
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ



**ІРПІНСЬКИЙ
ЮРИДИЧНИЙ
ЧАСОПИС**

Науковий журнал

Випуск 2 (11)

Ірпінь • ДПУ • 2023

ISSN 2617-4154
УДК 34:33(477)(08)

*Засновник: Університет державної фіскальної служби України
Заснований 2018 року*

*Продовжуване видання (виходить у міру накопичення матеріалу)
Мови видання: українська, англійська*

*Свідectво про Державну реєстрацію друкованого засобом масової інформації:
Серія КВ № 23215-13055ПР від 22.03.2018*

*Рекомендовано до друку та поширення через мережу «Інтернет» рішенням Вченої ради
Державного податкового університету (протокол № 9 від 30.03.2023)*

Редакційна колегія: д-р юрид. наук, професор *В. В. Топчій* (голов. ред.); канд. юрид. наук, доцент *О. М. Бодунова* (заст. голов. ред.); д-р юрид. наук, с.н.с. *Н. Б. Новицька* (заст. голов. ред.); канд. юрид. наук, доцент *Н. А. Лугова* (відп. секретар); д-р юрид. наук, доцент, *Ю. І. Аністратенко*; д-р юрид. наук, професор *В. Т. Білоус*; д-р юрид. наук, професор *С. В. Бобровник*; д-р юрид. наук, професор *О. Г. Боднарчук*; д-р юрид. наук, професор *Л. М. Касьяненко*; д-р юрид. наук, професор *О. Є. Костюченко*; д-р юрид. наук, професор *Н. А. Литвин*; д-р юрид. наук, професор *Т. О. Мацелик*; д-р юрид. наук, професор *Н. В. Никитченко*; д-р юрид. наук, професор *А. М. Новицький*; канд. юрид. наук, доцент *Л. В. Омельчук*; д-р юрид. наук, професор *О. П. Рябченко*; д-р юрид. наук, доцент *Ю. Ю. Рябченко*; д-р юрид. наук, професор *П. В. Цимбал*; д-р юрид. наук, професор *І. В. Чеховська*; д-р юрид. наук, професор *А. Є. Шевченко*; д-р юрид. наук, професор *Asar İsa oğlu Sadıgov* (Азербайджан), *Janusz Orłowski*, doctor nauk prawnych Uniwersytetu Warmińsko-Mazurski w Olsztynie (Poland).

Ірпінський юридичний часопис : науковий журнал / редкол. : *В. В. Топчій* (голов. ред.) та ін. – Ірпінь : Державний податковий університет, 2023. – Випуск 2 (11). – 170 с. – (Серія : право).

У виданні вміщені наукові статті, присвячені актуальним проблемам юридичної науки та практики.

Науковий журнал започатковано з метою опублікування результатів наукових досліджень проблем правової науки, теоретико-прикладних проблем правового забезпечення фіскальної політики держави, удосконалення законодавства та правозастосування.

Для науковців, викладачів, аспірантів, студентів та всіх, хто цікавиться проблемами теорії права та правозастосування.



Науковий журнал індексується в Google Scholar,



Національною бібліотекою України імені В. І. Вернадського.



Розміщений на відкритій інформаційній платформі OJS Державного податкового університету.



DOI (digital object identifier) – цифровий індикатор об'єкта привласнюється науковим статтям видання.

Редакція журналу веде систематичну роботу із включення наукового видання до міжнародних електронних бібліотек, каталогів та наукометричних баз даних з метою входження в світовий науковий інформаційний простір, підвищення рейтингу журналу та індексів цитування його авторів. Наразі редколегія провадить роботу щодо входження збірника у Scopus та Web of Science.

Адреса редакційної колегії:

Україна, 08201, Ірпінь, Київська обл., вул. Університетська, 31,
e-mail: irpin-yur-chas@ukr.net

Використання опублікованих у збірнику матеріалів дозволяється за умови обов'язкового посилання на джерело інформації.

У разі посилання на матеріали збірника наукових праць «Ірпінський юридичний часопис» потрібно використовувати транслітеровану назву «Irpinskyi yurydychnyi chasopys», або «Irpın legal chronicles».

