DOI: 10.33663/1563-3349-2023-34-496-507
УДК 343.2+340.13+007.51+165.12

В. Н. КУБАЛЬСЬКИЙ,
*кандидат юридичних наук, доцент**
ORCID: 0000-0001-6127-5786

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ДЕРЖАВНОГО СУВЕРЕНІТЕТУ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

У статті досліджується зміст поняття «державний суверенітет в інформаційній сфері» (інформаційний суверенітет), пропонується його авторське визначення. Проаналізовано особливості загроз державному суверенітету України в інформаційній сфері в умовах збройної агресії РФ. Державний суверенітет в інформаційній сфері розглядається як об'єкт кримінально-правової охорони. Визначено систему норм Особливої частини КК, які передбачають кримінальну відповідальність за посягання на державний суверенітет України в інформаційній сфері.

Ключові слова: *державний суверенітет в інформаційній сфері (інформаційний суверенітет), збройна агресія РФ, кримінально-правова охорона, інформаційна безпека.*

Kubalskiy Vladyslav. **Criminal legal protection of state sovereignty of Ukraine in the information sphere**

The article examines the content of the concept of «state sovereignty in the information sphere» (information sovereignty), and offers the author's own definition. The peculiarities of threats to state sovereignty of Ukraine in the information sphere in the context of Russia's armed aggression are analyzed. The state sovereignty in the information sphere is considered as an object of criminal law protection. The author defines the system of provisions of the Special Part of the Criminal code that provide for criminal liability for encroachment on the State sovereignty of Ukraine in the information sphere.

Key words: *state sovereignty in the information sphere (information sovereignty), armed aggression of the russian federation, criminal law protection, information security.*

Вступ. В умовах триваючої збройної агресії РФ проти України та процесів глобалізації в інформаційній сфері особлива увага вчених-правознавців привернена до вирішення проблем кримінально-правової охорони державного суверенітету України в інформаційній сфері. У Стратегії інформаційної безпеки, яка затверджена Указом Президента України від 28 грудня 2021 р., вказується, що «тривалий час спеціальні служби Російської Федерації прово-

* ***Kubalskiy Vladyslav****, Candidate of Juridical Sciences (Ph. D.), Docent*

дять свої спеціальні інформаційні операції, більшість із яких спрямовані на підрив національної безпеки України, її національних інтересів, ліквідацію української державності та знищення української ідентичності, провокування проявів екстремізму, панічних настроїв у суспільстві, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні»[1].

Вчені-юристи ще 2019 р. звертали увагу на те, що «саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної та релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України»[2].

На засіданні круглого столу на тему «Гібридна (інформаційна) війна РФ. Відповіді України» (2021 р.) на той час заступник начальника департаменту контррозвідувального захисту в сфері інформаційної безпеки СБУ Юлія Лапутіна у доповіді повідомила, що «вперше зібрано та проаналізовано факти, які свідчать про застосування Російською Федерацією проти України не лише фізичних агресивних дій, але і завчасно спланованої інформаційної війни, яка сприяла вирішенню військових цілей Російською Федерацією на шкоду безпеці, суверенітету та територіальній цілісності України»[3]. Отже, держава потребує забезпечення належної охорони засобами кримінального права державного суверенітету в інформаційній сфері.

