УДК 343.301
DOI:10.24144/2078-1431.2021.1(26).60-69

Денис Олейніков,
кандидат юридичних наук,
начальник відділу наукової та науково-дослідної роботи ІПЮК для СБУ
НЮУ ім. Ярослава Мудрого

ЗМІСТ ТА СКЛАДОВІ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ ЯК ОБ'ЄКТА КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ

Статтю присвячено науковому аналізу змісту та складових інформаційного суверенітету держави як сукупності суспільних відносин в інформаційній сфері, а також окремих аспектів його кримінально-правової охорони. В результаті здійсненого огляду наукових поглядів на визначення і зміст інформаційного суверенітету та окремих його складових, а також окремих міжнародних нормативно-правових актів отримано висновки щодо необхідності посилення уваги до інформаційного суверенітету як об'єкта забезпечення та охорони, у тому числі кримінально-правової. Аналізом окремих кримінально-правових норм, якими передбачається кримінальна відповідальність за суспільно небезпечні дії, що посягають на інформаційний суверенітет, визначено його складові – внутрішня та зовнішня. Наголошено на необхідності принаймні наукового групування окремих складів, розміщених у різних розділах Особливої частини КК України, в єдиний інститут злочинів, які посягають на інформаційний суверенітет України (чи інформаційну безпеку), що є необхідним у контексті формування дієвого та злагодженого механізму захисту інтересів держави в інформаційній сфері.

Ключові слова: *інформаційний суверенітет, об'єкт кримінально-правового захисту, об'єкт злочину.*

The work is devoted to the scientific analysis of the content and components of the information sovereignty of the state as a set of public relations in the information sphere, as well as some aspects of its criminal law protection. As a result of the review of scientific views on the definition and content of information sovereignty and its individual components, as well as certain international regulations, conclusions were obtained on the need to increase attention to information sovereignty as an object of security and protection, including criminal law. The analysis of certain criminal law norms, which provide for criminal liability for socially dangerous actions that encroach on information sovereignty, identifies its components - internal and external. Emphasis is placed on the need for at least scientific grouping of individual structures located in different sections of the Special Part of the Criminal Code of Ukraine into a single institution of crimes that encroach on Ukraine's information sovereignty (or information security), which is necessary in the context of forming an effective and coordinated mechanism of protection interests of the state in the information sphere.

Key words: *information sovereignty, object of criminal law protection, object of crime.*

Постановка проблеми. Процеси глобалізації та інтенсифікація інформаційних потоків у межах кожної держави створюють, з одного боку, умови для розвитку інформаційного суспільства та інтеграції в світову спільноту, та, з іншого боку, підвищують деструктивний вплив на внутрішні процеси самоідентифікації та регулювання державою інформаційної політики в суспільстві. Останнє може використовуватись з метою руйнування чи ослаблення самостійності та незалежності будь-якої держави в інформаційній сфері. Виокремлення науковим аналізом такої діяльності та початок формування ефективної системи протидії та захисту від її негативного впливу наразі є одним з пріоритетних завдань на шляху забезпечення національної безпеки в цілому та інформаційної безпеки зокрема. Вирішення цього завдання багато в чому залежить від усвідомлення місця інформаційного суверенітету в системі об'єктів кримінально-правової охорони.

Результати аналізу наукових публікацій. У науковій літературі питанням забезпечення інформаційного суверенітету присвячені наукові праці О. Баранова, В. Горового, О. Довганя, Д. Дубова, М. Ожевана, О. Олійника, В. Пилипчука, О. Солодкої, О. Сосніна, В. Супруна, Л. Шиманського та інших фахівців. Їх теоретичні та практичні здобутки, безперечно, є вагомим внеском у розвиток вчення про інформаційний суверенітет та його забезпечення в різних галузях права. Разом з цим, досвід правозастосовної діяльності свідчить про відсутність послідовного та системного розроблення концепції суверенітету держави в інформаційній сфері як об'єкта кримінально-правової охорони.