© Державний податковий університет, 2023

STATE TAX UNIVERSITY



IRPIN LEGAL CHRONICLES

The Scientific Journal

Issue 2 (11)

Irpin • STU • 2023

ISSN 2617-4154
UDC 34:33(477)(08)

*Founder: University of the State Fiscal Service of Ukraine
The scientific journal «Irpın legal chronicles» was founded in 2018
Continued edition (released with the accumulation of material)
Languages of edition: Ukrainian, English
The certificate of state registration of the printed mass media:
KV № 23215-13055PR, 22.03.2018
Recommended for printing and Internet distribution by the decision of the
Academic Council of the State Tax University (protocol № 9, 30.03.2023)*

Editorial Board: Dr., Professor V. V. Topchiy (Editor-in-chief); Ph.D. in Law, Associate Professor O. M. Bodunova (deputy Ed.); Dr., senior researcher N. B. Novytska (deputy Ed.); Ph.D. in Law, Associate Professor, N. A. Lugina (co-ed.); Dr., Associate Professor, Yu. I. Anistratenko; Dr., Professor V. T. Bilous; Dr., Professor S. V. Bobrovnik; Dr., Professor O. G. Bodnarchuk; Dr., Professor L. M. Kas'yanenko; Dr., Professor O. E. Kostyuchenko; Dr., Professor N. A. Lytvyn; Dr., Professor T. O. Matselyk; Dr., Professor N. V. Nikitchenko; Dr., Professor A. M. Novytsky; Ph.D. in Law, Docent L. V. Omelchuk; Dr., Professor O. P. Ryabchenko; Dr., Professor Yu. Yu. Ryabchenko; Dr., Professor P. V. Tsybal; Dr., Professor I. V. Chekhovska; Dr., Professor A. Eu. Shevchenko; Dr., Professor Asar Isa ogly Sadygov (Azerbaijan), Janusz Orłowski, doctor nauk prawnych Uniwersytet Warmiński-Mazurski w Olsztynie (Poland).

Irpın legal chronicles : The Scientific Journal / Editorial Board : V. V. Topchiy (Editor-in-chief) and others. – Irpin : State Tax University, 2023. – Issue 2 (11). – 170 p. – (Series : Law).

The edition contains scientific articles devoted to the actual problems of legal science and practice.

The scientific journal was founded with the purpose of publishing the results of researches on problems of legal science, theoretical and applied problems of legal provision of the state fiscal policy, improvement of legislation and law enforcement.

The journal is intended for researchers, lecturers, postgraduates, students and anyone who is interested in law theory and law enforcement.



The Scientific Journal is indexed by Google Scholar,



V. I. Vernadsky National Library of Ukraine.



The scientific journal is located on the open information platform OJS of the State Tax University.



DOI digital object identifier is assigned to the scientific articles of the edition.

The editorial board carries out systematic work on integration of the scientific edition to the international electronic libraries, catalogs and scientometric databases with the purpose of entering the world scientific information space, increasing the rating of the journal and the citation indices of its authors. The editorial board is currently working on the inclusion of the scientific journal in Scopus and Web of Science.

Address of the editorial board:

31, Universitetskaya str., Irpin, Kyiv region, Ukraine, 08201
e-mail: irpin-yur-chas@ukr.net

The use of the materials published in the journal is allowed in case of obligatory referring to an information source.

Referring to the materials of the scientific journal «Irpın legal chronicles» one must use the transliterated title «Irpinskyi yurydychnyi chasopys» or «Irpın legal chronicles».

© State Tax University, 2023

ЗМІСТ

Теорія та історія держави і права; конституційне право

Стівен Хамфріс

Справи, які збудували Америку. «Флетчер проти Пека» та комерціалізація американського суспільного договору 9

Копотун І. М., Рудик М. М.

Аналіз загроз безпеці України в умовах військового стану 20

Сухонос В. В., Сухонос В. В., Сластьоненко О. О.

Система економічної безпеки України: проблеми та перспективи у юридичному вимірі..... 28

Фатхутдінова О. В., Шевченко Д. А., Санжаров В. А.

Середньовічна дипломатична практика: Англія та авіньйонське папство 39

Шевченко А. Є., Француз А. Й., Кудін С. В.