Стан дослідження. Дослідженню різноманітних аспектів державного суверенітету в інформаційній сфері присвячені наукові праці українських та іноземних вчених – І. Арістова, О. Баранова, Д. Бєлих, І. Боднар, В. Брижка, В. Гапотія, В. Гонг, В. Горового, О. Задерейка, І. Дороніна, О. Джураєва, О. Джус, О. Довганя, Д. Дубова, К. Ісмайлова, В. Ковтуна, Б. Кормича, А. Майснера, М. Ожевана, О. Олійника, О. Солодкої, Н. Пархоменко, С. Пауерс, Н. Пічука, В. Пилипчука, А. Письменицького, В. Попика, В. Супруна, А. Селіванова, І. Слюсарчука, Є. Стрельцова, Д. Севрюкова, О. Скрипнюка, В. Тернавської, Т. Ткачука, О. Троянського, Л. Рябовол, Р. Чанишева, О. Яреми та багатьох інших. Окремим проблемам кримінально-правової охорони державного суверенітету України в інформаційній сфері присвячені наукові праці Д. Олєйнікова, О. Радутного, Н. Савінової. Проведені дослідження характеризуються плюралістичним розумінням змісту державного суверенітету в інформаційній сфері. При цьому необхідно констатувати, що серед вчених-юристів поки що не склалося єдиного підходу до розуміння змісту державного суверенітету в інформаційній сфері.

Постановка проблеми. Пріоритетним завданням у сучасних умовах є насамперед протидія руйнівному інформаційному впливу РФ на державний суверенітет України в умовах розв'язаної нею повномасштабної агресивної війни. Як підкреслює Д. В. Дубов, «для України ця проблема постає з особливою силою, зважаючи на системні спроби зовнішніх авторів впливати на суверенітет української держави за всіма напрямами, в тому числі за інфор-

маційним. І ключовим тут стає відповідність чинного законодавства відповідним викликам інформаційному суверенітету»[4].

Слушною є думка українських вчених-юристів про те, що незабезпечення суверенітету держави в інформаційній сфері може призвести до втрати суверенітету взагалі[5]. Тож навряд чи в умовах повномасштабної збройної агресії РФ можуть виникати сумніви щодо необхідності удосконалення та посилення кримінально-правової охорони державного суверенітету в інформаційній сфері.

Метою дослідження є визначення системи норм, які передбачають кримінальну відповідальність за посягання на державний суверенітет України в інформаційній сфері.

Виклад основного матеріалу. У 2022 р. після повномасштабного вторгнення РФ в Україну ухвалені закони, спрямовані передусім на посилення кримінально-правової охорони державного суверенітету в інформаційній сфері – «Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність», «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції», «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану», «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану», «Про внесення змін до статті 114^2 Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації» та ін.

Зазначені закони передбачають, зокрема, доповнення Кримінального кодексу України (далі – КК України) низкою норм, які передбачають відповідальність за посягання на державний суверенітет в інформаційній сфері. Ці новели спрямовані, зокрема, на протидію: 1) ідеологічному і культурно-освітньому колабораціонізму у формі здійснення пропагандистської та іншої інформаційної діяльності (ст. 111^1 КК); 2) несанкціонованому поширенню військово значущої інформації (ст. 114^2 КК); 3) ворожій пропаганді, виготовленню та поширенню забороненої інформаційної продукції (ст. 436^2 КК).

Закон України «Про національну програму інформатизації» від 4 лютого 1998 р. (втратив чинність 01.03.2023) у ст. 1 запровадив поняття «інформаційний суверенітет держави» 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[6]. Наведене визначення відображало лише один аспект інформаційного

суверенітету. У контексті аналізу цього питання необхідно уточнити, що в нещодавно схваленому Законі України «Про національну програму інформатизації» від 1 грудня 2022 р. вже не вживається зазначене поняття.

Закон України «Про науково-технічну інформацію» 1993 р. містить ст. 23 «Забезпечення суверенітету України у сфері науково-технічної інформації». Поняття «інформаційний суверенітет» використовується в Законі України «Про систему іномовлення України» 2015 р. і документах, присвячених регулюванню питань інформаційної безпеки. Зокрема, у Стратегії інформаційної безпеки, яка затверджена Указом Президента України від 28 грудня 2021 р., зазначається, що «Кабінет Міністрів України забезпечує формування та реалізацію інформаційної політики держави, забезпечує інформаційний суверенітет…»[7]. До стратегічних цілей цієї Стратегії належить, зокрема, «протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави…». У Стратегії також визначено, що «досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України…»[8].

