УДК 340:007
DOI https://doi.org/10.32782/2524-0374/2022-1/54

ПРОТИДІЯ ДЕСТРУКТИВНОМУ ІНФОРМАЦІЙНОМУ ВПЛИВУ В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ

COUNTERACTING DESTRUCTIVE INFORMATION INFLUENCE IN UKRAINE: LEGAL AND ORGANIZATIONAL ASPECTS

Черниш Р.Ф., к.ю.н., доцент,
завідувач спеціальної кафедри
Національна академія Служби безпеки України

Ігнатюк М.В., директор бібліотеки
Поліський національний університет

Заріцький О.Ю., здобувач вищої освіти другого (магістерського) рівня
факультету права, публічного управління та національної безпеки
Поліський національний університет

У статті досліджено мету нормативно-правового регулювання організаційних і практичних заходів із забезпечення інформаційної безпеки України. Проаналізовано класифікацію загроз та обґрунтовано пріоритети розвитку правових основ державної політики України у цій сфері. Визначено суб'єкти забезпечення інформаційної безпеки та шляхи удосконалення механізму протидії сучасним загрозам деструктивного інформаційного впливу в умовах гібридної війни проти України.

Захист українського інформаційного простору від негативних впливів інформаційно-психологічного характеру, операцій та інформаційних війн, гарантування безпеки та інформаційного суверенітету набувають особливого значення і трансформуються у фактори збереження української національної ідентичності та функціонування України як суверенної й незалежної держави. Важливість зазначених питань зумовила вибір теми дослідження та свідчить про її актуальність.

Система правового регулювання інформаційного захисту країни становить масив юридичних норм, що регулюють взаємовідносини в цій сфері, безпосередньо правові відносини, які формуються під час використання цих норм, та відповідні акти правозастосування. Сьогодні відсутні чітко обґрунтовані і взаємозумовлені підходи до забезпечення інформаційного захисту країни, тому ефективну систему протидії злочинності в інформаційному просторі може забезпечити запровадження і реалізація аргументованої чіткої державної політики за цим напрямом.

Наведені вище загрози являють собою комплекс умов та чинників, які становлять небезпеку життєво важливим державним, суспільним та особистісним інтересам у зв'язку з імовірністю виникнення негативного впливу інформації на свідомість і поведінку громадськості, а також на інформаційні ресурси країни та відповідну інфраструктуру. У сфері інформаційного захисту держави можуть визначатися зовнішні та внутрішні, потенційні та реальні тощо види загроз відповідно до джерел утворення, якими можуть бути людина, технічні або програмні засоби, технологічні схеми обробки, зовнішнє оточення тощо.

Державна інформаційна політика на сучасному етапі розвитку українського суспільства має бути спрямована на вирішення завдань щодо збалансованого забезпечення інформаційної безпеки громадян, суспільства та держави поряд з паралельним виділенням актуальних пріоритетів у необхідний момент.

Ключові слова: державна інформаційна політика, інформаційна безпека, інформаційний захист, інфраструктура, негативний вплив, суб'єкти державної влади.

The article examines the purpose of regulatory regulation of organizational and practical measures to ensure information security of Ukraine. The classification of threats is studied and the priorities of development of legal bases of the state policy of Ukraine in this sphere are substantiated. The subjects of information security and ways to improve the mechanism of counteracting modern threats of destructive information influence in the conditions of a hybrid war against Ukraine are identified.

Protection of the Ukrainian information space from the negative influences of information and psychological nature, operations and information wars, guaranteeing security and information sovereignty become especially important and are transformed into factors of preserving the Ukrainian national identity and functioning of Ukraine as a sovereign and independent state. The importance of these issues led to the choice of research topic and indicates its relevance.

The system of legal regulation of information protection of the country is an array of legal norms governing the relationship in this area, directly the legal relations that are formed when using these norms, and the relevant acts of law enforcement. Today there are no clearly grounded and mutually agreed approaches to ensuring information protection of the country, so an effective system of combating crime in the information space can provide the introduction and implementation of a reasoned clear public policy in this area.

