативних пропагандистсько-маніпулятивних інформаційно-психологічних впливів. Проаналізовано теоретичні підходи до визначення сутності поняття інформаційна безпека; всебічно досліджено види реальних і потенційних інформаційних загроз, принципи забезпечення інформаційної безпеки України, що є вихідними положеннями формування і функціонування системи інформаційної безпеки як системоутворюючого фактору всіх складових національної безпеки, норм і правил поведінки громадян, державних і суспільних інститутів у цій сфері. Досліджено такі актуальні сучасні явища як кібербезпека та кібертероризм.

Ключові слова: інформаційна безпека, кібербезпека, пріоритети інформаційної безпеки, національні інтереси, політична пропаганда, кібертероризм.

Літ.: 25.

CONSTITUTIONAL AND LEGAL BASIS OF INFORMATION SECURITY OF UKRAINE

PRAVDYUK Andrew,
Candidate of Law Science, Associate Professor of Law
Vinnitsa National Agrarian University
(Vinnitsia)

The article considers the priorities of improving information security of Ukraine on the basis of analysis of internal and external factors, European tendencies and the current situation in the country. It is grounded that information security is one of the key places in the system of maintenance of vital interests of all without exception of societies. This is primarily due to the urgent need to create a well-developed information environment for society. But precisely because of the information environment, threats to national security are most often carried out in various spheres of activity of the individual, society and the state. The problem of information security of Ukraine and protection of the national information space from negative propaganda-manipulative information-psychological influences is investigated. The theoretical approaches to the definition of the essence of the concept of information security are analyzed; The types of real and potential information threats, principles of information security of Ukraine, which are the starting points of the formation and functioning of the information security system as a system-forming factor of all components of national security, norms and rules of conduct of citizens, state and public institutes in this sphere, are thoroughly investigated. The following topical contemporary phenomena such as cybersecurity and cyberterrorism have been researched.

Key words: information security, cyber security, priorities of information security, national interests. political propaganda, cyberterrorism.

Ref.: 25.

КОНСТИТУЦИОННО ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УКРАИНЫ

ПРАВДЮК Андрей Леонидович,
кандидат юридических наук, доцент кафедры права
Винницкий национальный аграрный университет
(г. Винница)

В статье рассматриваются приоритеты совершенствования информационной безопасности Украины на основе анализа внутренних и внешних факторов, европейских тенденций и современной ситуации в стране. Обосновывается, что информационная безопасность занимает одно из ключевых мест в системе обеспечения жизненно важных интересов всех без исключения обществ. Это прежде всего обусловлено насущной необходимостью создания развитой информационной среды общества. Но именно из-за информационной среды чаще всего осуществляются угрозы национальной безопасности в различных сферах деятельности личности, общества и государства.

Исследована проблема информационной безопасности Украины и защиты национального информационного пространства от негативных пропагандистско-манипулятивных информационно - психологических воздействий.

Проанализированы теоретические подходы к определению сущности понятия информационная безопасность; всесторонне исследованы виды реальных и потенциальных информационных угроз, принципы обеспечения информационной безопасности Украины, являются исходными положениями формирования и функционирования системы информационной безопасности как системообразующего фактора всех составляющих национальной безопасности, норм и правил поведения граждан, государственных и общественных институтов в этой сфере. Исследовано такие актуальные современные явления как кибербезопасность и кибертерроризм.

Ключевые слова: информационная безопасность, кибербезопасность, приоритеты информационной безопасности, национальные интересы. политическая пропаганда, кибертерроризм.

Лит.: 25.

Постановка проблеми: Захищаючи свої інформаційні інтереси, кожна держава має дбати про інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України формується як складова частина її соціально-

економічної політики, виходячи з пріоритетності національних інтересів та загроз національній безпеці країни. У ст.17. Конституції України зазначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [1].