Незважаючи на наявність численних спроб законодавчо чи доктринально визначити, що таке державний суверенітет в інформаційній сфері (інформаційний суверенітет), у вітчизняній доктрині достатньо довго триває наукова дискусія щодо доцільності використання поняття «інформаційний суверенітет» у законодавстві та доктрині. Низка українських вчених-юристів (О. А. Баранов, Б. А. Кормич, О. В. Олійник, А. В. Пазюк та ін.) висловлюють доволі вагомі доводи проти використання категорії «інформаційний суверенітет», з якими в цілому варто погодитися. Більш доцільно, на нашу думку, використовувати поняття «державний суверенітет в інформаційній сфері», хоча і в юридичній літературі іноді використовується поняття «державний суверенітет в інформаційному просторі». У цьому контексті погоджуємося з підходом А. В. Пазюка про спрямованість державної влади в інформаційній сфері на власну територію, яка проявляється у повноваженнях держави самостійно регулювати, управляти та контролювати діяльність, пов'язану з передачею інформації в межах своєї юрисдикції[9]. При цьому зазначений вчений слушно звертає увагу на те, що «така сутнісна ознака, як «територіальність» дії державного суверенітету, не співвідноситься з екстериторіальністю інформаційних потоків»[10].

Українські вчені-юристи запропонували низку визначень інформаційного суверенітету, при формулюванні яких спираються переважно на поняття державного суверенітету, наведене в Декларації про державний суверенітет України, доповнивши його обмежувальною ознакою щодо інформаційного простору його реалізації. Так, на думку Д. О. Олєйнікова, суверенітет держа-

ви 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[11]. О. Е. Радутний пропонує під інформаційним суверенітетом України розуміти верховенство та незалежність держави в інформаційній справі, її здатність у відповідності до прав і свобод людини та громадянина контролювати і регулювати потоки інформації з-поза меж держави та всередині неї, спроможність ефективно протидіяти зовнішнім і внутрішнім інформаційним загрозам[12].

О. В. Олійник на підставі проведеного дисертаційного дослідження запропонував таке визначення: інформаційний суверенітет – це виключне право України самостійно і незалежно визначати внутрішні і геополітичні інтереси в інформаційній сфері, державну внутрішню і зовнішню інформаційну політику та здійснювати її, формувати і вільно розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір, забезпечувати інформаційну безпеку відповідно до Конституції і законодавства України та норм міжнародного права з додержанням балансу інтересів особи, суспільства і держави[13].

У науковій літературі висловлено слушну думку про те, що «створення належних умов для реалізації державної політики, спрямованої на захист національних цінностей та реалізацію національних інтересів України, гарантування безпеки особи, суспільства і держави від зовнішніх та внутрішніх загроз в інформаційній сфері, потребує формування сучасних ефективних механізмів забезпечення інформаційної безпеки, які відповідатимуть характеру і масштабам викликів сьогодення. Складна воєнно-політична, оперативно-стратегічна та економічна ситуація, яка склалася внаслідок збройної агресії Російської Федерації проти нашої держави, набула загрозливих проявів у інформаційному просторі»[14].

Враховуючи наведені визначення, під державним суверенітетом в інформаційній сфері необхідно розуміти верховенство та незалежність держави в інформаційній сфері, її здатність: 1) контролювати і регулювати потоки інформації з-поза меж держави та всередині неї; 2) самостійно і незалежно визначати державну внутрішню та зовнішню інформаційну політику та здійснювати її; 3) формувати і вільно розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору; 4) забезпечувати інформаційну безпеку відповідно до Конституції і законодавства України та норм міжнародного права з додержанням балансу інтересів особи, суспільства та держави; 5) забезпечувати реалізацію державної політики, спрямованої на: а) захист національної ідеї, національних цінностей і реалізацію національних інтересів України шляхом здійснення інформаційної функції держави та інформаційної політики; б) забезпечення

безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в інформаційній сфері; в) формування сучасних ефективних механізмів забезпечення інформаційної безпеки, які відповідають характеру і масштабам викликів сьогодення.

