УДК 342.9:004.056:347.83(477)
DOI https://doi.org/10.32850/sulj.2020.4.7

СУЧАСНІ ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ ТА ДОКТРИНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Михальський Я. В., Пишна А. Г.

У статті визначено інноваційні підходи до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації. Приділено увагу проблемам інформаційного суверенітету та інформаційної безпеки і наведено особливості становлення інформаційного суспільства в українських реаліях, визначено основні завдання і напрями державної інформаційної політики та можливі загрози національній безпеці. Надано аналіз рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» та Закону України від 21 червня 2018 року № 2469-VIII «Про основні засади забезпечення кібербезпеки України». Розглядаються такі терміни, як «стратегічні комунікації», «урядові комунікації», «кризові комунікації», «стратегічний наратив».

У статті зроблено висновки, що: 1) інформаційний суверенітет держави не повинен перетворюватися на самоціль; 2) соціальною цінністю суверенітету є юридична самостійність держави, котра виявляється в непідкоренні іншій державі або групі держав, тобто незалежність від чужої волі; 3) для виправлення неприпустимого становища, що утворилося в інформаційній сфері, необхідно чітко визначити законом інформацію, доступ до якої обмежується, і мету обмеження. При цьому перелік відомостей, які входять до кола обмежень, має бути вичерпно визначеним і систематично оприлюдненим; 4) державі необхідно дотримуватися принципів максимального оприлюднення та чіткого переліку щодо обмежень (винятки повинні бути зрозумілими, описуватися вузько, підлягати контролю на предмет наявності «шкоди» і впливу на «суспільні інтереси»); 5) доступність інформації має переважати над виправданням в обмеженні такої доступності. Вся інформація, яку зберігають державні органи влади, підлягає оприлюдненню, винятки можуть бути тільки для дуже обмеженого числа випадків.

Ключові слова: *державна інформаційна політика, інформаційний суверенітет, інформаційне суспільство, національний інформаційний простір, інформаційне законодавство, інформаційна безпека, доктрина інформаційної безпеки.*

Mykhalskyi Ya. V., Pyshna A. H. Current features of information sovereignty and a doctrine of information security of Ukraine

The article defines innovative approaches to the formation of a system of protection and development of the information space in the conditions of globalization and free circulation of information. The attention is paid to the problems of information sovereignty and information security, and the peculiarities of the formation of the information society in Ukrainian realities are pointed out, the main tasks and directions of the state information policy and possible threats to national security are determined. An analysis of the decision of the National Security and Defense Council of Ukraine dated December 29, 2016 "On the Doctrine of Information Security of Ukraine" was given. Terms such as "strategic communications", "government communications", "crisis communications", "strategic narrative".

The article concludes that: 1. Information sovereignty of the state should not become an end in itself. 2. The social value of sovereignty is the legal independence of the state, which is manifested in non-obedience to another state or group of states, that is, independence from the will of others. 3. In order to correct the unacceptable situation that has emerged in the information sphere, it is necessary to clearly identify the information, the access to which is restricted by law, and the purpose of the restriction. In this case, the list of information that is within the scope of restrictions should be exhaustively defined and systematically made public. 4. The state must comply with the principles of maximum disclosure and a checklist of restrictions (exceptions must be clear, narrowly described, put in control of the existence of "harm" and influence on "public interests"). 5. The availability of information should prevail over justifications in the limitation of such availability.

Key words: *state information policy, information sovereignty, information society, national information space, information law, information security, doctrine of information security.*

Постановка проблеми та її актуальність. Сьогодні активно обговорюється на всіх рівнях вплив Російської Федерації на різні сфери, сектори української держави. Безперечно, це так, але мало лише констатувати, що зараз Російською Федера-

цією поряд із реальними військовими діями в Донбасі та АР Крим проти України застосовуються технології гібридної війни. Наведемо визначення: гібридна війна – це війна з поєднанням у застосуванні конвенційної зброї, партизанської війни, тероризму, кібервійни та злочинної поведінки з метою досягнення певних політичних цілей, основним інструментом якої є створення державою-агресором у державі, вибраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням для досягнення політичних цілей агресії, які досягаються звичайною війною [1].

Необхідно розбиратися на доктринальному рівні, чому влада України дозволила вільно діяти російським кібервійськам.

