УДК 355.40

Р. Ю. Прав,
аспірант Міжрегіональної Академії управління персоналом,
Кафедра менеджменту та адміністрування начально-наукового інституту менеджменту, економіки та фінансів МАУП, Приватне акціонерне товариство "Вищий навчальний заклад "Міжрегіональна Академія Управління персоналом"
ORCID ID: 0000-0001-8064-2836

DOI: 10.32702/2306-6814.2020.2.141

ПРОТИДІЯ ЗОВНІШНІМ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ В УКРАЇНІ

R. Prav,
Graduate student of the Interregional Academy of Personnel Management Department of Management and Administration of the Educational — Scientific Institute of Management, Economics and Finance of IAPM, Private Joint-Stock Company "Higher Educational Institution "Interregional Academy of Personnel Management"

COMBATING EXTERNAL INFORMATION THREATS IN UKRAINE

Розвиток інформаційного суспільства на шляху глобалізації, несе в собі безліч викликів і загроз, серед яких на перший план виступають посилення владних повноважень окремих осіб, соціальних груп і держав. Небезпеки, що створюються даними загрозами, часто змушують залишати в стороні погодження гострих соціальних проблем, формують умови фінансово-економічної нестабільності і створюють передумови соціальної та політичної деструкції. При цьому відсутність жорсткої територіальної прив'язки ключових інформаційних ресурсів дозволяє інформаційно-комунікаційним лідерам опановувати і використовувати будь-яке втручання. Ефективне освоєння чужих територій стає можливим шляхом використання інформаційної локалізації. В результаті, на думку ряду дослідників, відбувається зміна характеру і стилю соціально-економічного життя, матеріальне середовище симулюється, зберігаючи атрибутику реальності в формі віртуально-операційного середовища, яке створюють інформаційно-комунікаційні комплекси, що відображають на пристроях візуалізації атрибутику реальності і забезпечує імітацію управління простим натисканням клавіші.

Забезпечення інформаційної безпеки обумовлена необхідністю прийняття ефективних, відповідних політичним завданням, управлінських рішень. Залежність від інформації та інформаційних технологій стає одним з передумов формування суспільства. Володіння своєчасними, точними, достовірними даними слугує надзвичайно важливим фактором ефективності прийняття управлінських рішень як на державному рівні, так і на рівні регіонів України.

Таким чином, у процесі написання статті досліджено проблему інформаційної безпеки України та проаналізували теоретичні підходи до визначення сутності поняття інформаційна безпека. Розкрито сутність політики державної безпеки у інформаційній сфері та зробилено аналіз загроз. Здійснено оцінювання ефективності та узагальнити проблеми в реалізації державної політики органами влади щодо протидії інформаційним загрозам в Україні. Встановлено, що позиції України у світовому масштабі щодо забезпечення інформаційної безпеки — є незначними.

The development of an information society on the path of globalization carries many challenges and threats, among which are the strengthening of the powers of individuals, social groups and states. The dangers posed by these threats often force them to agree on acute social problems, create conditions for financial and economic instability, and create preconditions for social and political destruction. In the absence of rigid territorial linkage of key information resources, information and communication leaders can master and use any interference. Effective development of foreign territories becomes possible through the use of information localization. As a result, according to

some researchers, there is a change in the nature and style of socio-economic life, the material environment is simulated, keeping the attributes of reality in the form of virtual — operating environment, which create information and communication complexes, reflecting on the devices of visualization of the attributes of reality and provide simulation of management a simple keystroke.

Ensuring information security is driven by the need to make effective, policy-relevant management decisions. Dependence on information and information technology is one of the prerequisites for shaping society. Having timely, accurate, reliable data is an extremely important factor in the effectiveness of managerial decision-making at both the state and regional levels of Ukraine.

Thus, in the process of writing the article, the problem of information security of Ukraine was explored and theoretical approaches to defining the essence of the concept of information security were analyzed. Disclosed the essence of national security policy in the information field and analyzed the threats. Assessment of effectiveness and generalization of problems in the implementation of state policy by the authorities on counteracting information threats in Ukraine. It is found that Ukraine's position in the world on information security is insignificant.