The above threats are a set of conditions and factors that threaten vital state, public and personal interests due to the likelihood of negative impact of information on public consciousness and behavior, as well as on the country's information resources and infrastructure. In the field of information protection of the state, external and internal, potential or real and other types of threats can be identified according to the sources of education, which can be people, hardware or software, technological processing schemes, external environment, etc.

State information policy at the present stage of development of Ukrainian society should be aimed at solving problems of balanced information security of citizens, society and the state, along with the parallel allocation of current priorities at any time.

Key words: state information policy, information security, information protection, infrastructure, negative impact, subjects of state power.

Інформаційна безпека виступає інтегрованим компонентом національної безпеки і позиціонується як пріоритетна функція держави. З одного боку, інформаційна безпека спрямована на забезпечення якісного всебічного інформування громадян та їх необмеженого доступу до різних інформаційних джерел. З іншого боку, вона передбачає контроль за непоширенням дезінформації, сприяння суспільній цілісності, охорону інформаційного суверенітету, протидію негативним інформаційним впливам пропагандистського та психологічного характеру, а також захист державного інформаційного простору від різних маніпуляційних дій та інформаційних війн. Розв'язання комплексної проблеми інформаційної безпеки дасть можливість, по-перше, захистити суспільні і державні інтереси, по-друге, гарантувати права громадян на користування інформацією всебічного, об'єктивного та якісного характеру.

Вітчизняний дослідник Б. Кормич виокремлює два аспекти характеристики інформаційної безпеки відносно поняття «національна безпека». З одного боку, інфор-

маційна безпека трактується як самостійний компонент національної безпеки будь-якої держави. З іншого боку, інформаційна безпека – це інтегрований складовий елемент будь-якої іншої безпеки – військової, економічної, політичної тощо. На думку вченого, оптимальним є таке визначення: «Інформаційна безпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і країни, за якого мінімізується завдання збитків через неповноту, невчасність і невідповідність інформації, негативний інформаційний вплив, негативні наслідки реалізації інформаційних технологій, а також через заборонене розповсюдження інформації» [1].

Забезпеченню інформаційної безпеки України, безпеки державних інтересів в інформаційному просторі сприятиме пріоритетний розвиток відповідної системи нормативно-правового регулювання протидії загрозам цих інтересів та впорядкування правотворчого процесу у сфері аналізу, узагальнення, використання та розповсюдження інформації.

Необхідність такого розвитку системи нормативно-правового забезпечення зумовлена певними факторами. По-перше, в умовах функціонування правової держави та громадянського суспільства основні функції органів державної влади, на які покладено основну відповідальність за національну безпеку, мають регулюватися визначеними правовими нормами, спрямованими на забезпечення громадянських конституційних прав і свобод. Правотворчість у цьому контексті спрямована на нормативне закріплення завдань протидії загрозам національній безпеці України, засобів та методів їх виконання, забезпечення погоджувальної політики владних органів. По-друге, курс України на інтеграцію в міжнародне співтовариство істотно розширює можливості закріплення концептуальних засад державної інформаційної безпеки шляхом участі в розвитку міжнародно-правових норм у цій сфері, формування міжнародної системи забезпечення інформаційної безпеки в світовому масштабі та в рамках кожної окремої країни. По-третє, реалізація гарантій громадянських прав та свобод, захисту державних інтересів нашої країни передбачає суттєве збільшення ролі владних органів у регулюванні відповідних суспільних відносин, присутність прозорої та зрозумілої державної політики [2].

Ю. Максименко під нормативно-правовим регулюванням інформаційної безпеки України розуміє таку форму владного правового впливу на інформаційні відносини у суспільстві, яка реалізується державою з метою їх упорядкування, закріплення і забезпечення. Також вчений підкреслює, що у сучасних умовах існування українського суспільства одним із найважливіших напрямів стратегії адміністративно-правового забезпечення інформаційної безпеки нашої країни виступає аналіз та удосконалення нормативно-правового регулювання за цим напрямом [3].

Н. Новицька зазначає, що система правового регулювання інформаційної безпеки являє собою масив правових норм, які регулюють відносини в цій галузі, правові відносини, які формуються на підставі застосування правових норм, та відповідні акти правозастосовного характеру.