Аналізуючи положення ст. 361 КК України, Р. О. Мовчан звертає увагу на те, що «перш ніж оголосити про проведення «спеціальної операції» та перейти до відкритого використання танків, артилерії, авіації, одурманених пропагандою солдат тощо, РФ ще протягом кількох тижнів перед 24 лютого 2022 р. широко вдавалась і до застосування іншої форми агресії – масштабних кібератак проти нашої держави, призначенням яких було не лише втручання в роботу об'єктів критичної інфраструктури, а й поширення панічних настроїв серед українців»[15]. Як зазначає А. В. Майснер, «кібератаки є швидше елементами інформаційної агресії, розглядаються як акти такої агресії за умови їх державницького походження або ж вияву системної боротьби радикальних (терористичних) збройних формувань»[16]. Кібератаки вчиняються в межах кіберпростору, який, як відомо, належить до інформаційного простору.

У контексті аналізу положень ст. 436[2] КК України Р. О. Мовчан зазначає, що «серед виявів ворожої пропаганди значну небезпеку становить поширення в Україні інформаційних матеріалів, спрямованих на пряме чи опосередковане виправдовування збройної агресії РФ та заперечення тимчасової окупації частини території України»[17]. Наявні підстави вважати, що наведене діяння посягає на державний суверенітет в інформаційній сфері.

Заслуговує на увагу висновок про те, що «головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку». Як підкреслює І. Р. Боднар, «власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні»[18].

Вчені слушно звертають увагу на те, що одну з найгостріших проблем національного масштабу становить інформаційна експансія. Н. А. Савінова пропонує розуміти інформаційну експансію як «суспільно небезпечне діяння у кримінально-правовому розумінні, а саме умисне захоплення із метою подальшого використання на свою користь інформаційного простору, або значного сегменту інформаційного простору певної держави чи групи держав. Інформаційні війни можуть створювати загрозу суспільним інтересам, починаючи від суверенітету держав, інформаційний простір яких не убезпечений належним чином»[19].

Варто погодитися з висновком Д. О. Олєйнікова про те, що «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)»[20].

У вітчизняній юридичній літературі ще 2014 р. вказувалось, що «чинний КК України містить достатню кількість норм, які здатні здійснювати охоронну та превентивну функції щодо інформаційного суверенітету України»[21]. Повномасштабна збройна агресія, нові загрози та виклики зумовили ситуацію, коли вітчизняний законодавець у 2022 р. після початку повномасштабного вторгнення запровадив кримінальну відповідальність за нові форми поведінки та виокремив нові спеціальні норми у цій сфері в КК України, які передбачають відповідальність за посягання на державний суверенітет в інформаційній сфері.

О. Е. Радутний дійшов висновку про необхідність кримінально-правової охорони інформаційного суверенітету України, але водночас наголосив на відсутності необхідності доповнення КК нормою з формулюванням «порушення інформаційного суверенітету України» у назві та (або) диспозиції[22]. Цей дослідник наголошує, що «порушення навіть інформаційного суверенітету завжди виявлятиметься в конкретних формах. Наприклад, це можуть бути заклики до дій, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, надання інформаційної допомоги іноземній державі, збирання з метою передачі або передача відомостей, що становлять державну, банківську, комерційну таємницю, відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, розголошення державної таємниці тощо. Проте відповідальність за такі дії вже передбачена ст. 109, 111, 114, 231, 328, 330 КК України»[23].

На думку Д. О. Олєйнікова, до посягань на інформаційний суверенітет України належать, зокрема, 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)[24]. Загалом погоджуючись із запропонованим автором підходом, необхідно зазначити, що наведена система посягань на державний суверенітет в інформаційній сфері не обмежується цими діяннями.