Ключові слова: інформаційна безпека, інформація, загрози, державна безпека, інформаційні загрози.
Key words: information security, information, threats, state security, information threats.

ПОСТАНОВКА ПРОБЛЕМИ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ АКТУАЛЬНИМИ ЗАВДАННЯМИ

Інформація представляє собою стратегічну цінність як для держави, так і будь-якої управлінської структури в системі політичного управління. Якість функціонування та безпека інформаційної сфери, так само як і стан нормативно-правового регулювання відносин у цій сфері визначає рівень розвитку держави. Варто відзначити, що останнім часом виникає досить багато питань щодо того, як саме має виглядати протидія зовнішнім загрозам в Україні.

Необхідність гарантування інформаційної безпеки зумовлене [2]:

— потребою забезпечення національної безпеки України загалом;

— існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам;

— врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей.

Завдання інформаційної безпеки — створення системи протидії інформаційним загрозам [3] та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. У разі виникнення криз, загострення конфліктів інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї [2, с. 69].

ДОСЛІДЖЕННЯ ТА ПУБЛІКАЦІЇ, НА ЯКІ СПИРАЄТЬСЯ АВТОР, ВИДІЛЕННЯ НЕВИРІШЕНИХ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ ДАНА СТАТТЯ

Проблемними питання циркулювання інформації та формування політики державної безпеки в інформаційній сфері займались такі дослідники В.В. Антонюк [1], І.Р. Бондаря [4], О.С. Виговська [6], В.П. Горбулін [7; 8], Г.П. Ситник [13], О.М. Степко [14], Т.Ю. Ткачук [15] та інші. Аналізуючи внесок науковців у розвиток досліджень з окресленої тематики стверджуємо, що значно менша увага приділялась питанню державного управління у інформаційній сфері, а саме: формуванню дієвої політики державної безпеки у інформаційному аспекті, механізмів її формування та реалізації, особливо, в умовах гібридних загроз. У ст. 1 Закону України "Про національну безпеку України" № 2469-VIII від 21 червня 2018 року (зі змінами та доповненнями) зазначено, що державна безпека — захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво-важливих національних інтересів від реальних і потенційних загроз невоєнного характеру [12]. Разом із тим, подолання зовнішніх інформаційних загроз висвітлено авторами недостатньо.

МЕТА СТАТТІ

Мета статті — дослідити проблему інформаційної безпеки України та проаналізувати теоретичні підходи до визначення сутності поняття інформаційна безпека.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Ринок інформаційної безпеки в Україні існує і розвивається, не враховуючи небезпечної неприємної ринкової обстановки. У нашому розумінні учасники ринкової інформаційної безпеки окрім користувачів та надання послуг і рішень, також українські та міжнародні регулятори. Також учасниками можна вважати новий для України сегмент, страхування ризиків інформаційних технологій (послуга в Україні лише починає розвиватися). На рисунку 1 приведено структуру сучасного ринку інформаційної безпеки України.