Конституційні засади забезпечення інформаційної безпеки визначені в Основному Законі України фрагментарно і не системно, що ускладнює процеси виявлення й упровадження національних інтересів та їх реалізації за допомогою середньо- і довгострокових інструментів(доктрин, програм, аналітичних документів тощо). Головним критерієм у забезпеченні інформаційної безпеки України є юридична визначеність у реалізації інформаційних прав і свобод, що зумовлює відповідну організацію публічної влади та накладає на неї обов'язки згідно зі статтею 3 Конституції України. Також ця система передбачає виявлення і чітке визначення можливих внутрішніх і зовнішніх загроз національним інформаційним інтересам України. Процес формування національної свідомості й відповідного їй політико-правового укладу, через який проходить Україна, зумовлює необхідність досягнення цілісного історичного шляху української нації для утвердження сильної національної держави та українського ідеалу демократії. Розвиток України як демократичної держави робить дуже актуальною проблему залучення громадян до процесу вироблення і прийняття державних рішень, контролю за діяльністю держави, розвитку усіх форм безпосередньої демократії. Право на доступ до публічної інформації в сучасному інформаційному суспільстві є одним з ключових конституційних прав [2,с.85]. Доступ кожного до інформації про діяльність органів і посадових осіб державної влади, місцевого самоврядування сприяє реалізації контролю громадянського суспільства за їх діяльністю, є засобом протидії корупції, забезпечує можливість особі задовольняти її суспільні та індивідуальні інтереси. Сьогоднішні умови політичного і соціально-економічного розвитку країни викликають загострення розбіжностей між потребами суспільства в розширенні вільного обміну інформацією і необхідністю збереження окремих обмежень на її поширення. Відсутність дієвих механізмів регулювання інформаційних відносин у суспільстві та державі призводить до багатьох негативних наслідків. З огляду на глибоку інформатизацію сучасного життя і загальне визнання пріоритетів інформаційного суспільства, інформаційні права людини мають значення не тільки як певна сукупність правомочностей, а й як пріоритетний життєво важливий інтерес, реалізація якого визначально впливає на життєдіяльність сучасної людини. Разом із тим, ефективне планування, організація та управління процесом забезпечення інформаційної безпеки сьогодні не можуть бути забезпечені, якщо не визначені відповідні наукові засади. В цьому зв'язку одним з актуальних аспектів цієї проблеми є необхідність визначення базових наукових принципів, за якими доцільно розбудовувати інформаційну безпеку України. Усі ці чинники зумовлюють необхідність глибокого дослідження правової природи цього виду прав та розроблення уніфікованого підходу до їх розуміння. Питання забезпечення інформаційної безпеки є вкрай важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо. У Доктрині інформаційної безпеки України визначено Національними інтересами України в інформаційній сфері є: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації; забезпечення вільного обігу інформації, крім випадків, передбачених законом; розвиток та захист національної інформаційної інфраструктури; захищеність від руйнівних інформаційно-психологічних впливів; Крім того, доктрина визначила актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері є: здійснення спеціальних інформаційних операцій, спрямованих на підриив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні; проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в

інших державах; інформаційне домінування держави-агресора на тимчасово окупованих територіях; недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України; неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного нормативу, недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [3].

Щодо державної політики, то у сфері інформаційної безпеки – спрямована на накопичення та захист національних інформаційних ресурсів, розробку та впровадження сучасних безпечних інформаційних технологій, побудову захищеної національної інформаційної інфраструктури, формування і розвиток інформаційних стосунків тощо. Вона повинна реалізовуватись шляхом створення і забезпечення ефективного функціонування в Україні цілісної системи інформаційної безпеки, а також вдосконалення існуючої і розробки нової нормативно-правової бази, яка регулює відносини в сфері інформаційної безпеки, встановлює вимоги і правила провадження діяльності у цій сфері [4, с.78].

Аналіз останніх досліджень і публікацій. Вивченням сутності та стану забезпечення інформаційних прав та інформації займалися і провідні вітчизняні науковці, серед яких можна назвати Є.П. Тептюк [2], О.М. Солодка, М.В. Саврук [4], О.Г. Кушніренко, О.В. Нестеренко, Н.Б. Мезенцева[5], О.В. Олійник [6], Г.М. Калетнік [7], В.М. Бришко [8], В.М. Вакулич [9], Л.В. Вакарюк [11], Ю. Ірха [12], В.О. Антонов [14], Ю.В. Литвиненко, Д.Павлов [15], І.М. Діордіца [16], Р.А. Калюжний [17], О.М. Яхно [18], В.В. Топчій [19], Д.С. Бірюков [24] В.П. Шеломенцев [25], В.Я. Настюк, В.М. Богуш та багатьох інших вчених.

Формулювання цілей статті. Метою статті є дослідження теоретичних і практичних аспектів формування і функціонування системи інформаційної безпеки як системоутворюючого фактору всіх складових національної безпеки, норм і правил поведінки громадян, державних і суспільних інститутів у цій сфері, розробка рекомендацій з удосконалення механізм забезпечення інформаційної безпеки.