Правові норми формують базу забезпечення інформаційної безпеки і зумовлюють ефективність діяльності держави, суспільства та окремих громадян у контексті захисту національних інтересів України в сфері споживання і використання інформації. До такої нормативно-правової бази належать норми міжнародних договорів України, закони України, акти Президента України, постанови Уряду, нормативно-правові документи органів державної влади, які спрямовані на регулювання відносин у досліджуваній сфері [4].

Ключовим недоліком нормативно-правового регулювання інформаційної безпеки в нашій країні є його розгалуження через велику кількість нормативно-правових документів різної юридичної сили. Дуже часто виникає ситуація, коли важливі і нагальні питання унормовуються за допомогою підзаконних нормотворчих актів. Не сприяє результативному забезпеченню інформаційної безпеки України й неузгодженість нормативно-правових документів як між собою, так і з чинними конституційними нормами.

Характерною рисою положень українського законодавства, яке регулює процеси в інформаційній сфері, є декларативність багатьох юридичних норм без визначення шляхів їх реалізації, що зумовлює невисокий рівень ефективності їх застосування у рамках регулювання суспільних відносин для забезпечення інформаційної безпеки. До того ж присутність значної кількості бланкетних (відсильних) правових норм, певного масиву абстрактних або суб'єктивних понять, яким необхідне офіційне тлумачення або чіткіше трактування, відсутність закріплення фундаментальних основних дефініцій виступають джерелами загроз українській інформаційній безпеці. Дослідження нормативно-правової бази із забезпечення інформаційної безпеки нашої країни свідчить про необхідність удосконалення відповідного законодавства [5].

Питання забезпечення державних інтересів і державної безпеки у сфері отримання і використання інформації не втрачають своєї актуальності. Інформаційна безпека забезпечується здійсненням єдиної державної політики в рамках національної інформаційної безпеки, а також системою економічних, політичних та організаційних заходів, що спрямовані на протидію наявним і можливим загрозам та небезпекам національним інтересам (особисті, суспільні та державні) в інформаційній сфері.

Для досягнення і підтримання необхідного рівня національної безпеки в інформаційному просторі розробляється система юридичних норм, спрямованих на регулювання відносин в інформаційній сфері, виокремлення ключових напрямів діяльності органів державного управління, заснування або реорганізацію органів і сил забезпечення інформаційної безпеки, формування механізму контролю за їхньою діяльністю.

Заслуговує на увагу думка В. Ліпкана, який зазначає, що робота системи забезпечення інформаційної безпеки не може обмежуватися значною кількістю нормативно-правових документів. Це не свідчить про закінченість процесу формування ключових елементів системи забезпечення інформаційної безпеки. У цьому контексті доцільно також враховувати загальну несформованість системи забезпечення національної безпеки, а також невизначеність державної інформаційної політики. До того ж недосконаліть нормативно-правового регулювання досліджуваних процесів негативно впливає і на якість державного управління у вказаній сфері [6].

Таким чином, недоліки нормативно-правової бази, яка врегульовує правові відносини в інформаційній сфері, значно ускладнюють настання якісних змін у цьому секторі суспільних відносин. Сьогодні через відсутність чітко визначених і взаємопов'язаних заходів і теоретичних розробок щодо забезпечення інформаційної безпеки країни виникає низка перешкод на шляху до повноцінної реалізації державою її обов'язку з забезпечення інформаційної безпеки як невід'ємного компонента національної безпеки. Ефективну систему протидії правопорушенням в інформаційній сфері може створити тільки розробка і реалізація обґрунтованої державної політики.

Усі компоненти структури національної безпеки є взаємопов'язаними, проте доцільно зауважити, що деякі види безпеки є не тільки самостійними, а й такими, яким притаманні відповідні виміри в інших напрямах життєдіяльності суспільства. Серед таких інтегративних видів, на думку С. Пирожкова та О. Майбороди, важливе місце посідає інформаційна безпека.