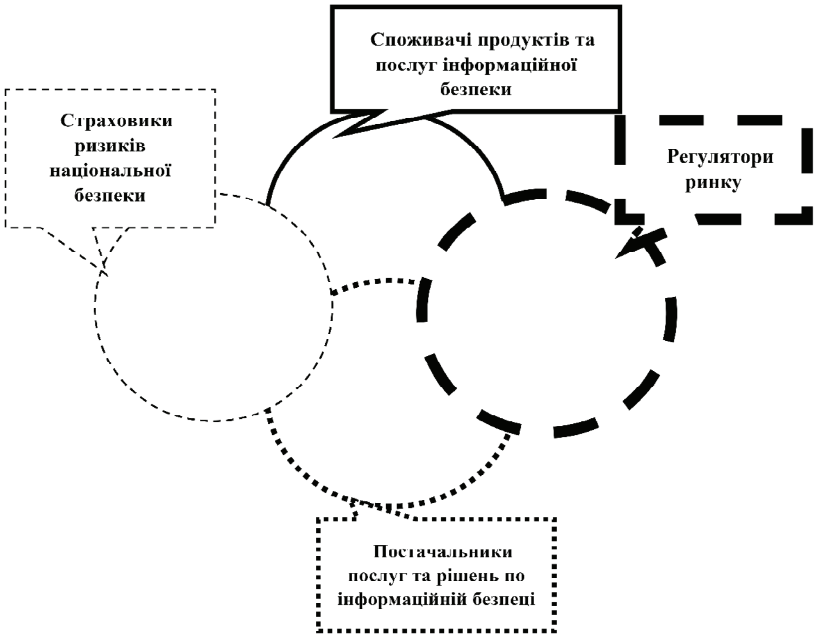

Рис. 1. Структура учасників ринку інформаційної безпеки України

Джерело: власна розробка автора на основі [9; 12; 13].

Загалом ринок інформаційної безпеки в Україні в основному сформовано і досить успішно розвивається.

Можна виділити основні проблеми для ринку інформаційної безпеки в Україні:

— відсталість законодавства в питаннях регулювання захисту інформації, що становить комерційну таємницю;

— психологічна проблема менеджменту більшості компаній (спочатку інцидент ІБ повинен завдати шкоди і тільки після цього починаються заходи щодо захисту інформації);

— відсутність дієвого механізму оцінки бренду (нездатність оцінити репутаційні ризики для компанії);

— нечітке сегментування ринку і, як наслідок, непрозоре ціноутворення.

Щодо загроз безпеці, то їх у загальному вигляді визначають як сукупність чинників та умов, що створюють небезпеку певному об'єкту. В. Горбулін та А. Качинський розглядають загрозу як родову ознаку безпеки (можливість чи неминучість виникнення соціальних, природних або техногенних явищ із прогнозованими, але неконтрольованими небажаними подіями, що можуть статись у певний момент часу в межах певної території, спричинити смерть людей чи завдати шкоди їхньому здоров'ю, призвести до матеріальних і фінансових збитків тощо) [8, с. 14, 27—28]. Небезпеку ж науковці вважають якісним станом — безпекою на її нульовому рівні [8, с. 13].

Під час аналізу інформаційних загроз можна виокремити їх види, але самі загрози постійно змінюються, тому механізм протидії конкретним загрозам розробляється після їх виявлення та ідентифікацію. Загрози, як правило, мають комплексний характер, відтак їх прояви дуже різноманітні. Зовнішні загрози впливають на внутрішню безпеку країни, і не лише в інформаційній сфері; так само загрози, що виникають всередині країни, можуть впливати на її зовнішню безпеку.

Зовнішні загрози залежать передусім від незалежних і неконтрольованих факторів, на які важко вплинути, тому досягти такого стану, в якому б цих загроз не було, практично неможливо. Також важко скласти список усіх загроз "на всі часи", оскільки вони змінюються, а ще частіше приховуються. Тому наразі відбувається відхід від сприйняття загроз як сталої проблеми і перехід до управління ризиками. Аналіз загроз — це виявлення ризиків з метою їх зменшення; він має бути процесом постійним і включати:

— аналіз інцидентів небезпек у попередньому періоді та заходів, що приймалися для усунення ризиків;

— аналіз корисності та ефективності заходів протидії, здійснених для усунення ризиків;

— виявлення нових потенційних загроз для суспільних, державних, інформаційних, організаційних процесів тощо;

— аналіз ймовірності ескалації загроз;

— аналіз можливих прямих та непрямих наслідків реалізації загроз;

— визначення ризиків, від яких необхідно забезпечити захист;

— визначення заходів запобігання ризикам, мінімізації шкоди від них;

— оцінювання, чи мінімізований ризик є прийнятним;

— вживання заходів для попередження аналогічних ризиків;

— оцінка, після визначеного періоду, ефективності вжитих заходів; якщо загрози залишаються, слід розробляти і вживати заходи на протидію їм.

Заходи протидії спрямовуються саме на ризики як об'єкти управління. Визначимо заходи протидії інформаційним загрозам, актуальним для України в сучасних умовах гібридної війни з Росією.