Виклад основного матеріалу дослідження. У світлі подій, які розгорнулися в Україні та у світі, в цілому, вирішення питань законодавчого забезпечення інформаційної безпеки України набули невідкладного характеру. Сьогодні ми живемо в інформаційному суспільстві, в якому інформаційні права відіграють надзвичайно важливу роль. Проте значної уваги потребує захист інформації від будь-яких посягань. Це означає що забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. Тому за сучасних умов сповнених технологічними новаціями особливо актуально постає питання забезпечення інформаційної безпеки у процесі діяльності апарату управління держави. Пріоритетним завданням є створення законодавчої і нормативно-правової бази щодо розподілу і використання персональної інформації з метою створення умов для інформаційних стосунків між органами державної влади і суспільства, формування передумов досягнення соціального компромісу, створення умов становлення соціального партнерства як основи демократичного розвитку суспільства, розробки регламенту інформаційного обміну для органів державної влади і управління, реєстру інформаційних ресурсів, закріплення відповідальності посадових осіб, громадян за додержання вимог інформаційної безпеки [5, с.214]. Цілком зрозуміло, що ефективно планування, організація та управління процесом забезпечення інформаційної безпеки сьогодні не можуть бути забезпечені, якщо не здійснений аналіз уже існуючих у правовій науці принципів організації та управління забезпеченням інформаційної безпеки.

Аналіз принципів забезпечення інформаційної безпеки дає змогу констатувати, що вітчизняне право виробило необхідні теоретичні засади для вирішення проблеми обґрунтування узагальненої системи принципів організації та управління забезпеченням інформаційної безпеки. Головна мета забезпечення інформаційної безпеки має визначатися на основі широкого розуміння цього поняття як важливої складової національної безпеки та системоутворюючого фактору всіх сфер життєдіяльності особи, суспільства, держави, політичної, економічної, соціокультурної, науково-технологічної, оборонної, екологічної, власне інформаційної тощо складових національної безпеки. Таким чином, пріоритет державної політики інформаційної безпеки має полягати у захисті: конституційних прав і свобод людини і громадянина, забезпеченні єдності їх прав і обов'язків; духовних, морально-етичних, культурних, історичних, інтелектуальних та

матеріальних цінностей суспільства, його інформаційного і природного середовища; конституційного ладу, суверенітету, територіальної цілісності, інформаційної безпеки в політичній, економічній, соціокультурній, науково-технологічній, оборонній і державній безпеці, екологічній, власне інформаційній тощо складових національної безпеки [6, с.75].

Очевидно, що роль правового регулювання держави у забезпеченні інформаційної безпеки набуває особливо важливого значення. Г.М. Калетнік наголошує, що правове регулювання - метод державного управління, суттю якого є юридичний вплив на соціально-правову сферу та її окремі елементи у процесі впорядкування суспільних відносин, основним учасником якого є державна влада [7].

Державна інформаційна політика це політика, яка засобами державної влади створює та забезпечує функціонування правової системи регулювання інформаційних відносин, захисту прав людини й основних свобод, та забезпечення збалансування інтересів людини, суспільства та держави у всіх сферах інформаційної діяльності. Іншими словами, під державною інформаційною політикою розуміється регулююча діяльність державних органів, спрямована на розвиток інформаційної сфери суспільства, що охоплює не тільки інформаційні системи, телекомунікації і засобів масової інформації, але й всю сукупність виробництва і відносин, пов'язаних зі створенням, одержанням, зберіганням, обробкою, використанням і поширенням інформації у всіх її видах – статистичної, адміністративної, масової, інформації про діяльність органів державної влади та органів місцевого самоврядування, правової інформації, інформації про особу, інформації довідково-енциклопедичного характеру та соціологічної інформації. Таке широке трактування інформаційної політики, представляється сьогодні обґрунтованим, тому що новітні інформаційні технології інтенсивно розвивають бар'єри між різними секторами інформаційного середовища [8,с.168].

Основні правила щодо ведення інформаційної діяльності, тобто одержання, використання, поширення та зберігання інформації і захисту прав суб'єктів інформаційних відносин містяться у статтях 15, 32 і 34 Конституції України, а також у Цивільному кодексі України, законах України: «Про інформацію», «Про доступ до публічної інформації», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про інформаційні агентства», «Про державну підтримку засобів масової інформації та соціальний захист журналістів», «Про науково-технічну інформацію», «Про захист від недобросовісної конкуренції», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну статистику», «Про бібліотеки і бібліотечну справу», «Про Національний архівний фонд та архівні установи», «Про державну таємницю», «Про Національну систему конфіденційного зв'язку», «Про банки і банківську діяльність», «Про Державну службу спеціального зв'язку та захисту інформації України» [9, с.100].