Метою статті є теоретичний аналіз інформаційного суверенітету держави в контексті належності до об'єктів кримінально-правової охорони, а також характеристика його змісту та складових як сукупності суспільних інтересів, яким завдається шкода відповідними видами суспільно небезпечних дій.

Виклад основного матеріалу. В контексті аналізу діяльності, спрямованої на підрив інформаційної незалежності держави, Є.М. Мануілов та Ю.Ю. Калиновський вказують на руйнівні сили, як зовнішні, так і внутрішні, які намагаються зруйнувати моральні основи життя української нації, маніпулюють громадською думкою та формують антидержавні ідеї серед громадян. При цьому загрози та виклики моральному життю українського суспільства впливають на інформаційний суверенітет України [1, с. 29]. Цілком очевидно, що потреба в створенні дієвої системи інформаційного протистояння може бути реалізована у тому числі через впровадження кримінальної відповідальності за окремі види суспільно небезпечної діяльності, яка завдає шкоди інформаційному суверенітету. Зокрема, окремими міжнародними нормативно-правовими актами закладено підвалини досягнення цієї мети. Так, держави-члени Шанхайської організації співробітництва уклали угоду про співробітництво у сфері забезпечення міжнародної організаційної безпеки. При цьому основними загрозами у сфері забезпечення міжнародної інформаційної безпеки визначені: 1) розробка й застосування інформаційної зброї, підготовка й ведення інформа-

ційної війни; 2) інформаційний тероризм; 3) інформаційна злочинність; 4) використання домінуючого становища в інформаційному просторі на шкоду інтересам і безпеці інших держав; 5) поширення інформації, що завдає шкоди суспільно-політичній та соціально-економічній системам, духовному, моральному й культурному середовищу інших держав; 6) загрози природного та/чи техногенного характеру безпечному, стабільному функціонуванню глобальних та національних інформаційних інфраструктур.

Конвенцією про забезпечення міжнародної інформаційної безпеки (концепція) на міжнародному рівні були закріплені такі зобов'язання держав:

– докладати зусиль з криміналізації використання інформаційних ресурсів та (чи) впливу на них в інформаційному просторі з протиправними цілями, до яких у тому числі належать неправомірне розповсюдження інформації, порушення конфіденційності, цілісності та доступності інформації, а також вживати законодавчих й інших заходів, що є необхідними для встановлення та застосування відповідальності осіб, які вчинили замах, співучасть чи підбурювання до вчинення чи вчинили криміналізовані соціально небезпечні дії в інформаційному просторі;
– вживати законодавчих й інших заходів, що є необхідними для того, щоб до осіб, які вчинили правопорушення в інформаційному просторі, застосовувались ефективні, співрозмірні та переконливі міри покарання [2].

Згадані вище документи та організаційні задуми щодо подальшої реалізації окремих стратегій дозволяють зробити висновок про необхідність активізації окремих елементів безпекової динаміки, у тому числі шляхом формування організаційних та правових засад протидії основним загрозам у сфері інформаційної безпеки держави. Тим більше, що потреба в цих діях виникла вже давно та загострилась, як мінімум, напередодні подій, пов'язаних із російською збройною агресією в АР Крим та окремих територіях Донецької та Луганської областей.

У Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 25 лютого 2017 року № 47/2017, наголошується, що застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України. При цьому зазначається, що комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [3]. Окрім того, до пріоритетів державної політики в інформаційній сфері, окрім іншого, віднесено:

– посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу Збройних сил України та інших військових формувань, загострення суспільно- політичної ситуації;
– виявлення та притягнення до відповідальності згідно із законодавством суб'єктів українського інформаційного простору, що створені та/або використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;
– унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни, національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення.

Наведені вище заходи нами було обрано навмисно, щоб продемонструвати відносно відокремлений сегмент ресурсів держави в інформаційній сфері, який стосується саме захисту окремих інтересів, пов'язаних з основами національної безпеки. Іншими словами, прогностичні методи аналізу уразливості окремих об'єктів кримінально-правової охорони дозволили виділити відносно самостійну складову державної безпеки, на завдання шкоди якій спрямований розвідувально-підривний інформаційний вплив держави-агресора. Цю складову ми визначаємо як суверенітет держави в інформаційній сфері, ураження якого, на думку військових та політичних аналітиків РФ, у перспективі призведе до суттєвого ослаблення конституційного ладу України та розшарування суспільства з подальшою сепаратизацією за мовною, національною, етнічною чи іншими ознаками.