До прикладу, у 2018 році було виявлено, проаналізовано та спростовано у відкритих джерелах ряд фейкових і маніпулятивних повідомлень, які є загрозами національній інформаційній безпеці. Зокрема [10]:

— фейк "Україна включила Естонію до списку офшорів";

— маніпулятивний звіт Amnesty International;

— блокування українських активістів у соціальних мережах через скарги російських тролів;

— фейк "українці радіють смертям у Кемерово";

— публікації "НА Харьков" та "Политнавигатора", що розпалюють міжнаціональну ворожнечу;

— фейковий канал ГУР МО в Telegram;

— фейки про Україну від журналістів міжнародних видань у Москві;

— фейк про підрив автомобіля з бійцями НАТО на Донбасі;

— пов'язування України з діяльністю ІДІЛ;

— містифікація про трьох мертвих канадських солдатів в Україні від росЗМІ;

— фейк "Шотландский парламент аплодує візиту українського фашиста";

— публікація архіву з 3 млн твітів російських тролів;

— зміна політики Telegram щодо персональних даних;

— візит "представників громадських організацій США" до Криму.

Захист вітчизняного інформаційного простору потребує забезпечення громадян "чистим" контентом, фільтрованим від сепаратистського, проросійського наповнення. Заборона поширення російської пропаганди на території України немає нічого спільного з придушенням свободи слова і демократії, як говорять про це симпатики "руського міра". Це захист національних інтересів від деструктивних впливів країни-агресора. Тому в Україні має бути заблоковане мовлення ворожих нам ЗМІ, які віщують як з території Росії, так і з підконтрольних їй українських територій.

Необхідно прийняти спеціальний закон щодо регулювання діяльності інтернет-медіа. Саме його відсутність у наш час уможливлює поширення неконтрольованого потоку новин сепаратистського спрямування, що розпалює ворожнечу між членами суспільства, які живуть в різних частинах держави. У спеціальному законі має бути визначено порядок ліцензування, правовий статус, принципи діяльності інтернет-медіа, їхні права й обов'язки, передбачено відповідальність за пропагандистський / ворожий контент, аж до відібрання ліцензії на діяльність.

Як конкретні методи протидії інформаційно-психологічним впливам для захисту інформаційного простору фахівцями пропонуються [5, с. 187]:

— встановлення та перекриття (знешкодження) потенційних каналів проникнення деструктивної інформації в національний інформаційний простір;

— пряме та непряме спростування джерела деструктивного впливу (сумнівність щодо джерела інформації; абсурдність звинувачень; прив'язка джерела інформації до будь-якої негативної події; введення ще одного негативного факту, який легко піддається спростуванню);

— відволікання уваги (відволікання ресурсів противника на інший об'єкт шляхом перенаправлення його на іншу діяльність; введення в інформаційний простір нового сенсаційного повідомлення; відвертання уваги;

— аудиторії на малозначущий факт у рамках поточної проблеми);

— мовчання у відповідь;

— мінімізація впливу (акцентування на тому, що в повідомленні вказано на деякі правдиві події тощо);

— дискредитація (обнародування компромату; негативна "похвала"; громадське обурення);

— розмиття негативу (генерація нейтральної або позитивної інформації про об'єкт в об'ємах, що перевищують об'єми негативної інформації).

На державному рівні повинна бути створена інформаційна технологія протидії ворожій російській пропаганді, яку повинні використовувати всі владні структури, відповідальні за інформаційну безпеку в Україні. Вони повинні оперативно реагувати на нові компромати, що постійно з'являються у вітчизняному інформаційному просторі, який, на жаль, нині не контролюється ефективно державою. Отже, слід створити базу контраргументів російським повідомленням, яку можна було б використовувати не лише постфактум, а й попереджувально.

ВИСНОВКИ І ПРОПОЗИЦІЇ

За результатами дослідження можна встановити, що актуальність зовнішніх інформаційних загроз у сучасних умовах є вищою, ніж внутрішніх в Україні. Щороку Україна стикається із великою кількості неправдивої інформації, що поширюється в мережах і потребує виявлення та спростування. Не напрацьовано ефективної системи протидії таким загрозам та попередження їх виникнення, недостатньо екфективно сформована інформаційна політика держави на зовнішніх ринках. Перспективними для подальших досліджень є питання напрацювання механізмів подолання зовнішніх загроз.