Декларація прав людини і громадянина у своїх статтях наголошує що кожна людина має право на свободу своїх переконань та на вільне вираження їх. Це право включає свободу безперешкодно дотримуватися своїх переконань, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів (стаття 19)[10]. Конституція України 1996 р. відповідно до вже наявних тенденцій основоположних міжнародно-правових актів у галузі прав людини право кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір – об'єднала в нормах різних частин статті 34 з іншим правом кожного на свободу думки і слова, на вільне вираження своїх поглядів і переконань, визначивши їх самостійність. Основний Закон включає низку правоможливостей: право збирати, право зберігати, право використовувати та право поширювати інформацію усно, письмово або в інший спосіб – на свій вибір, які, у свою чергу, структуруються в інші численні інформаційні права [11, с.157]. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадянського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення для захисту репутації та інших прав людей, для запобігання розголошенню інформації одержаної конфіденційно або для підтримання авторитету і неупередженості правосуддя. Обмеження конституційних прав і свобод людини і громадянина з названих підстав спрямоване на досягнення розумного балансу між інтересами окремих осіб, суспільства та держави. Однак на практиці непоодинокими є випадки, коли законодавець і правозастосовні органи надто широко інтерпретують допустимі обмеження зазначених прав і свобод, особливо в інтересах національної безпеки, внаслідок чого спотворюється або взагалі нівелюється їхня сутність. Крім того, часто громадяни гіперболізують

обсяг належних їм конституційних прав і свобод та межі їх реалізації, ставлять свої інтереси вище за національні, а тому вважають неправомірним встановлення будь-яких обмежень щодо них, навіть із метою забезпечення національної безпеки [12, с.79]. У статті 32 Конституції України закріплено право кожного громадянина знайомитись в органах державної влади, органах місцевого самоврядування, установах та організаціях з відомостями про себе, які не є державною чи захищеною законом інформацією. Захист інформації, згідно з законом України «Про інформацію» – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [13]. Інформаційна сфера суспільства була та залишається особливо чутливою до зовнішніх впливів в умовах розвитку та становлення демократичних інститутів. На цей час основною загрозою є розповсюдження у світовому інформаційному просторі неправдивої чи викривленої інформації, що, своєю чергою завдає певної шкоди національній безпеці, а її спростування чи заперечення потребує дійсно великих затрат як часу, зусиль, так і фінансів. Сучасний етап розвитку інформаційних технологій характеризується можливістю масового інформаційного впливу на індивідуальну та суспільну свідомість, що може призвести до масштабних інформаційних війн. Спостерігається небезпечна тенденція перегляду національних кордонів поза нормами міжнародного права, де застосування сили і погрози силою повернулися до практики міжнародних відносин, у тому числі в Європі [14, с.6]. Можна з впевненістю стверджувати що військові дії на сході України стали продовженням інформаційної пропаганди. Сьогодні будь-яке повідомлення ідентифікують як пропаганду, якщо воно є неправдивим або спотворює сприйняття реальності. До слів та виразів, що часто використовують як синоніми пропаганди, належать брехня, перекручування, омана, маніпуляція, контроль над свідомістю, психологічна війна, промиванням мізків, балаканина. Іншими словами, поняття «пропаганда» слугує певним маркером, щоб кваліфікувати повідомлення як інформаційно-дефективні [15, с.329]. Реалії сьогодення показують відсутність механізмів ефективного та швидкого блокування (обмеження доступу) ресурсів з протиправним контентом, зокрема розміщених на технічних майданчиках закордоном, як і власне визначення шкідливого контенту. Іноземні спецслужби безперешкодно поширюють інформаційну продукцію антиукраїнського змісту, що містить заклики до порушення конституційного ладу, територіальної цілісності, пропаганду війни, фашизму, національної та релігійної ворожнечі. Певні спроби держави проявились в обмеженні доступу до новин російських телеканалів, але інший медіа продукт (серіали, фільми, телешоу, концерти) ніколи не зникали з екранів телевізорів. Недолуга спроба перекладу на українською мовою вище вказаної продукції додала більше запитань, аніж відповідей. Видозмінена інформація стала потоком маніпулювання як індивідуальною, так і масовою свідомістю. Проте ми цілком підтримуємо думку Діордіца І.В., що не загроза з боку Росії визначає державну політику, а необхідність створення сприятливих умов для реалізації національних інтересів. Лише за умови того, що на цьому етапі історичного розвитку Росія становить загрозу і перешкоджає реалізації даних інтересів, не можна визначати і зводити усю державну політику до вирішення одного тимчасового, нехай і важливого, але оперативного завдання. Ефективною держава є тоді, коли в ній державна політика виконує створювальну та проактивну функції, а не є реактивною і заборонувальною [16, с. 68].