Методологічні засади нормативно-правового забезпечення інформаційної безпеки 48

Адміністративне право і процес; фінансове право;

інформаційне право

Касьяненко Л. М.

Правове регулювання податкових перевірок під час воєнного стану 56

Господарське право і процес

Дяченко С. В., Щербина А. А.

Господарське судочинство під час воєнного стану – зупиняти не можна продовжувати 66

Кримінальне право та кримінологія; кримінально-виконавче право

Бодунова О. М., Яцик Т. П., Лугіна Н. А.

Участь засобів масової інформації у запобіганні злочинності в умовах воєнного стану в Україні (на прикладі міста Ірпінь Київської області)..... 76

Вітюк Д. Л.

Характеристика міжнародних механізмів запобігання злочинності в умовах воєнного стану в Україні 90

Лаговська Н. В., Теслицький А. А.

Міжнародний досвід регулювання кримінальної відповідальності за ухилення від призову в умовах воєнного стану: досвід для України 97

Лугіна Н. А., Дем'яненко С. В.

Корупційні кримінальні правопорушення в умовах дії воєнного стану 108

Сперкач Н. А.

Торгівля людьми: сучасний стан, динаміка та напрями протидії..... 115

Топчій В. В., Дідківська Г. В.

Необхідність інформаційної безпеки під час окупації:

Ірпінь, Буча, Гостомель..... 125

*Кримінальний процес та криміналістика; судова експертиза;
оперативно-розшукова діяльність*

Кузьменко О. В., Левчук П. Р.

Особливості доказування у кримінальних провадженнях про пособництво

державі-агресору (на прикладі періоду окупації Київської області) 132

Свінцицький А. В.

Забезпечення участі осіб у кримінальному провадженні

в умовах воєнного стану: прикладні аспекти..... 141

Міжнародне право та право ЄС

Дідич Т. О., Шевченко А. Є.

Порівняльно-правовий аналіз положень Будапештського

меморандуму та його значення 150

Добрянська О. Д., Пунда О. О., Новицька Н. Б.

Правове положення військовополонених у міжнародному

гуманітарному праві: досвід російсько-української війни 157

CONTENTS

Theory and history of state and law; constitutional law

Stephen Humphreys

Cases That Made America. Fletcher v Peck, Fletcher v Peck and the Commercialization of America's Social Contract 9

Kopotun, I. Rudyk M.

Analysis of the security threats of Ukraine in the conditions of the martial state 20

Sukhonos V., Sukhonos V., Slastonenko O.

Economic Security System of Ukraine: Problems and Prospects in the Legal Dimension 28

Fathutdinova O., Shevchenko D., Sanzharov V.

Medieval Diplomatic Practice: England and Avignon Papacy 39

Shevchenko A., Frantsuz A., Kudin S.

Methodological principles of regulatory and legal support of information security 48

Administrative law and process; financial law; informational law

Kasianenko L.

Legal regulation of tax audits during martial law 56

Commercial law and process

Diachenko S., Shcherbyna A.

Commercial jurisdiction during martial state – it cannot be stopped to continue 66

Criminal law and criminology; Penal law

Bodunova O., Yatsyk T., Luhina N.

Participation of mass media in detection of crimes in martial law in Ukraine (on the example of Irpin, Kyiv region) 76

Vitiuk D.

Characteristics of international crime prevention mechanisms under the conditions of martial state in Ukraine 90

Lagovska N., Teslytskyi A.

International experience regulating criminal responsibility for conscription evasion in the conditions of martial state: experience for Ukraine 97

Luhina N., Demyanenko S.

Corruption criminal offenses under martial law 108

Sperkach N.

Human trafficking: current state, dynamics and countermeasures 115

Topchii V., Didkivska G.

The need for information security during the occupation:

Irpin, Bucha, Gostomel..... 125

*Criminal procedure and criminalistics; forensic examination;
operational-search activity***Kuzmenko O., Levchuk P.**

Features of proof in criminal proceedings on assistance to the aggressor state

(on the example of the period of occupation of the Kyiv region)..... 132

Svintsytskyi A.