Література:

1. Антонюк В.В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці / В.В. Антонюк // Державне управління: удосконалення та розвиток. — Вип. 8 (10). — 2014. — С. 1—5.

2. Боднар І.Р. Державна політика та інформаційна безпека України: післякризові виклики / І.Р. Боднар, О.М. Вовчанська // Вісник Львівської комерційної академії. Серія економічна. — 2014. — Вип. 46. — С. 28—32 [Електронний ресурс]. — Режим доступу: http://nbuv.gov.ua/UJRN/Vlca_ekon_-2014_46_7

3. Бойченко О.В. Міжнародна інформаційна безпека: проблеми і перспективи / О.В. Бойченко // Форум права. — 2009. — № 3. — С. 74—79.

4. Бондаренко В., Литвиненко О. Інформаційна безпека сучасної держави: концептуальні роздуми / В. Бондаренко, О. Литвиненко [Електронний ресурс]. — Режим доступу: http://www.crime-research. iatp. org. ua/ library/strateg. Htm

5. Вакуленко Р.В. Огляд та аналіз методів протидії інформаційним впливам супротивника в умовах інформаційної війни / Р.В. Вакуленко // Актуальні задачі та досягнення у галузі кібербезпеки. Матеріали Всеукраїнської науково-практичної конференції 23—25 листопада 2016 року, м. Кропивницький. — С. 186—187.

[Електронний ресурс]. — Режим доступу: https://core.ac.uk/download/pdf/84825417.pdf

6. Виговська О.С. Теоретико-методологічні підходи до проблеми державного регулювання політики інформаційної безпеки / О.С. Виговська // Актуальні проблеми міжнародних відносин. — 2012. — Вип. 108 (1). — С. 96—101 [Електронний ресурс]. — Режим доступу: http://nbuv.gov.ua/UJRN/apmv_2012_108%281%29__15

7. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: [монографія] / В. Горбулін, О. Додонов, Д. Ланде. — К.: Інтертехнологія, 2009. — 164 с.

8. Горбулін В.П. Засади національної безпеки України / В. Горбулін, А. Качинський. — К.: Інтертехнологія, 2009. — 272 с.

9. Державний центр кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України [Електронний ресурс]. — Режим доступу: https://cert.gov.ua/

10. Моніторинг інформаційних загроз 2018 [Електронний ресурс]. — Режим доступу: https://www.ukrinform.ua/rubric-society/2606432-monitoring-informacijnih-zagroz-2018.html

11. Питання Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України: Указ Президента України від 06 жовт. 2000 р. № 1120 // Офіц. вісн. України. — 2000. — № 41.

12. Про національну безпеку України: Закон Україні від 21.06.2018 р. № 2469-VIII // Відомості Верховної Ради (ВВР). 2018. № 31. Ст. 241.

13. Ситник Г.П. Державне управління у сфері забезпечення національної безпеки України: теорія і практика: дис. доктора наук з держ. упр. за спеціальністю 25.00.01. — теорія та історія державного управління. — Національна академія державного управління при Президентові України. — Київ, 2004.

14. Степко О.М. Аналіз головних складових інформаційної безпеки держави / О.М. Степко // Науковий вісник Інституту міжнародних відносин НАУ. — Сер.: Економіка, право, політологія, туризм. — К.: Вид-во Нац. авіац. ун-ту "НАУ-друк", 2011. — Вип. 1 (3). — С. 90—99.

15. Ткачук Т.Ю. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі / Т.Ю. Ткачук // Науковий вісник Ужгородського національного університету. Серія Право. — 2017. — Вип. 46. Том 2. — С. 39—42.

16. Третяк Г.С. Державне регулювання економіки та економічна політика [Текст]: навч. посіб. / Г.С. Третяк, К.М. Бліщук. — Львів: ЛРІДУ НАДУ, 2011. — 128 с.