Сучасне суспільство можна відзначити злетом людського розуму, всеохоплюючою ідеєю прогресу, стрімким зростанням ролі інформації [17, с.14]. Як зазначає у своїй роботі О. М. Яхно «Україна в сучасному геополітичному просторі (політико-медійний аспект)», рівень розвитку інформаційної складової тісно пов'язаний із безпекою держави: період становлення механізмів інформаційного суспільства є дуже небезпечним, оскільки країна може увійти у світові інфраструктури, не створивши при цьому механізмів захисту [18, с.10]. Розвиток суспільства, впровадження інноваційних технологій породив таке явище, як комп'ютерний тероризм, що є реальною загрозою функціонуванню інформаційно-телекомунікаційних систем держави за допомогою глобальної мережі Інтернет. Для всесвітньої мережі немає державних кордонів, атаку можна здійснити з будь-якої частини світу за допомогою гаджетів, які доступні кожному. Під кібертероризмом розуміють навмисну мотивовану атаку на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу; вона пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування воєнного конфлікту [19, с.66]. У Законі України «Про основні засади забезпечення кібернетичної безпеки України»

кібертероризм визначено як терористичну діяльність, що здійснюється у кіберпросторі або з його використанням [20]. Іншими словами це війна де інформація є надпотужною зброєю, про що свідчить те, що сьогодні на другому місці за негативним впливом для світової спільноти після природних катаклізмів перебувають кібератаки (рік тому технологічні ризики разом із кіберзлочинністю займали третє місце). Це зазначено в щорічній доповіді експертів Всесвітнього економічного форуму в Давосі про глобальні ризики у світі під назвою “Global Risks Report 2018”, яка опублікована в січні 2018 року [21]. Також зростають збитки від кіберзлочинів, які відповідно до звіту компанії McAfee і Центру стратегічних і міжнародних досліджень (CSIS) склали у 2017 році близько 600 млрд доларів [22]. Новою загрозою для кібербезпеки є створення кібервійськ, які здатні впливати на інфраструктуру «противників», що створюються багатьох країнах. Генеральний секретар ООН Антоніу Гутерріша під час виступу в Лісабонському університеті 19 лютого 2018 року застеріг: «Наступна війна почнеться з масової кібератаки з метою знищення військового потенціалу і паралічу базової інфраструктури, такої, як електричні мережі» [23]. Гібридна війна породжує ще більші кіберзагрози під час якої об’єкти критичної інфраструктури стають полігонами, для випробування нових технологій кібератак. Критична інфраструктура України – системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки [24,с.14-15]. У цілому ж до об’єктів національної критичної інфраструктури, що потребують захисту від кібератак, необхідно віднести об’єкти, реалізація кібернетичних загроз щодо яких може призвести до настання таких наслідків, як надзвичайна ситуація; блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об’єктів підвищеної небезпеки; органів військового управління, Збройних Сил України в цілому, або втручання в автоматизовані системи керування зброєю; порушення безпечного функціонування банківської або фінансової системи держави; розголошення державної таємниці; масові заворушення [25]. Так для захисту вітчизняного кіберпростору були розроблені та прийняті ряд важливих нормативно-правових актів, серед яких слід зазначити Стратегію кібербезпеки України, Рішення РНБО України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», Закон України «Про основні засади кібербезпеки України» та інші документи у сфері кібербезпеки. Інформаційні інтервенції становлять суттєву загрозу кібернетичній безпеці, оскільки остання є частиною національної безпеки, та може завдавати шкоди як державі в цілому, так і окремим фізичним особам. Створення дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення правових засад державної політики у цій сфері та своєчасного реагування на динамічні зміни, що відбуваються у світі у сфері забезпечення кібернетичної безпеки із можливістю застосування міжнародного досвіду [16, с. 191].

Висновки. Проведений аналіз наукових та нормативних джерел дослідження надає можливість зазначити наступне:

1. Україна на нормативно-правовому рівні закріпила готовність реалізовувати політику інформаційної безпеки. Водночас практичні форми та методи реалізації відповідної політики залишаються не повною мірою впровадженими. Проблемою залишається формування ефективних механізмів захисту інформації від несанкціонованих втручань, однак держава вживає рішучих заходів щодо протидії сьогоденним загрозам і формування національної системи кібернетичної безпеки.

2. Проблема кібербезпеки не є притаманною окремим суспільствам, а становить специфічну, водночас глобальну проблему безпечного розвитку усього суспільства. Досвід минулих років показав що не лише Україна, а й Європа та світ загалом виявилися неготовими до інформаційної війни окремих держав, які заперечують будь-які встановлені міжнародні правила поведінки держави. Вважаємо, що лише скоординовані дії дадуть змогу ефективно реалізовувати кібербезпекову політику.

3. Національні інтереси України у сфері інформаційної безпеки повинні полягати у дотриманні конституційних прав та свобод громадян щодо отримання інформації та її використання, у розвитку сучасних телекомунікаційних технологій, у захисті державних інформаційних ресурсів від несанкціонованого доступу.