Висновки. Кримінально-правова охорона державного суверенітету України в інформаційній сфері здійснюється на підставі норм КК України, що передбачають кримінальну відповідальність за вчинення відповідних посягань. Як свідчить проведений аналіз норм Особливої частини КК, до цих діянь можуть у певних випадках належати такі кримінальні правопорушення, як: публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади (ч. 2 ст. 109); публічні заклики до дій, вчинених з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України (ч. 1 ст. 110), державна зрада (ст. 111), публічні заклики до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора; публічні заклики до співпраці з державою-агресором, збройними формуваннями та (або) окупаційною адміністрацією держави-агресора; публічні заклики до невизнання поширення державного суверенітету України на тимчасово окуповані території України (ч. 1 ст. 111^1), здійснення громадянином України пропаганди у закладах освіти незалежно від типів та форм власності з метою сприяння здійсненню збройної агресії проти України, встановленню та утвердженню тимчасової окупації частини території України, уникненню відповідальності за здійснення державою-агресором збройної агресії проти України, а також дії громадян України, спрямовані на впровадження стандартів освіти держави-агресора у закладах освіти (ч. 3 ст. 111^1), публічні заклики до проведення незаконних виборів та/або референдумів на тимчасово окупованій території (ч. 5 ст. 111^1), організація та проведення заходів політичного характеру, здійснення інформаційної діяльності у співпраці з державою-агресором та/або його окупаційною адміністрацією, спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або на уникнення нею відповідальності за збройну агресію проти України, за відсутності ознак державної зради, активна участь у таких заходах (ч. 6 ст. 111^1), шпигунство (ст. 114), несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (ст. 114^2), терористичний акт (ст. 258), розголошення державної таємниці (ст. 328), втрата документів, що містять державну таємницю (ст. 329), передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330), несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361), публічні заклики до агресивної війни або до розв'язування воєнного конфлікту (ст. 436), виготовлення, поширення комуністичної, нацистської символіки і пропаганда комуністичного та націонал-соціалістичного (нацистського)

тоталітарних режимів (ст. 436[1]), виправдовування, визнання правомірною, заперечення збройної агресії РФ проти України, глорифікація її учасників (ст. 436[2]) та ін.

Поряд з тим кримінально-правова охорона державного суверенітету в інформаційній сфері потребує якісно нових підходів законодавця до конструювання відповідних кримінально-правових норм, врахування підвищеної небезпеки та поширеності таких посягань в умовах збройної агресії РФ проти України.