Ensuring the participation of persons in criminal proceedings

under martial law: applied aspects..... 141

*International law and European Union law***Didych T., Shevchenko A.**

Comparative legal analysis of the norm of Budapest

Memorandum and its significance..... 150

Dobrianska O., Punda O., Novytska N.

Legal status of a prisoner of war in the international humanitarian law:

the experience of the russian-ukrainian war 157

УДК 343.9

DOI 10.33244/2617-4154.2(11).2023.125-131

В. В. Топчій,*д-р юрид. наук, професор,
заслужений юрист України
e-mail: tv1959@ukr.net***ORCID ID 0000-0003-4596-6469;****Г. В. Дідківська,***д-р юрид. наук, професор,
Державний податковий університет
e-mail: galynadid@gmail.com***ORCID ID 0000-0002-3545-0429**

НЕОБХІДНІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС ОКУПАЦІЇ: ІРПІНЬ, БУЧА, ГОСТОМЕЛЬ

У статті зазначено, що окупація територій Ірпеня, Бучі, Гостомеля та інших територій, що і досі в окупації, показала, що інформаційна маніпуляція є небезпечним чинником в умовах війни, яка, безперечно, ведеться повною мірою також і у кіберпросторі. Акцентується увага і на тому, що терміни «інформаційна війна», «інформаційна зброя» та «інформаційний тероризм» давно набули поширення, але в умовах воєнного часу вони набувають зовсім іншого значення з огляду на загрози, які існують. Тому пріоритетним завданням держави є сприяння формуванню інформаційної культури суспільства. Одним з елементів такої культури є здатність аналізувати інформацію та фільтрувати джерела її поширення.

Вказується, що на сьогодні основними можливостями розповсюдження інформаційних викривлень та отримання недостовірної інформації, особливо в умовах військових конфліктів та війни, можуть бути джерела надання інформації через інтернет-мережу різних соціальних груп або зчитування інформації з підроблених соціальних сторінок відомих політиків, акторів, підроблених сторінок відомих блогерів, отримання інформації через перегляд новин на теле- та радіомовних каналах країни-агресора.

У статті також зазначається, що інформаційна безпека має велике значення, а саме в періоди ведення війни та воєнних конфліктів. Адже неправильно, неправдиво подана інформація може призвести до хаосу у суспільстві, мати негативний вплив на перебіг подій, недовіру до керівництва держави, підривати авторитет ЗСУ, що може негативно впливати на ведення бойових дій, а також завдати невиправних тяжких наслідків перебігу військових дій. Ось чому запобігання розповсюдженню недостовірної інформації, особливо під час війни, має надважливе значення для стабілізації ситуації у нашій державі та остаточної перемоги над ворогом.

Ключові слова: інформаційна безпека, війна, військова агресія, тяжкі наслідки, воєнний конфлікт, кібератака, протидія розповсюдженню недостовірної інформації.

Враховуючи, що Україна зазнала військової агресії та щодо неї здійснено повномасштабне вторгнення з території рф і Білорусі від 24 лютого 2022 року, у нашій державі запроваджено воєнний стан. Водночас російські військові здійснюють агресію проти України і через соціальні мережі, інші засоби зв'язку. Кількість кібератак на державні інформаційні системи та об'єкти критичної інформаційної інфраструктури зростає втричі. Більшість нападів здійснюють військові хакери з ворожого боку, діяльність яких фінансується владою-терористом. Це відчутно особливо на територіях, які були окуповані: Буча, Ірпінь, Гостомель, інші тимчасово окуповані території, також які досі під окупацією і на територіях яких відчувається сильний інформаційний тиск ворога.

Тому основними механізмами протидії неправдивої, викривленої, неперевіреної інформації в умовах військових конфліктів і бойових дій вважають такі: необхідність формування медіаграмотності населення; медіаграмотність виступає як комплексний феномен, що дозволяє населенню захищатися, зокрема, від маніпулятивних впливів та брати участь у реалізації інформаційної безпеки; медіа грамотність має чотири важливі складові: критичне мислення, медіаорієнтування, медіаспоживання та медіадизайн. Медіаманіпуляція суспільною свідомістю чи думкою досягається за рахунок впливів на наше сприйняття через зір (це медіадизайн); через можливість орієнтуватися в інформаційних потоках, часто у рядового споживача їх досить багато, а часу мало на фактичне орієнтування; через великі обсяги контенту, які сипляться на кожну людини, також через неможливість критично сприймати інформацію через довіру, наприклад, конкретним ЗМІ [1].