References:

1. Antoniuk, V.V. (2014), "Mechanisms of state response to modern challenges and threats information security", Derzhavne upravlinnia: udoskonalennia ta rozvytok, vol. 8 (10), pp. 1—5.

2. Bodnar, I.R. and Vovchanska, O.M. (2014), "State Policy and Information Security of Ukraine: Post-Crisis Challenges", Visnyk Lvivskoi komertsijnoi akademii. Seriia ekonomichna, vol. 46, pp. 28—32, available at: http://nbuv.gov.ua/UJRN/Vlca_ekon_2014_46_7 (Accessed 12 Jan 2020).

3. Bojchenko, O.V. (2009), "International Information Security: Challenges and Prospects", Forum prava, vol. 3, pp. 74—79.

4. Bondarenko, V. and Lytvynenko, O. (1999), "Information security of the modern state: conceptual reflections", available at: http://www.crime-research.iatp.org.ua/library/strateg.Htm (Accessed 11 Jan 2020).

5. Vakulenko, R.V. (2016), "Review and analysis of methods of counteraction to information influences of the enemy in the conditions of information war", Aktualni zadachi ta dosiahnennia u haluzi kiberbezpeky. Materialy Vseukrainskoinaukoi praktychnoi konferentsii 23—25 lystopada 2016 roku, m. Kropyvnytskyj, pp. 186—187, available at: https://core.ac.uk/download/pdf/84825417.pdf (Accessed 10 Jan 2020).

6. Vyhovska, O.S. (2012), "Theoretical and methodological approaches to the problem of state regulation of information security policy", Aktualni problemy mizhnarodnykh vidnosyn, vol. 108 (1), pp. 96—101, available at: http://nbuv.gov.ua/UJRN/apmv_2012_108%281%29__15 (Accessed 12 Jan 2020).

7. Horbulin, V. Dodonov, O. and Lande, D. (2009), Informatsijni operatsii ta bezpeka suspilstva: zahrozy, protydiia, modeliuvannia [Information operations and society security: threats, counteraction, modeling], Inter tekhnolohiia, Kyiv, Ukraine.

8. Horbulin, V.P. and Kachyns'kyj, A. (2009), Zasady natsionalnoi bezpeky Ukrainy [National Security Principles of Ukraine], Inter tekhnolohiia, Kyiv, Ukraine.

9. Computer Emergency Response Team of Ukraine (2019), available at: https://cert.gov.ua/ (Accessed 11 Jan 2020).

10. Zolotukhin, D. (2018), "Monitoring information threats in 2018", available at: https://www.ukrinform.ua/rubric-society/2606432-monitoring-informacijnih-zagroz-2018.html. (Accessed 10 Jan 2020).

11. President of Ukraine (2000), Decree "Questions of the Special Telecommunication Systems and Information Protection Department of the Security Service of Ukraine", Ofitsijnyj visnuk Ukrainy, vol. 41.

12. The Verkhovna Rada of Ukraine (2018), The Law of Ukraine "On national security of Ukraine", Vidomosti Verkhovnoi Rady (VVR), vol. 31, pp. 241.

13. Sytnyk, H.P. (2004), "Public Administration in the Field of National Security of Ukraine: Theory and Practice", Abstract of Doctor of Science in Public Administration, Theory and history of public administration, National Academy of Public Administration under the President of Ukraine, Kyiv, Ukraine.

14. Stepko, O.M. (2011), "Analysis of the main components of information security of the state", Naukovyj visnyk Instytutu mizhnarodnykh vidnosyn NAU. Ser: Ekonomika, pravo, politolohiia, turyzm, vol. 1 (3), pp. 90—99.

15. Tkachuk, T.Yu. (2017), "State policy in the field of information security at the present stage", Naukovyj visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia Pravo. vol. 46, no. 2, pp. 39—42.

16. Tretiak, H.S. and Blischuk, K.M. (2011), Derzhavne rehuliuvannia ekonomiky ta ekonomichna polityka [State regulation of the economy and economic policy], LRIDU NADU, Lviv, Ukraine.

Стаття надійшла до редакції 13.01.2020 р.