Отже, загрози інформаційного характеру можуть бути спрямовані на різноманітні складники державної безпеки, але їх негативна дія завжди опосередковується завданням

шкоди інформаційній безпеці країни. Наприклад, економічна безпека в сучасних умовах інформаційно-мережевої економіки залежить від безпеки інформаційного характеру, тому що ключовим ресурсом розвитку виробництва в таких обставинах виступає інформаційний продукт [7].

Швидке формування і стрімкий розвиток глобального інформаційного простору, розповсюдженість інформаційно-комунікаційних технологій у всіх сферах життєдіяльності зумовили відповідний розвиток інформаційного суспільства в Україні та виведення на перший план проблем інформаційної безпеки. У таких обставинах одним із ключових напрямів забезпечення інформаційної безпеки держави є створення комплексної системи оцінки загроз інформаційного характеру та відповідного реагування на них [8].

Загрози національній безпеці України в інформаційній сфері можуть бути представлені у вигляді сукупності умов і факторів, які становлять небезпеку життєво необхідним державним, суспільним та особистим інтересам у зв'язку з імовірністю виникнення негативного інформаційного впливу на свідомість та поведінку громадян країни, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру. З огляду на це система загроз інформаційній безпеці може включати такі категорії: загрози безпеці інформації та відповідної інфраструктури; загрози безпеці суб'єктів інформаційного впливу та соціальних зв'язків між ними від дій (або впливів) інформаційного характеру; загрози існуючому і законному порядку реалізації прав та інтересів суб'єктів інформаційної площини [9].

На думку У. Ільницької, сукупність загроз національній безпеці України в інформаційному просторі формується сукупністю ознак. Вона називає такі ознаки: виявлення обмеження свободи слова та доступу громадян до інформації; перекручення, спотворення, блокування, приховування, упереджене та суб'єктивне відображення інформації; протизаконне розповсюдження інформації; відкриті неправдиві інформаційні дані; інформаційне завойовування з боку інших країн та руйнувальне інформаційне вторгнення в державний інформаційний простір, коли держави з більшим інформаційним потенціалом використовують можливість посилити свій вплив через ЗМІ на населення і громадськість менш могутньої країни; створення і функціонування у державному інформаційному просторі неконтрольованих інформаційних потоків; розповсюдження через засоби масової інформації культу насильства, жорстокості; неспішність входження України в інформаційний простір світового масштабу; нерозважливість національної інформаційної політики та відсутність необхідної інфраструктури в інформаційній площині; розповсюдження дезінформації через Інтернет [10].

Р. Хмелевський зазначає, що навіть розгорнуті переліки загроз не можуть бути вичерпними та стабільними. Це пояснюється тим, що джерела загроз можуть бути різноманітними, а саме: людина, технічні засоби, моделі, алгоритми, програмні та технологічні схеми обробки, зовнішнє оточення тощо [11].

Отже, технічний аспект не є центральним у структурі інформаційної безпеки. З урахуванням наведених класифікацій доцільно забезпечувати не тільки безпеку інформаційних даних від знищення, спотворення або блокування, а й загальну інформаційну безпеку суспільства.

Система забезпечення інформаційної безпеки як компонент системи забезпечення державної безпеки характеризується відповідними силами та засобами. У цьому контексті сили доцільно представити як суб'єктний склад системи забезпечення інформаційної безпеки, а засоби – як технології, а також технічні, програмні, лінгвістичні, юридичні, організаційні засоби (зокрема, телекомунікаційні канали, які використовуються для збирання, формування, аналізу, передачі або прийому інформаційних даних щодо стану державної безпеки та застосування заходів, спрямованих на її посилення).

У сучасних умовах розвитку інформаційного суспільства дотримання інформаційної безпеки є функцією кожного з суб'єктів інформаційної сфери. При цьому синергетичні особливості інформаційної безпеки пояснюють наявність певного дуалізму: кожен суб'єкт може одночасно бути об'єктом інформаційної безпеки, а також джерелом імовірних і реальних загроз або каналом їх розповсюдження. Саме тому ефективність забезпечення інформаційної безпеки залежить від можливостей не тільки спеціально призначених для цього державних структур, а й кожного суб'єкта інформаційних відносин щодо свого самозахисту в інформаційній сфері. Водночас держава характеризується особливою позицією серед суб'єктів забезпечення інформаційної безпеки, адже, як зазначає О. Тихомиров, це єдиний суб'єкт, потенціал якого поряд з економічними, політичними та ідеологічними засобами опосередкованого впливу містить можливість прямої управлінської дії, спрямованої на врегулювання інформаційних відносин за допомогою юридичних засобів [12].