Цілком логічно припустити, що, оскільки тактичні та стратегічні зусилля ворога спрямовані на цьому напрямі, відповідно заходи щодо його охорони, захисту та забезпечення є недостатніми. І окремі законодавчі ініціативи, організаційно-правові заходи на рівні держави та формування стратегій забезпечення безпеки в тих або інших сферах є тому підтвердженням. Враховуючи, що питання кримінально-правового забезпечення суверенітету держави в інформаційній сфері є надзвичайно важливими, зауважимо, що послідовне та чітке впровадження кримінальної відповідальності за вчинення суспільно небезпечних діянь, які на нього посягають, неможливе без визначення місця інформаційного суверенітету серед об'єктів кримінально- правової охорониу та аналізу його основних ознак. При цьому необхідно враховувати, що, обираючи об'єкти кримінально-правової охорони і встановлюючи кримінально-правові заборони, законодавець повинен враховувати, перш за все, соціальну обумовленість правового припису, цінність окремих суспільних відносин, їх роль та значення для всієї системи суспільних відносин [4, с. 171].

Єдина легальна дефініція інформаційного суверенітету міститься у ст. 1 Закону України «Про Національну програму інформатизації», де він визначається як «здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави». Натомість у науці кримінального права вироблено низку наукових поглядів на визначення та зміст інформаційного суверенітету.

Так, О. Олійник, О. Соснін та Л. Шиманський визначають інформаційний суверенітет Української держави як виключне право України відповідно до Конституції, законодавства України та норм міжнародного права самостійно і незалежно з додержанням балансу інтересів особи, суспільства і держави визначати й здійснювати внутрішні та геополітичні національні інтереси в інформаційній сфері, державну внутрішню і зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку держави [5]. Розглядаючи інформаційний суверенітет дещо під іншим кутом зору, В.М. Супрун визначає його як стан самостійності формування певних ресурсів даних, створених у результаті здійснення державою своєї свободи, за рахунок держави або суб'єктів держави, внаслідок реалізації права на інформацію, що забезпечує рівність її у міжнародному інформаційному просторі, які вказують на її авторську належність державі, органам влади, органам місцевого самоврядування. До ознак інформаційного суверенітету, на його думку, належать пріоритетність держави в інформаційних відносинах, самостійність, рівноправ'я у зовнішніх відносинах, незалежність у зовнішніх відносинах, невідчужуваність [6, с. 5; 75].

Цитований науковець також зауважує, що забезпечення державою інформаційного суверенітету передбачає такі чинники: 1) реалізація інформаційного суверенітету можлива лише за наявності повноцінного права на інформацію у всіх суб'єктів інформаційних соціальних відносин; 2) реалізація державою інформаційного суверенітету включає забезпечення її інформаційної безпеки; 3) реалізація інформаційного суверенітету повинна ґрунтуватися на основі інформаційної свободи та рівноправності [7, с. 39]. На думку О.М. Солодкої, інформаційний суверенітет – це властивість державної влади, що полягає у її верховенстві, самостійності, повноті і неподільності в інформаційному просторі України та рівноправності і незалежності у відносинах з іншими державами у глобальному інформаційному просторі [8, с. 83].

Як видно, в науці наразі відсутня єдність поглядів на сутність інформаційного суверенітету, що обумовлює необхідність його визначення через усталені визначення суверенітету держави в цілому. Ключовим у цьому питанні є положення Декларації про державний суверенітет України, яка визначає його як верховенство, самостійність, повноту і неподільність влади Республіки в межах її території та незалежність і рівноправність у зовнішніх зносинах. Таким чином, суверенітет має 2 складові: внутріш-

ню та зовнішню, які характеризують дещо різні форми його вираження. Внутрішня характеризує «верховенство, самостійність, повноту і неподільність влади» в межах території України, а зовнішня – незалежність у зносинах з зовнішніми суб'єктами. Отже, одразу зауважимо, що визначення інформаційного суверенітету держави, яке міститься в ст. 1 Закону України «Про Національну програму інформатизації», враховує винятково його зовнішню складову.