1. Стратегія інформаційної безпеки (затверджена Указом Президента України від 28 грудня 2021 р. № 685/2021). URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 11.12.2022). **2.** Ісмайлов К. Ю., Бєлих Д. В. Інформаційний суверенітет і доктрина інформаційної безпеки України. *Порівняльно-аналітичне право.* 2019. № 1. С. 206. **3.** Доповідь заступника начальника департаменту контррозвідувального захисту в сфері інформаційної безпеки СБУ Юлії Лапутіної 12 червня 2018 р. на круглому столі в Укрінформі на тему: «Гібридна (інформаційна) агресія РФ. Відповіді України». URL: https://www.ukrinform.ua/rubric-presshall/2243886-gibridne-pole-bou-vidpovidiukraini-na-informaciinu-agresiu-rf.html (дата звернення: 28.12.2022). **4.** Дубов Д. В. Проблеми нормативно-правового забезпечення інформаційного суверенітету в Україні. *Вісник Національної академії керівних кадрів культури і мистецтв.* 2014. № 1. С. 233–238. **5.** Задерейко О. В., Троянський О. В., Чанишев Р. І. Концептуальні основи захисту інформаційного суверенітету України: монографія. Одеса: Фенікс, 2018. С. 10. **6.** Про національну програму інформатизації: Закон України від 04 лютого 1998 р. № 74/98-ВР. URL: http://zakon3.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80 (дата звернення: 10.12.2022). **7.** Стратегія інформаційної безпеки 2021 р. **8.** Там само. **9.** Пазюк А. В. Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти: дис. … д-ра юрид. наук: 12.00.11. Київ, 2016. С. 260. **10.** Пазюк А. В. Назв. праця. С. 263. **11.** Олєйніков Д. О. Зміст та складові інформаційного суверенітету як об'єкта кримінально-правової охорони. *Геополітика України: історія і сучасність:* збірник наукових праць. 2021. Випуск 1. С. 67. **12.** Радутний О. Е. Можливість захисту інформаційного суверенітету України кримінально-правовими засобами. *Інформація і право.* 2014. № 3. С. 114. **13.** Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України: автореф. дис. ... канд. юрид. наук: 12.00.07. Харків, 2006. С. 7. **14.** Довгань О. Д., Ткачук Т. Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право.* 2018. № 1 (24). С. 100. **15.** Новели кримінального законодавства України, прийняті в умовах воєнного стану: наук.-практ. комент. / А. А. Вознюк, О. О. Дудоров, Р. О. Мовчан, С. С. Чернявський та ін.; за ред. А. А. Вознюка, Р. О. Мовчана, В. В. Чернея. Київ: Норма права, 2002. С. 197. **16.** Майснер А. В. Міжнародний злочин «агресія» в сучасній доктрині міжнародного права: дис. … канд. юрид. наук. Київ, 2018. С. 148. **17.** Новели кримінального законодавства України, прийняті в умовах воєнного стану: наук.-практ. комент. С. 224. **18.** Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation.* 2014. № 1. С. 69. **19.** Савінова Н. А. Інформаційні війни в інформаційному суспільстві. *Інформаційна безпека людини, суспільства, держави.* 2012. № 3 (10). С. 70. **20.** Олєйніков Д. О. Назв. праця. С. 67. **21.** Радутний О. Е. Назв. праця. С. 117, 119.

22. Там само. **23.** Радутний О. Е. Вказ. праця. С. 117–118. **24.** Олєйніков Д. О. Назв. праця. С. 66.