З урахуванням положень ст. 17 Конституції України [13] забезпечення інформаційної безпеки віднесене до найважливіших функцій держави нарівні із захистом українського суверенітету та територіальної цілісності. Діяльність держави у цьому напрямі здійснюється через відповідні владні органи. Зокрема, визначено коло суб'єктів, які відповідають за забезпечення державної безпеки та здійснення комплексу інших заходів аналогічного спрямування. До цих суб'єктів належать військові формування та правоохоронні державні органи, зміст і порядок функціонування яких визначені в законодавчому порядку.

Згідно з положеннями ст. 12 Закону України «Про національну безпеку України» сектор національної безпеки і оборони формують чотири таких взаємопов'язаних елементи: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та їх об'єднання, які можуть у добровільному порядку брати участь у забезпеченні безпеки держави. Функції та компетенція елементів сектору безпеки і оборони встановлюються у чинному законодавстві України.

Склад сектору безпеки і оборони формують: Міністерство оборони України, Збройні сили України, Державна спеціальна служба транспорту, Міністерство внутрішніх справ України, Національна гвардія України, Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба України з надзвичайних ситуацій, Служба безпеки України, Управління державної охорони України, Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, органи розвідки, центральний орган виконавчої влади, діяльність якого спрямована на формування та реалізацію державної військово-промислової політики. Інші органи державної влади та органи місцевого самоврядування реалізують власні функції щодо забезпечення безпеки держави у безпосередній взаємодії з органами, які включені до складу сектору безпеки та оборони [14].

Особливості здійснення державою функцій забезпечення інформаційної безпеки полягають у тому, що діяльність кожного державного органу здійснюється шляхом використання інформаційної інфраструктури суспільства, формування та споживання ресурсів інформаційного характеру, встановлення відносин із громадянами. З огляду на це державні органи як власники таких ресурсів і представники відповідної інфраструктури повинні застосовувати спектр заходів, спрямованих на забезпечення збереження ресурсів і безпеки роботи систем інформації, телекомунікації, управління та зв'язку [15].

У Доктрині інформаційної безпеки України (2016 р.) масив функцій, спрямованих на забезпечення безпеки у сфері отримання і використання інформації, покладено на: Раду національної безпеки і оборони України, Кабінет Міністрів

України, відповідні міністерства (зокрема, інформаційної політики, закордонних справ, оборони), Службу безпеки та Державну службу спеціального зв'язку та захисту інформації України, а також органи розвідки [16].

В. Ліпкан доводить, що з урахуванням функціональності суб'єктів система забезпечення інформаційної безпеки формується зі стратегічного, тактичного та оперативного рівнів управління безпекою. До суб'єктів вищого, стратегічного рівня дослідник відносить Раду національної безпеки і оборони України та Кабінет Міністрів України. Суб'єктами нижчого, тактичного рівня виступають центральні органи виконавчої влади. На оперативному рівні розташовані місцеві органи виконавчої влади [17]. Погоджуючись з В. Ліпканом, зазначимо, що з трирівневої системи «випадають» Служба безпеки України та органи розвідки.

Результати дослідження генезису нормативно-правового регулювання організаційних і практичних заходів із забезпечення інформаційної безпеки України дають підстави вважати, що в сучасних умовах інформаційного протистояння національний інформаційний простір України залишається недостатньо захищеним від негативних інформаційно-психологічних впливів і загроз внутрішнього і зовнішнього характеру [18; 19; 20], тому захист інформаційного суверенітету, формування потужної та результативної системи інформаційної безпеки нашої країни, розробка та впровадження ефективних стратегій і тактик протидії інформаційним загрозам повинні бути пріоритетними завданнями органів державної влади та недержавних інститутів.