Проте необхідно навести також приклади реалізації державою внутрішньої складової інформаційного суверенітету. Так, відповідно до ст. 1 Закону України «Про державну таємницю», державна таємниця - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою. Стаття 18 вказаного Закону передбачає основні організаційно-правові заходи щодо охорони державної таємниці, а ст. 39 - відповідальність за порушення законодавства про державну таємницю. Наведені норми встановлюють механізм реалізації державної влади у сфері захисту чутливої інформації в межах держави. Що ж стосується тих саме відносин, до яких є дотичним іноземний суб'єкт, то в контексті кримінально- правової охорони необхідно згадати положення ст. 114 КК України, що передбачає кримінальну відповідальність за передачу або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства. Аналогічно, ст. 330 КК України передбачає кримінальну відповідальність за передачу або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства.

На міжнародному рівні також встановлені окремі механізми реалізації інформаційного суверенітету держави. Так, Європейська конвенція «Про інформацію щодо іноземного законодавства» від 7 червня 1968 року визначає основні засади взаємодії держав, що підписали Конвенцію, у сфері надання інформації і зобов'язалися надавати одна одній, відповідно до положень цієї Конвенції, інформацію щодо свого законодавства і процедур у цивільній та комерційній сферах, а також щодо їхньої судової організації. Статтею 11 Конвенції встановлюються винятки у наданні інформації: «Держава, до якої звернено запит, може відмовитись вжити заходів із запиту про інформацію, коли її інтереси зачіпаються справою, із якої виникає запит, або коли вона вважає, що відповідь може завдати шкоди її суверенітету або безпеці» [9].

Незважаючи на відносну нерозробленість теми інформаційного суверенітету держави, як було вказано вище, КК України передбачає відпові-

дальність за окремі види суспільно небезпечних дій, які тим або іншим чином посягають на інформаційний суверенітет України, як на внутрішню, так і на зовнішню його складові. Отже, інформаційний суверенітет є одним із об'єктів кримінально-правової охорони, хоча жодного разу не згадується за текстом КК України. Натомість ч. 1 ст. 1 КК України до завдань Кримінального кодексу України відносить правове забезпечення охорони прав і свобод людини і громадянина, власності, громадського порядку та громадської безпеки, довкілля, конституційного устрою України від кримінально- протиправних посягань, забезпечення миру і безпеки людства, а також запобігання кримінальним правопорушенням.

Відповідно суспільні інтереси у сфері інформаційного суверенітету держави, яким завдається шкода, поглинаються більш широкими категоріями, зазначеними вище, та входять до їх змісту. Досить характерним прикладом такої ситуації є норми, які передбачають кримінальну відповідальність за публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій (ч. 2 ст. 109 КК України) та публічні заклики чи розповсюдження матеріалів із закликами до вчинення умисних дій з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України (ч. 1 ст. 110 КК України). Цілком очевидно, що вказаними діями завдається шкода суспільним відносинам у сфері інформаційного суверенітету держави, а саме – його внутрішній складовій. Проте законодавцем вказані норми поміщені до Розділу I Особливої частини КК України «Злочини проти основ національної безпеки України», що свідчить про ототожнення суспільних відносин у сфері інформаційного суверенітету з окремими суспільними відносинами у сфері національної безпеки України (яка є значно ширшою за змістом та співвідноситься з інформаційним суверенітетом як ціле та складова).

Разом з цим кримінальне право не є статичним, оскільки в такому разі воно б втратило свою дієвість та функціональність. Нові загрози та нові виклики, які спрямовані на найбільш уразливі чи найменш захищені об'єкти, обумовлюють зміни та нововведення в чинну нормативну матерію.