Оскільки на початок військової агресії населення нашої держави не було інформаційно підготовленим, країна агресор всебічно цим скористалась.

Одним з основних завдань рф постало намагання завдати якомога більше шкоди звичайним людям шляхом як ракетних та інших обстрілів, так і кібератак, у зокрема і в інформаційному просторі.

Через воєнні дії багато установ перенесли свої дані – хтось в інші, більш спокійні регіони країни, хтось – у хмару на території України, хтось – у хмару за кордон. Проте, як і раніше, всі інформаційні системи, вимагають захисту. Захисту, який закріплений у законодавстві України. Інформаційні системи мають бути захищені за чинними стандартами. Зокрема, КСЗІ, а в деяких випадках допустиме використання європейських стандартів ISO/IEC 27 серії. Саме системи захисту інформації є першим кордоном, що стримує ворога від знищення нашої країни в кіберпросторі [2].

Варто акцентувати увагу, що поняття інформаційної безпеки, залежно від його використання, розглядається у декількох аспектах.

У найзагальнішому випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Під інформаційним середовищем розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на три основні предметні частини: створення і розповсюдження

вихідної та похідної інформації; формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг; споживання інформації. Також дві забезпечувальні предметні частини: створення та застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення; створення та застосування засобів і механізмів інформаційної безпеки.

Більш розгорнуте формулювання інформаційної безпеки – це стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Варто зазначити, що задоволення будь-якою мірою потреб в інформації приводить до оволодіння відомостями про навколишній світ та процеси, що протікають у ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності та, як наслідок, обґрунтованість рішень і дій, що приймаються.

Залежно від виду загроз інформаційній безпеці інформаційну безпеку можна розглядати так: забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації; інформація та інформаційні ресурси від неправомірного впливу сторонніх осіб; інформаційні права і свободи людини та громадянина.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави й акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [3].

Дещо відмінними є визначення, наведені та закріплені на законодавчому рівні.

Так, інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій;

інформаційна сфера – сукупність інформаційних технологій, ресурсів, продукції і послуг, інформаційної інфраструктури, суб'єктів інформаційної діяльності та системи регулювання суспільних інформаційних відносин;

інформаційна інфраструктура – сукупність організаційних структур і систем, які забезпечують функціонування та розвиток інформаційного простору, засобів інформаційної взаємодії та доступу користувачів до інформаційних ресурсів;

забезпечення інформаційної безпеки – діяльність, спрямована на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз інформаційній безпеці України;

загрози інформаційній безпеці – наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини та громадянина, суспільства і держави в інформаційній сфері [4].

Метою інформаційної безпеки вважають насамперед забезпечення безперервності бізнесу і захисту інформаційних даних, інфраструктури від випадкового чи навмисного втручання, що може стати причиною втрати даних або їх несанкціонованої зміни [5].

Етичні норми передбачають, що користувачі комп'ютерів не використовують комп'ютерну техніку та програмне забезпечення для завдання шкоди іншим людям, не порушують авторських прав.

Правові основи захисту даних базуються на правових актах, що утверджують права і свободи людини та якими встановлено відповідальність за злочини в галузі інформаційної безпеки. В Україні ухвалено ряд законів та постанов щодо забезпечення інформаційної безпеки: «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про захист персональних даних», «Про авторське право та суміжні права» тощо. Незаконне втручання в роботу комп'ютерів, комп'ютерних мереж та розповсюдження вірусів зумовлює кримінальну відповідальність (ст. 361 Кримінального кодексу України) [6].

Як показала окупація територій Ірпеня, Бучі, Гостомеля та інших територій, що і досі в окупації, інформаційна маніпуляція є небезпечним чинником в умовах війни, яка, безперечно, ведеться повною мірою також й у кіберпросторі. Терміни «інформаційна війна», «інформаційна зброя» та «інформаційний тероризм» давно набули поширення, але в умовах воєнного часу вони набувають зовсім іншого значення з огляду на загрози, які існують. Тому пріоритетним завданням держави є сприяння формуванню інформаційної культури суспільства. Одним з елементів такої культури є здатність аналізувати інформацію та фільтрувати джерела її поширення [7].