References

1. Stratehiia informatsijnoi bezpeky (zatverdzhena Ukazom Prezydenta Ukrainy vid 28 hrudnia 2021 r. № 685/2021). URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (data zvernennia: 11.12.2022) [ukr.]. **2.** Ismajlov K. Yu., Bielykh D. V. Informatsijnyj suverenitet i doktryna informatsijnoi bezpeky Ukrainy. *Porivnial'no-analitychne pravo.* 2019. № 1. S. 206 [ukr.]. **3.** Dopovid' zastupnyka nachal'nyka departamentu kontrrozviduval'noho zakhystu v sferi informatsijnoi bezpeky SBU Yulii Laputinoi 12 chervnia 2018 r. na kruhlomu stoli v Ukrinformi na temu: «Hibrydna (informatsijna) ahresiia RF. Vidpovidi Ukrainy». URL: https://www.ukrinform.ua/rubric-presshall/2243886-gibridne-pole-bou-vidpovidiukraini-na-informaciinu-agresiu-rf.html (data zvernennia: 28.12.2022) [ukr.]. **4.** Dubov D. V. Problemy normatyvno-pravovoho zabezpechennia informatsijnoho suverenitetu v Ukraini. *Visnyk Natsional'noi akademii kerivnykh kadriv kul'tury i mystetstv.* 2014. № 1. S. 233–238 [ukr.]. **5.** Zaderejko O. V., Troians'kyj O. V., Chanyshev R. I. Kontseptual'ni osnovy zakhystu informatsijnoho suverenitetu Ukrainy: monohrafiia. Odesa: Feniks, 2018. S. 10 [ukr.]. **6.** Pro natsional'nu prohramu informatyzatsii: Zakon Ukrainy vid 04 liutoho 1998 r. № 74/98-VR. URL: http://zakon3.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80 (data zvernennia: 10.12.2022). [ukr]. **7.** Stratehiia informatsijnoi bezpeky 2021 r. [ukr.]. **8.** Tam samo [ukr.]. **9.** Paziuk A. V. Mizhnarodno-pravove rehuliuvannia informatsijnoi sfery (teoretychni i praktychni aspekty: dys…. d-ra iuryd. nauk: 12.00.11. Kyiv, 2016. S. 260 [ukr.]. **10.** Paziuk A. V. Vkaz. pratsia. S. 263 [ukr.]. **11.** Oliejnikov D. O. Zmist ta skladovi informatsijnoho suverenitetu iak ob'iekta kryminal'no-pravovoi okhorony. *Heopolityka Ukrainy: istoriia i suchasnist'.* Zbirnyk naukovykh prats'. 2021. Vypusk 1. S. 67 [ukr.]. **12.** Radutnyj O. E. Mozhlyvist' zakhystu informatsijnoho suverenitetu Ukrainy kryminal'no-pravovymy zasobamy. *Informatsiia i pravo.* 2014. № 3. S. 114 [ukr.]. **13.** Olijnyk O. V. Orhanizatsijno-pravovi zasady zakhystu informatsijnykh resursiv Ukrainy: avtoref. dys. ... kand. iuryd. nauk: 12.00.07. Kharkiv, 2006. S. 7 [ukr.]. **14.** Dovhan' O. D., Tkachuk T. Yu. Systema informatsijnoi bezpeky Ukrainy: ontolohichni vymiry. *Informatsiia i pravo.* 2018. № 1 (24). S. 100 [ukr.]. **15.** Novely kryminal'noho zakonodavstva Ukrainy, pryjniati v umovakh voiennoho stanu: nauk.-prakt. koment. / A. A. Vozniuk, O. O. Dudorov, R. O. Movchan, S. S. Cherniavs'kyj ta in.; za red. A. A. Vozniuka, R. O. Movchana, V. V. Cherneia. Kyiv: Norma prava, 2002. S. 197 [ukr.]. **16.** Majsner A. V. Mizhnarodnyj zlochyn «ahresiia» v suchasnij doktryni mizhnarodnoho prava: dys. … kand. iuryd. nauk. Kyiv, 2018. S. 148 [ukr.]. **17.** Novely kryminal'noho zakonodavstva Ukrainy, pryjniati v umovakh voiennoho stanu: nauk.-prakt. koment. S. 224 [ukr.]. **18.** Bodnar I. R. Informatsijna bezpeka iak osnova natsional'noi bezpeky. *Mechanism of Economic Regulation.* 2014. № 1. S. 69 [ukr.]. **19.** Savinova N. A. Informatsijni vijny v informatsijnomu suspil'stvi. Informatsijna bezpeka liudyny, suspil'stva, derzhavy. 2012. № 3 (10). S. 70 [ukr.]. **20.** Oliejnikov D. O. Vkaz. pratsia. S. 67 [ukr.]. **21.** Radutnyj O.E. Vkaz. pratsia. S. 117, 119 [ukr.]. **22.** Tam samo [ukr.]. **23.** Radutnyj O.E. Vkaz. pratsia. S. 117-118 [ukr.]. **24.** Oliejnikov D.O. Vkaz. pratsia. S. 66 [ukr.].

Kubalskiy Vladyslav. **Criminal legal protection of state sovereignty of Ukraine in the information sphere**

Introduction. *In the context of the ongoing armed aggression of the russian federation against Ukraine and globalization processes in the information sphere,*

special attention of legal scholars is drawn to solving the problems of criminal legal protection of Ukraine's state sovereignty in the information sphere. Against Ukraine, the russian federation uses the latest information technologies to influence the minds of citizens aimed at inciting national and religious hatred, propaganda of an aggressive war, changing the constitutional order by force or violating the sovereignty and territorial integrity of Ukraine. Failure to ensure the sovereignty of the state in the information sphere can lead to the loss of sovereignty in general. Therefore, the state needs to ensure proper protection of state sovereignty in the information sphere by means of criminal law.