4. Безпека інформаційного простору є передумовою та вагомим елементом вирішення нагальних проблем що загрожують соціальній безпеці. Сучасні інформаційні протистояння,

засвідчила що інформаційний простір України потребує додаткового захисту від зовнішніх негативних інформаційно-психологічних впливів.

5. Вважаємо, що внутрішні загрози є не менш небезпечними, оскільки в державі відсутні політико-правові підходи до захисту інформаційного суверенітету. Монополізація інформації призводить до того що певне коло осіб керують свідомістю громадян для прийняття необхідного корисливого рішення для них. Такий розвиток подій є особливо загрозливим для України в контексті формування вищих органів державної влади.

6. Однією з головних причин відсутності правового механізму, здатного ефективно регулювати суспільні відносини в інформаційній сфері в цілому та в секторі безпеки зокрема є брак легітимної державної інформаційної політики, як діяльності стратегічного рівня, щодо внутрішніх та зовнішніх правостосунків і взаємодій, в який має бути комплексно визначені основні соціальні, організаційні, правові, методологічні, технологічні та інші засади позиції держави в процесі розвитку національної інформаційної сфери, шляхи формування та розбудови інформаційного суспільства в Україні, а також інтеграції в світовий інформаційний простір.

7. Інформаційна система повинна мати певний запас міцності на випадок непередбачених і надзвичайних обставин з тим, щоб державні органи могли оперативнo і своєчасно відреагувати на виникнення будь-яких загроз і по можливості запобігти, нейтралізувати або звести до мінімуму потенційні соціально-економічні втрати. Саме професійно формалізована державна інформаційна політика має замінити незчисленні концепції, програми, доктрини та стратегії, об'єднавши їх в єдиний законодавчий акт.

Список використаних джерел

1. Конституція України : станом на 1 верес. 2016 р. / Верховна Рада України. Харків: Право, 2016. 82 С.

2. Тептюк Є. П. Конституційно-правове визначення поняття права на доступ до публічної інформації Науковий вісник Міжнародного гуманітарного університету. Сер. Юриспруденція. 2014. 7. С. 85–87.

3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» Указ Президента України від 25.02.2017 р. № 47/2017. <http://www.rnbo.gov.ua/documents/439.html>

4. Саврук М. В. Актуальність проблеми забезпечення інформаційної безпеки України та шляхи її розв'язання системи обробки інформації. 2010. № 3(84).С. 77-79.

5. Мезенцева Н.Б. Правові засади протидії загрозам інформаційній безпеці та розвитку інформаційного законодавства. Наукові записки Львівського університету бізнесу та права. 2013.10. С. 214-216.

6. Олійник О.В. Принципи забезпечення інформаційної безпеки України. Юридичний вісник повітряне і космічне право . 2016. Том 4, № 41. С. 72 – 78.

7. Калетнік Г. М., Мазур А. Г., Кубай О. Г. Державне регулювання економіки: Навчальний посібник. - К.: «Хай-Тек Прес», 2011. - 428 с.- [Електронний ресурс].-Режим доступу: https://pidruchniki.com/1813011338682/ekonomika/derzhavne_regulyuvannya_ekonomiki

8. Брижко В.М, Цимбалюк В.С. Орехов А.А, Гальченко О.Н. Е-будущее и информационное право/Под ред. Р.А. Калюжного, М.Я. Швеца.-К.: «Интеграл», 2002.-264 с.

9. Вакулич В. Державна інформаційна політика як механізм реалізації інформаційної функції сучасної держави. Публічне управління: теорія та практика. 2014. №1 (17). С. 97 – 107.

10. Загальна декларація прав людини. Прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/995_0153.

11. Вакарюк Л. В. Основні підходи до розуміння поняття «інформаційні права людини». Підприємництво, господарство і право. 2018. № 2. С. 155-159

12. Ірха Ю. Обмеження конституційних прав і свобод людини і громадянина в інтересах національної безпеки України в сучасних умовах. Вісник Конституційного Суду України . 2015. № 5. С. 78-88.

13. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-XII. Дата оновлення: 1.01.2017. URL: <http://zakon5.rada.gov.ua/laws/show/2657-12>.

14. Антонов В. О. Конституційно-правові засади національної безпеки України: монографія . Київ: ТАЛКОМ, 2017. 576 с.