Вказану особливість висвітлює О.В. Тихонова, зазначаючи, що «… поняття об'єкта кримінально-правової охорони є первинним щодо поняття «об'єкт злочину», адже насамперед кримінальний закон бере під свою охорону відповідні відносини, і лише згодом вони перетворюються на об'єкт злочину (у разі злочинного посягання на них), або можуть не стати ним узагалі (у разі їх порушення діяннями з боку неосудних або малолітніх), але все ж таки перебувають під охороною кримінального закону». Продовжуючи свою думку, вона стверджує, що існування об'єкта кримінально-правової охорони є обов'язковою передумовою визнання порушених відносин об'єктом злочину. Тобто об'єкт кримінально-правової охорони є первинним стосовно об'єкта злочину та змістовно ширше, ніж об'єкт злочину [10, с. 249]. Отже, враховуючи наявність норм, що передбачають кримінальну відповідальність за вчинення суспільно небезпечних

дій, які завдають шкоди інформаційному суверенітету, доходимо висновку, що він вже є об'єктом кримінально-правової охорони. Зазначена обставина вказує на існування передумов до визнання суспільних відносин у сфері інформаційного суверенітету держави, яким злочинним діянням завдається шкода, об'єктом злочину.

Висновки. Підсумовуючи результати наукового аналізу заявленої тематики, необхідно зупинитись на кількох висновках, які мають принципове значення. Так, по-перше, наука кримінального права не виробила єдиної позиції щодо визначення інформаційного суверенітету держави. Існує низка наукових думок та підходів, які мають як спільні погляди, так і певні розбіжності. Не вирішуючи в цілому цю проблему, вважаємо, що за основу необхідно взяти визначення державного суверенітету, наведене в Декларації про державний суверенітет України, доповнивши його обмежувальною ознакою щодо інформаційного простору його реалізації. Так, на нашу думку, суверенітет держави в інформаційній сфері (інформаційний суверенітет) характеризує верховенство, самостійність, повноту і неподільність влади України в межах її інформаційного простору та незалежність і рівноправність у зовнішніх зносинах, пов'язаних із реалізацією інтересів в інформаційній сфері. При цьому інформаційний суверенітет є складовою державного суверенітету та, у свою чергу, містить 2 складові – внутрішню та зовнішню.

По-друге, навіть поверховий аналіз окремих складів злочинів, передбачених Особливою частиною КК України, вказує на те, що інформаційний суверенітет держави та обидві його складові вже давно є об'єктами кримінально-правової охорони, проте в науці кримінального права поки що відсутні ґрунтовні наукові праці з цих питань. Зазначене обумовлює доцільність більш предметних наукових розвідок у частині кримінально-правової охорони інформаційного суверенітету держави як складової державного суверенітету та принаймні наукового групування окремих складів, розміщених у різних розділах Особливої частини КК України, в єдиний інститут злочинів, які посягають на інформаційний суверенітет України (чи інформаційну безпеку). Ці кроки є необхідними в контексті формування дієвого та злагодженого механізму захисту інтересів держави в інформаційній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Manuilov E. M. Information sovereignty of Ukraine: modern moral challenges and threats / E. M. Manuilov, Y. Y. Kalynovsky // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія : Філософія. 2019. № 3. С. 22-33.
2. Конвенция об обеспечении международной информационной безопасности (концепция) от 22.09.11. URL: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.
3. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374.

4. Коржанский Н.И. Объект и предмет уголовно-правовой охраны. М.: Юридическая литература, 1980. 248 с.
5. Олійник О. В., Соснін О. В., Шиманський Л. Є. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави. URL: niss.gov. ua/book/Sosnin_2.htm.
6. Супрун В. М. Теоретико-правові основи інформаційного суверенітету : дис. канд. юрид. наук : 12.00.01. Х., 2010. 212 с.
7. Супрун В. М. Інформаційний суверенітет як один з елементів інформаційної безпеки держави: теоретико-правовий аспект // Вісник Харківського національного університету ім. В. Н. Каразіна. Серія: Право. 2009. № 841. С. 136 – 139.
8. Солодка О.М. Забезпечення інформаційного суверенітету держави: правовий дискурс // Інформація і право. 2020. № 1(32). С. 80-87.
9. Європейська конвенція про інформацію щодо іноземного законодавства від 7 червня 1968 р. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.
10. Тихонова О. В. Об'єкт кримінально-правової охорони та об'єкт злочину: співвідношення понять // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. 2014. Вип. 2. С. 244-251.