Загрози національній безпеці України в інформаційній сфері можуть бути представлені у вигляді сукупності умов і факторів, які становлять небезпеку життєво важливим державним, суспільним та особистісним інтересам у зв'язку з імовірністю виникнення негативного інформаційного впливу на свідомість і поведінку громадян країни, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру. Аналіз наявних класифікацій загроз інформаційній безпеці України свідчить про відсутність єдиного підходу до виділення їх окремих видів, адже кожен з дослідників може застосовувати певні суб'єктивні критерії, тому їх перелік досить складно зробити вичерпним.

Серед суб'єктів забезпечення інформаційної безпеки України доцільно виокремлювати спеціально уповноважені державні органи, для яких забезпечення безпеки є одним із ключових завдань діяльності, та суб'єктів, які можуть брати участь у її забезпеченні.

ЛІТЕРАТУРА

1. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса : Юридична література, 2007. 471 с.
2. Почепцов Г. Сучасні інформаційні війни. Київ : Видавничий дім «Києво-Могилянська академія», 2015. 497 с.
3. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України : дис. … канд. юрид. наук : 12.00.01. Київ, 2007. 186 с.
4. Новицька Н.Б. Правове забезпечення інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави*. 2009. № 1. С. 44–47.
5. Прозоров А.Ю. Ціннісні основи інформаційної безпеки особи, суспільства та держави. *Інформаційна безпека людини, суспільства, держави*. 2016. № 1 (20). С. 29–37.
6. Ліпкан В.А., Макименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. Київ : КНТ, 2006. 280 с.
7. Цивілізаційний вибір України: парадигма осмислення і стратегія дії : національна доповідь / ред. кол. : С. Пирожков, О. Майборода, Ю. Шайгородський та ін. ; Інститут політичних і етнонаціональних досліджень ім. І.Ф. Кураса НАН України. Київ : НАН України, 2016. 284 с.
8. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р., введене в дію Указом Президента від 1 травня 2014 р. № 449/2014. URL: http://www.zakon5.rada.gov.ua/laws/show/n0004525-14 (дата звернення: 02.11.2021).
9. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. URL: http://www.justinian.com.ua/article.php?id=3222 (дата звернення: 07.11.2021).
10. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. 2016. № 2–1. С. 27–32.
11. Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. *Сучасний захист інформації*. 2016. № 4. С. 65–70.
12. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави : монографія / заг. ред. Р.А. Калюжний. Київ : Центр навчально-наукових та науково-практичних видань Національної академії СБ України, 2014. 196 с.
13. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 03.11.2021).
14. Про основи національної безпеки України : Закон України від 19 червня 2003 р. № 964-IV. URL: http://uadocs.exdat.com/docs/index-208817.html (дата звернення: 02.11.2021).
15. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства. *Науковий вісник Ужгородського національного університету. Серія «Право»*. Випуск 43. Том 1. 2017. С. 34–39.
16. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 р. № 47/2017. URL: http://www.zakon3.rada.gov.ua/laws/show/514/2009 (дата звернення: 01.11.2021).
17. Ліпкан В.А. Національна безпека України : навчальний посібник. Київ : Кондор, 2009. 280 с.
18. Черниш Р.Ф. Організаційні та правові методи протидії маніпулюванню свідомістю громадян у соціальних мережах. *Вісник кримінального судочинства*. 2020. № 3–4. С. 168–177. URL: https://doi.org/10.17721/2413–5372.2020.3–4/168–177.
19. Formation and application of communication strategies through social networks: legal and organizational aspects / R.F. Chernysh, V.L. Pogrebnaya, I.I. Montrin, T.V. Koval, O.S. Paramonova. *International Journal of Management*. Volume 11. Issue 06. June 2020. P. 476–488. Article ID: IJM_11_06_041. URL: http://www.iaeme.com/ijm/issues.asp?JType=IJM&VType=11&IType=6. DOI: 10.34218/IJM.11.6.2020.041.
20. Development of Internet communication and social networking in modern conditions: institutional and legal aspects / R.F. Chernysh, V.L. Pogrebnaya, I.I. Montrin, T.V. Koval, O.S. Paramonova. *Revista San Gregorio* (special issues Nov). URL: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1572.