The aim of the article. *This research is aimed at defining the system of norms that provide for criminal liability for encroachment on the state sovereignty of Ukraine in the information sphere.*

Results. *State sovereignty in the information sphere should be understood as the supremacy and independence of the state in the information sphere, its ability to: 1) to control and regulate information flows from outside and within the state; 2) to independently and independently determine the state internal and external information policy and implement it; 3) to form and freely dispose of its own information resources, to form the infrastructure of the national information space; 4) to ensure information security in accordance with the Constitution and legislation of Ukraine and international law, while maintaining the balance of interests of the individual, society and the state; 5) to ensure the implementation of the state policy aimed at: a) protection of the national idea, national values and realization of the national interests of Ukraine through the implementation of the information function of the state and information policy, b) ensuring the security of the individual, society and the state from external and internal threats in the information sphere, c) formation of modern effective mechanisms for ensuring information security that meet the nature and scale of the current challenges.*

According to the analysis of the provisions of the Special part of the Criminal code, these acts may in certain cases include the following criminal offenses: public calls for violent change or overthrow of the constitutional order or seizure of state power (part 2 of Art. 109); public calls for actions committed with the aim of changing the boundaries of the territory or state border of Ukraine in violation of the procedure established by the Constitution of Ukraine (part 1 of Art. 110), high treason (Art. 111), public calls to support decisions and/or actions of the aggressor state, armed formations and/or the occupation administration of the aggressor state; public calls to cooperate with the aggressor state, armed formations and/or the occupation administration of the aggressor state; public calls to non-recognition of the extension of state sovereignty of Ukraine to the temporarily occupied territories of Ukraine (part. 1 of Art. 111[1]), propaganda by a citizen of Ukraine in educational institutions regardless of type and form of ownership to facilitate the armed aggression against Ukraine, the establishment and consolidation of the temporary occupation of part of the territory of Ukraine, avoidance of responsibility for the armed aggression against Ukraine by the aggressor state, as well as actions of citizens of Ukraine aimed at implementing the education standards of the aggressor state in educational institutions (part 3 of Art. 111[1]), public calls for illegal elections and/or referendums in the temporarily occupied territory of Ukraine (part 3 of Art. 111[1]), organizing and conducting political events, carrying out information activities in cooperation with the aggressor state and/or its occupation administration aimed at supporting the aggressor state, its occupation administration

or armed formations and/or avoiding responsibility for armed aggression against Ukraine, in the absence of signs of treason, active participation in such events (part 6 of Art. 111[1]), espionage (Art. 114), unauthorized dissemination of information on the sending, movement of weapons, armaments and ammunition to Ukraine, movement, movement or deployment of the Armed Forces of Ukraine or other military formations formed in accordance with the laws of Ukraine, committed under martial law or a state of emergency (Art. 114[2]), terrorist act (Art. 258), disclosure of state secrets (Art. 328), loss of documents containing state secrets (Art. 329), transfer or collection of data constituting official information collected in the course of operational and investigative, counterintelligence activities, in the field of defense of the country (Art. 330), unauthorized interference with the operation of information (automated), electronic communication, information and communication systems, electronic communication networks (Art. 361), public calls for aggressive war or for the outbreak of a military conflict (Art. 436), production, distribution of communist and Nazi symbols and propaganda of communist and national socialist (Nazi) totalitarian regimes (Article 436[1]), justification, recognition as lawful, denial of the armed aggression of the Russian Federation against Ukraine, glorification of its participants (Art. 436[2]) and others.

Conclusions. *The criminal law protection of state sovereignty in the information sphere requires qualitatively new approaches of the legislator to the construction of relevant criminal law provisions, taking into account the increased danger and prevalence of such encroachments in the context of the armed aggression of the russian federation against Ukraine.*

Key words: *state sovereignty in the information sphere (information sovereignty), armed aggression of the russian federation, criminal law protection, information security.*