REFERENCES

1. Manuilov, E. M. (2019). Information sovereignty of Ukraine: modern moral challenges and threats. *Visnyk Natsional'noho universytetu «Yurydychna akademiya Ukrayiny imeni Yaroslava Mudroho - Bulletin of the National University "Yaroslav the Wise Law Academy of Ukraine, 3*, 22-33 [in English].
2. Konventsiya ob obespechenii mezhdunarodnoy informatsionnoy bezopasnosti (kontseptsiya) ot 22.09.11. [Convention on ensuring international information security (concept) of 22.09.11.] (n.d.). *www.mid.ru/foreign_policy.* Retrieved from https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 [in Russian].
3. Doktryna informatsiynoyi bezpeky Ukrayiny, zatverdzhena Ukazom Prezydenta Ukrayiny vid 25 lyutoho 2017 roku № 47/2017 [Doctrine of information security of Ukraine, approved by the Decree of the President of Ukraine of February 25, 2017 № 47/2017]. (n.d.). *www.president.gov.ua.* Retrieved from https://www.president.gov.ua/documents/472017-21374 [in Ukrainian].
4. Korzhanskiy, N.I. (1980). *Ob»yekt i predmet ugolovno-pravovoy okhrany [Object and subject of criminal law protection].* M.: Yuridicheskaya literature [in Russian].
5. Oliynyk, O. V., Sosnin, O. V., & Shymans'kyy, L. YE. Polityko-pravovi aspekty formuvannya informatsiynoho suspil'stva suverennoyi i nezalezhnoyi derzhavy [Political and legal aspects of the formation of the information society of a sovereign and independent state]. (n.d.). *niss. gov. ua*. Retrieved from niss. gov. ua/book/Sosnin_2.htm [in Ukrainian].
6. Suprun, V. M. (2012). Teoretyko-pravovi osnovy informatsiynoho suverenitetu [Theoretical and legal foundations of information sovereignty]. *Candidate's thesis.* Kharkiv [in Ukrainian].
7. Suprun, V. M. (2009). Informatsiynyy suverenitet yak odyn z elementiv informatsiynoyi bezpeky derzhavy: teoretyko-pravovyy aspekt [Information sovereignty as one of the elements of information security of the state: theoretical and legal aspect]. *Visnyk Kharkivs'koho natsional'noho universytetu im. V. N. Karazina - Bulletin of Kharkiv National University. VN Karazin, 841,* 136 – 139 [in Ukrainian].
8. Solodka, O.M. (2020). Zabezpechennya informatsiynoho suverenitetu derzhavy: pravovyy dyskurs [Ensuring the information sovereignty of the state: legal discourse]. *Informatsiya i pravo - Information and law, 1(32),* 80-87 [in Ukrainian].

9. Yevropeys'ka konventsiya pro informatsiyu shchodo inozemnoho zakonodavstva vid 7 chervnya 1968 r. [European Convention on Information on Foreign Law of June 7, 1968]. (n.d.). *zakon1.rada.gov.ua.* Retrieved from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. [in Ukrainian].
10. Tykhonova, O. V. (2014). Ob''yekt kryminal'no-pravovoyi okhorony ta ob''yekt zlochynu: spivvidnoshennya ponyat' [Object of criminal-legal protection and object of crime: correlation of concepts]. *Naukovyy visnyk L'vivs'koho derzhavnoho universytetu vnutrishnikh sprav. Ceriya yurydychna - Scientific herald of the Lviv state university of internal affairs. The series is legal, 2,* 244-251 [in Ukrainian].