15. Павлов Д. Політична пропаганда: до визначення поняття. Гілея: науковий вісник. 2013. Вип. 79. С. 328-331.
16. Діордіца І.М. Адміністративно-правове регулювання кібербезпеки в Україні.: дис. д-ра юрид. наук : 12.00.07; Запоріжжя, 2018. 521 с.
17. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії та практики. Монографія/ За ред. Р.А. Калюжного та В.О. Шамрая – Київ, 2002. 296 с
18. Яхно О. М. Україна в сучасному геополітичному просторі (політико- медійний аспект) : автореф. дис. ... канд. політ. наук : 23.00.03. Київ, 2006. 14 с.
19. Топчий В. В. Кібертероризм в Україні: поняття та запобігання кримінально-правовим та кримінологічними засобами. Науковий вісник Херсонського університету. Сер. Юридичні науки. 2015. Вип. 6. Том 3 С. 65-68.
20. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: <http://zakon2.rada.gov.ua/laws/show/2163-19>
21. Global Risks Report 2018” URL: <http://www.weforum.org>.
22. Збитки світової економіки від хакерів досягли \$ 600 млрд URL: <https://ua.korrespondent.net/world/3943548-zbitky-svitovoi-ekonomiky-vid-khakerivdosiahly-600-mlrd>
23. Генсекретар ООН закликав до глобальної боротьби проти кібервоєн URL: <https://www.radiosvoboda.org/a/news/29049044.html>.
24. Бірюков Д.С. Кондратов С.І. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. Нарад. Київ: НІСД, 2015. 176 с: URL: http://www.niss.gov.ua/public/File/2016_book/Syuhodolya_ost.pdf
25. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1 (27). С. 312–320.

References

1. Konstytucija (Osnovnyj zakon)Ukraiiny [Constitution (The Main Law) of Ukraine]. (n.d.)zakon1.rada.gov.ua. URL:<http://zakon1.rada.gov.ua/laws/show/254%D0%B2%D-1%80> (Last accessed : 18.04.2018) [in Ukrainian].
2. Teptiuk Y.P. (2014)Konstytutsiino-pravove vyznachennia poniattia prava na dostup dopublichnoi informatsii [Constitutional and legal definition of the right to access public information] *Scientific Herald of the International Humanitarian University. Series "Jurisprudence"*, 7, 85-87 [in Ukrainian].
3. Ukaz Prezydenta Ukrainy № 47 vid 25.02.2017 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29.12. 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy» [Decree of the President of Ukraine of 25.02.2017 № 47About the doctrine of information security of Ukraine]. 2017, on.rada.gov.ua URL: <http://www.rnbo.gov.ua/documents/439.html> (Last accessed: 18.04.2018) [inUkrainian].
4. Savruk M. V.(2010) Aktualnist problemy zabezpechennia informatsiinoi bezpeky Ukrainy ta shliakhy yii rozviazannia[The urgency of the problem of ensuring the information security of Ukraine and the ways of its solution] *Information processing systems*, 3 (84), 77-79. [inUkrainian].
5. Mezentseva N.B.(2013) Pravovi zasady protydii zahrozam informatsiinii bezpetsi ta rozvytku informatsiinoho zakonodavstva[Legal principles of counteraction to threats to information security and development of information legislation] *Scientific notes of Lviv University of Business and Law*, 10, 214-216. Retrieved from : http://nbuv.gov.ua/UJRN/Nzlubp_2013_10_51[inUkrainian].
6. Oliinyk O.V.(2016)Pryntsypy zabezpechennia informatsiinoi bezpeky Ukrainy[Principles of ensuring information security of Ukraine] *Legal newsletter air and space law*, 4, (41). 72 - 78. [inUkrainian].
7. Kaletnik H. M., Mazur A. H., Kubai O. H.(2011) *Derzhavne rehuliuвання ekonomiky[State regulation of Economy]* Kiev High-Tech Press. [inUkrainian].
8. V.M. Bryzhko, V.S. Tymbaliuk, A.A. Orekhov, O.N. Halchenko.(2002) E-budushee i informatsionnoe pravo[E-future and information law].Kiev [inUkrainian].
9. Vakulych V.(2014) Derzhavna informatsiina polityka yak mekhanizm realizatsii informatsiinoi funktsii suchasnoi derzhavy[State information policy as a mechanism for the implementation of the information function of the modern state] *Public Administration: Theory and Practice*, 1 (17),97 - 107. [inUkrainian].
10. Zahalna deklaratsiia prav liudyny. Adopted and proclaimed by resolution 217 A (III) of the General Assembly of the United Nations of December 10, 1948 Retrieved from: http://zakon1.rada.gov.ua/laws/show/995_0153 [inUkrainian].