Отже, цілком слушною є думка, що інформаційна безпека передбачає: належний рівень інформаційної культури, тобто теоретичної та практичної підготовки особистості, за якого досягається захищеність і реалізація її життєво важливих інтересів та гармонійний розвиток в умовах інформаційного суспільства незалежно від наявності інформаційних загроз; здатність держави створити умови для гармонійного розвитку й задоволення потреб особи в інформації незалежно від наявності інформаційних загроз; гарантування, розвиток і використання інформаційного середовища в інтересах особистості; захищеність від різних інформаційних загроз [8]. У цьому контексті важливо зазначити важливість освітньої складової, яка полягає в систематичному навчанні інформаційній безпеці й інформаційній культурі у закладах середньої та вищої освіти, підвищенні кваліфікації для працівників органів державної влади та місцевого самоврядування, які працюють з інформацією. Згідно із Законом України «Про національну безпеку України» загрозами національній безпеці України є явища, тенденції і чинники, що унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [9].

Отже, варто мати на увазі, що гарною запорукою є підготовка кращої допомоги близьким і тим, хто особливо її потребує. Необхідно чітко розуміти послідовність впровадження заходів, які допоможуть більш ефективно впоратися з кризою окупації чи військової агресії та зменшити негативні наслідки для суспільства загалом. Коли безпека суспільства під загрозою, готовність до взаємної допомоги стає вирішальним чинником.

В умовах військової агресії Україна вимушена протидіяти ворожій пропаганді та дезінформації. Агресивні дії з боку росії мають на меті дестабілізувати наше суспільство та дискредитувати керівництво країни, змусити нас сумніватися у своїх силах і готовності захищатися. Питання інформаційної безпеки набуває особливого значення в умовах кризи, адже ворожі інформаційні атаки стають більш інтенсивними саме тоді, коли здатність суспільства чинити опір послаблено. Найкраще підґрунтя для ворожих операцій впливу – страх, паніка, дезорієнтація. Тому важливо дотримуватися базових правил інформаційної гігієни і бути особливо пильними до інформації, яка надходить і яку поширюєте ви самі [10].

Як бачимо, стрімке зростання соціальної значущості інформаційних технологій полягає в тому, що, як вважають дослідники, «соціальні мережі, месенджери, інтернет-магазини, онлайн-банкінг – усі ці засоби зв'язку та комунікації потенційно вразливі» [11].

На сьогодні основними можливостями розповсюдження інформаційних викривлень та отримання недостовірної інформації, особливо в умовах військових конфліктів і війни, можуть бути джерела надання інформації через інтернет-мережу різних соціальних груп або зчитування інформації з підроблених соціальних сторінок відомих політиків, акторів, підроблених сторінок відомих блогерів, отримання інформації через перегляд новин на теле- та радіомовних каналах країни-агресора.

Висновки. Як бачимо, інформаційна безпека має велике значення, а саме в періоди ведення війни та воєнних конфліктів. Адже неправильно, неправдиво подана інформація може призвести до хаосу у суспільстві, мати негативний вплив на перебіг подій, недовіру до керівництва держави, підривати авторитет ЗСУ, що може негативно впливати на ведення бойових дій, а також може завдати невинуватих тяжких наслідків перебігу військових дій. Ось чому запобігання розповсюдженню недостовірної інформації, особливо під час війни, має надзвичайне значення для стабілізації ситуації у нашій державі та остаточної перемоги над ворогом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bykov I. A., Balakhonskaya L. V., Gladchenko I. A., Balakhonsky V. V. Verbal aggression as a communication strategy in digital society. Proceedings of the 2018 IEEE Communication Strategies in Digital Society Workshop. Saint-Petersburg, 2018. P. 12–14.
2. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку. URL : <https://www.kmu.gov.ua/news/vymohy-do-zakhystu-informatsii-v-informatsiinykh-systemakh-u-voiennyi-chas-roziasnennia-derzhspetsvziazku> (дата звернення: 31.01.2023).
3. Поняття інформаційної безпеки. URL : <https://sites.google.com/site/infobezosob/home/informacijna-dialnist> (дата звернення: 31.01.2023).
4. Про засади інформаційної безпеки України : проєкт Закону України. URL : <https://ips.ligazakon.net/document/JG3TH00A?an=8> (дата звернення: 31.01.2023).
5. Хто стоїть на варті кібербезпеки. URL : <https://wiseit.com.ua/services/rishennya-ta-servisy/informacijna-bezpeka/> (дата звернення: 31.01.2023).

6. Основні поняття інформаційної безпеки. URL : <https://miyklas.com.ua/p/informatica/9-klas/programne-zabezpechennia-ta-informatciina-bezpeka-327110/informatciina-bezpeka-327251/re-813d7f93-b124-47bb-92c6-261cf0cd2162> (дата звернення: 31.01.2023).

7. Француз-Яковець Т. А. Інформаційна безпека в умовах війни. URL : <http://dspace.onua.edu.ua/bitstream/handle/11300/19251/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7-%D0%AF%D0%BA%D0%BE%D0%B2%D0%B5%D1%86%D1%8C%20%D0%A2%D0%B5%D1%82%D1%8F%D0%BD%D0%B0%20%D0%90%D0%BD%D0%B0%D1%82%D0%BE%D0%BB%D1%96%D1%97%D0%B2%D0%BD%D0%B0.pdf?sequence=1&isAllowed=y> (дата звернення: 31.01.2023).

8. Інформаційна безпека (соціально-правові аспекти) : підручник / В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк та ін. К. : КНТ, 2010. 776 с.

9. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради (ВВР)*. 2018. № 31.

10. Грошева Е. К., Невмержицкий П. И. Информационная безопасность: современные реалии. *Бизнес-образование в экономике знаний*. 2017. № 3. С. 35–38.

11. Пархоменко-Куцевіл О. І. Проблеми забезпечення інформаційної безпеки під час здійснення військових операцій та бойових дій. *Публічне управління у сфері державної безпеки та охорони громадського порядку*. 2022. Випуск 28. С. 177–181.

REFERENCES

1. Bykov I. A., Balakhonskaya L. V., Gladchenko I. A., Balakhonsky V. V. Verbal aggression as a communication strategy in digital society. *Proceedings of the 2018 IEEE Communication Strategies in Digital Society Workshop*. Saint-Petersburg, 2018. P. 12–14.

2. Vymohy do zakhystu informatsii v informatsiinykh systemakh u voiennyi chas: roz'iasnennia Derzhspetsviazku. URL : <https://www.kmu.gov.ua/news/vymohy-do-zakhystu-informatsii-v-informatsiinykh-systemakh-u-voiennyi-chas-roziasnennia-derzhspetsviazku> (data zvernennia: 31.01.2023).

3. Poniattia informatsiinoi bezpeky. URL : <https://sites.google.com/site/infobezosob/home/informacijna-dialnist> (data zvernennia: 31.01.2023).

4. Pro zasady informatsiinoi bezpeky Ukrainy : proekt Zakonu Ukrainy. URL : <https://ips.ligazakon.net/document/JG3TH00A?an=8> (data zvernennia: 31.01.2023).

5. Khto stoit na varti kiberbezpeky. URL : <https://wiseit.com.ua/services/rishennya-ta-servisy/informacijna-bezpeka/> (data zvernennia: 31.01.2023).

6. Osnovni poniattia informatsiinoi bezpeky. URL : <https://miyklas.com.ua/p/informatica/9-klas/programne-zabezpechennia-ta-informatciina-bezpeka-327110/informatciina-bezpeka-327251/re-813d7f93-b124-47bb-92c6-261cf0cd2162> (data zvernennia: 31.01.2023).