11. Vakariuk L. V. (2018) Osnovni pidkhody do rozuminnia poniattia «informatsiini prava liudyny» [Basic Approaches to Understanding the Notion of "Information Rights of Man"] *Entrepreneurship, economy and law*, 2, 155-159 [in Ukrainian].
12. Irkha Yu. (2015) Obmezhenia konstytutsiinykh prav i svobod liudyny i hromadianyna v interesakh natsionalnoi bezpeky Ukrainy v suchasnykh umovakh [Limitation of the constitutional rights and freedoms of man and citizen in the interests of national security of Ukraine in modern conditions] *Bulletin of the Constitutional Court of Ukraine*, 5, 78-88. [in Ukrainian].
13. Pro informatsiiu [About information]: Law of Ukraine dated 02.10.1992 №2657-XII. – Access mode: <http://zakon3.rada.gov.ua/laws/show/2657-12>.
14. Antonov V. O. & Yu. S. Shemshuchenko. (2017) Konstytutsiino-pravovi zasady natsionalnoi bezpeky Ukrainy. [Constitutional and Legal Principles of National Security of Ukraine] Kyiv: TALKOM [in Ukrainian].
15. D. Pavlov (2013) Politychna propahanda: do vyznachennia poniattia [Political propaganda: to define the concept] *Gilea: Scientific Herald*, 79, 328-331 [in Ukrainian].
16. Diorditsa I. M. (2018) Administratyvno-pravove rehuliuвання kiberbezpeky v Ukraini. [Administrative and legal regulation of cybersecurity in Ukraine] Doctor's thesis. Zaporizhzhia [in Ukrainian].
17. R. A. Kaliuzhnyi. & V. O. Shamrai (2002) Informatsiine zabezpechennia upravlinskoï diialnosti v umovakh informatyzatsii: orhanizatsiino-pravovi pytannia teorii ta praktyky. [Information provision of management activity in the conditions of informatization: organizational and legal issues of theory and practice.] Kyiv [in Ukrainian].
18. Iakhno O. M. (2006) Ukraina v suchasnomu heopolitychnomu prostori (polityko- mediinyi aspekt) [Ukraine in the modern geopolitical space (political and media aspect)] : Extended abstract of candidate's thesis. Kyiv: National University. Taras Shevchenko. Institute of Journalism [in Ukrainian].
19. Topchii V. V. (2015) Kiberteroryzm v Ukraini: poniattia ta zapobihannia kryminalno-pravovymy ta kryminolohichnymy zasobamy. [Cyber Terrorism in Ukraine: the notion and prevention of criminal-legal and criminological means.] *Scientific Herald of Kherson University. Series "Legal Sciences"*. 6(3), 65-68.
20. Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [About the basic principles of providing cyber security of Ukraine] : Law of Ukraine dated 05.10.2017 № 2163-VIII. – Access mode: <http://zakon2.rada.gov.ua/laws/show/2163-19>
21. Global Risks Report (2018) [Global Risks Report] Published 17 January Retrieved from URL: www.weforum.org/reports/the-global-risks-report-2018 [in Ukrainian].
22. Zbytky svitovoi ev dosiahly \$ 600 mlrd [The losses of the global economy from hackers reached \$ 600 billion] Retrieved from URL: <https://ua.korrespondent.net/world/3943548-zbytky-svitovoi-ekonomiky-vid-khakerivdosiahly-600-mlrd> [in Ukrainian].
23. Hensekretar OON zaklykav do hlobalnoi borotby proty kibervoien [UN Secretary-General called for a global fight against cyberwar] Retrieved from RL: <https://www.radiosvoboda.org/osnovni-napriamy-yii-udoskonalennia>. [in Ukrainian].
24. D. S. Biriukov & S. I. Kondratov (2015) Zelena knyha z pytan zakhystu krytychnoi infrastruktury v Ukraini [Green book on critical infrastructure protection in Ukraine] O. M. Sukhodoli (Eds.) *Collection of international materials. expert. meetings* Kiev: NISS [in Ukrainian].
25. Shelomentsev V. P. (2012) Pravove zabezpechennia systemy kibernetychnoi bezpeky Ukrainy ta osnovni napriamy yii udoskonalennia. [Legal support of the system of cybernetic security of Ukraine and the main directions of its improvement.] *Fighting Organized Crime and Corruption (theory and practice)*, 1 (27), 312-320. [in Ukrainian].

Інформація про автора

ПРАВДЮК Андрій Леонідович – кандидат юридичних наук, доцент кафедри права, Вінницький національний аграрний університет (21008, м.Вінниця, вул.Сонячна, 3, e-mail: a.pravd4449@ gmail.com)

PRAVDYUK Andrew –Candidate of Law Science, Associate Professor of Law, Vinnitsa National Agrarian University (21008, 3, Sonyachnastr., Vinnitsia, e-mail: a.pravd4449@ gmail.com)

ПРАВДЮК Андрей Леонидович – кандидат юридических наук, доцент кафедры права, Винницкий национальный аграрный университет (21008, г.Винница, ул.Солнечная, 3, e-mail: a.pravd4449@ gmail.com)