7. Frantsuz-Yakovets T. A. Informatsiina bezpeka v umovakh viiny. URL : <http://dspace.onua.edu.ua/bitstream/handle/11300/19251/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D1%83%D0%B7-%D0%AF%D0%BA%D0%BE%D0%B2%D0%B5%D1%86%D1%8C%20%D0%A2%D0%B5%D1%82%D1%8F%D0%BD%D0%B0%20%D0%90%D0%BD%D0%B0%D1%82%D0%BE%D0%BB%D1%96%D1%97%D0%B2%D0%BD%D0%B0.pdf?sequence=1&isAllowed=y>

Топчій В. В., Дідківська Г. В. Необхідність інформаційної безпеки під час окупації: Ірпінь, Буча, Гостомель

%90%D0%BD%D0%B0%D1%82%D0%BE%D0%BB%D1%96%D1%97%D0%B2%D0%BD%D0%B0.pdf?sequence=1&isAllowed=y (data zvernennia: 31.01.2023).

8. Informatsiina bezpeka (sotsialno-pravovi aspekty) : pidruchnyk / V. V. Ostroukhov, V. M. Petryk, M. M. Prysiazhniuk ta in. K. : KNT, 2010. 776 s.

9. Pro natsionalnu bezpeku Ukrainy : Zakon Ukrainy vid 21 chervnia 2018 roku № 2469-VIII. Vidomosti Verkhovnoi Rady (VVR). 2018. № 31.

10. Hrosheva E. K., Nevmerzhytskyi P. Y. Ynformatsyonnaia bezopasnost: sovremennyye realyy. Byznys-obrazovanye v ekonomyke znanyi. 2017. № 3. S. 35–38.

11. Parkhomenko-Kutsevil O. I. Problemy zabezpechennia informatsiinoi bezpeky pid chas zdiisnennia viiskovykh operatsii ta boiovykh dii. *Publichne upravlinnia u sferi derzhavnoi bezpeky ta okhorony hromadskoho poriadku*. 2022. Vypusk 28. S. 177–181.

V. Topchii, G. Didkivska. The need for information security during the occupation: Irpin, Bucha, Gostomel

This article states that the occupation of the territories of Irpin, Buchi, Gostomel and other territories, which are still under occupation, showed that information manipulation is a dangerous factor in the conditions of war, which is undoubtedly being waged in full in cyberspace as well. Attention is also focused on the fact that the terms "information war", "information weapon" and "information terrorism" have long been widespread, but in wartime conditions they acquire a completely different meaning in view of the threats that exist. Therefore, the priority task of the state is to promote the formation of society's information culture. One of the elements of such a culture is the ability to analyze information and filter the sources of its distribution.

It is indicated that today, the main possibilities of spreading information distortions and obtaining unreliable information, especially in the conditions of military conflicts and war, can be the sources of providing information through the Internet network of various social groups, or reading information from fake social pages of famous politicians, actors, fake pages of famous bloggers. Obtaining information through watching news on TV and radio channels of the aggressor country.

The article also notes that information security is of great importance, namely during periods of war and military conflicts. After all, incorrectly, falsely presented information can lead to chaos in society, have a negative impact on the course of events, distrust of the state leadership, undermine the authority of the Armed Forces, which can negatively affect the conduct of hostilities, and can also cause irreparable and serious consequences of the course of hostilities. That is why preventing the spread of false information, especially during wartime, is of paramount importance for the stabilization of the situation in our country and the final victory over the enemy.

Keywords: information security, war, military aggression, grave consequences, military conflict, cyber attack, countering the spread of false information.

Стаття надійшла до редколегії 28 лютого 2023 року

Наукове видання

ІРПІНСЬКИЙ ЮРИДИЧНИЙ ЧАСОПИС

Науковий журнал
2023. Випуск 2 (11)

НАД ВИПУСКОМ ПРАЦЮВАЛИ:

Відповідальний за випуск

Бодунова О. М.

Редактор-коректор

Грабарчук М. М.

**Технічне редагування
та комп'ютерне верстання**

Лисенко О. В.

Підп. до друку 10.05.2023. Формат 75 × 108/16.

Ум.-друк. арк. 9.7. Обл.-вид. арк. 10.0.

Тираж 300 пр. Зам. № 1046.

Видавець і виготовлювач

Державний податковий університет

вул. Університетська, 31, м. Ірпінь, Київська обл., 08205

+38(068)904-22-32

e-mail: irpin-yur-chas@ukr.net

*Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції
Серія ДК № 7669 від 20.09.2022*