Аналіз останніх досліджень і публікацій. Так, не можна казати, що питанням інформаційного суверенітету та безпеки раніше не приділялася увага. Різні зазначені аспекти досліджували Д. Белл, М. Кастельс, Ю. Хаяши, Е. Тоффлер, які надали визначення інформаційного суспільства, окреслили його основні риси. В Україні такі вчені, як В. Гапотій, Г. Почепцов, В. Голобуцький, В. Брижко, В. Цимбалюк, О. Олійник, Л. Шиманський та ін., приділяли значну увагу у своїх дослідженнях питанням вивчення особливостей становлення інформаційного суспільства в українських реаліях, визначали основні завдання та напрями державної інформаційної політики й можливі загрози національної безпеки. Зараз дослідження актуальних загроз українській національній безпеці в інформаційній сфері потребує негайного вирішення.

Метою статті є визначення інноваційних аспектів до формування розвитку системи захисту та інформаційного простору в умовах сьогодення.

Виклад основного матеріалу. Досліджуючи окреслене питання, необхідно зазначити, що 25-го лютого 2017 року Президент України підписав Указ [2] про введення в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [3]. Також не можна не приділити уваги Закону України від 21.06.2018 р. № 2469-VIII «Про основні засади забезпечення кібербезпеки України» [4]. Також треба зазначити, що ми підтримуємо анонсування міністром культури України Володимиром Бородянським підготовку законопроекту «Про дезінформацію», який вводить спеціальний орган – уповноваженого з питань інформації, який покликаний захищати інформаційний український простір від дезінформації, виявлятиме її, попереджатиме про неї та буде звертатись до суду для покарання [5].

Таким чином, перераховані нормативно-правові акти безпосередньо опікуються політикою держави щодо інформаційної безпеки держави та визначають національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями та пріоритети державної політики в інформаційній сфері.

Дослідимо Доктрину інформаційної безпеки 2017 року та її корисність для України. Так, вказана Доктрина визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері, тому більш детально розглянемо текст документу.

Так, у 1-му пункті Доктрини «Загальні положення» наведені визначення понять «стратегічні комунікації», «урядові комунікації», «кризові комунікації», «стратегічний наратив». Розглянемо детально кожне з цих понять.

Поняття «стратегічні комунікації» сформульоване щонайменше некоректно. Стратегічні комунікації визначаються як скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави.

Якщо порівняти запропоноване визначення в Доктрині та загальноприйняте поняття, то виникають певні питання, які необхідно вирішувати.

1. У Доктрині розглядається лише використання комунікативних можливостей держави, але ще існує використання комунікативних можливостей корпорацій та громади. Треба думати, що корпорації не можуть (не хочуть) діяти на благо держави, і громада не здатна до стратегічних комунікацій, чи держава не хоче це все координувати. Покажемо на прикладі. Телеканали «112 Україна» та «NewsOne» не належать до «комунікативних можливостей держави» (чи може їхня державність є однією з державних таємниць), але українська громада бачить безпосередній вплив держави на політику цих приватних телеканалів. Яким чином це відбувається? Бо в понятті «стратегічні комунікації» це не відображено ніяким чином.

2. Не вказано походження стратегії для так званих «стратегічних комунікацій» – хто її розробляє, хто втілює. Тобто незрозуміло, чому раптом комунікації держави стають стратегічними. Тобто якість «стратегічності» введена у визначення формально. Якщо Доктрина – не місце для обговорення питання, звідки береться стратегія та як

вона впроваджується та коригується, то потрібно сказати хоча би про головну стратегічну установку інформаційної політики задля безпеки України.

3. Не вказані базові установки для стратегічних комунікацій – збереження, розвиток та експансія України з такими основними атрибутами – цілісною територією; політичною, економічною, соціальною, культурною та інформаційною незалежністю; правом на незалежну Конституцію; правом на незалежну внутрішню політику та правом на суб'єктну зовнішню політику.

Поняття «урядові комунікації» визначено однобічно. Розглядати ж дійсні «урядові комунікації» потрібно значно ширше:

– по-перше, урядові комунікації – це такі комунікації, які є тактичною реалізацією стратегії України в стратегічних комунікаціях. Тобто ми маємо вже у визначенні пов'язати урядові комунікації (тактика) зі стратегічними комунікаціями (стратегія);

– по-друге, якщо Уряд лише роз'яснює, а не коригує у своїй комунікації власну політику, то в такому визначенні урядової політики фактично сформульована «непомильність Уряду».

Поняття «кризові комунікації» має ознаки маніпулятивного поняття та є лише «комунікацією під час війни», в яких Президент та Уряд можуть обмежувати урядові комунікації ситуацією монологу чи диктату від Уряду до корпорацій та громади. Але такі комунікації мають бути чітко пов'язані з уведенням військового стану. В іншому разі Президент та Уряд можуть будь-який стан, що їм не подобається, оголосити кризовим, як це вже не раз бувало в історії незалежної України, і як це відбувається зараз під час так званої штучної кризи в електроенергетиці, якою Уряд шантажує блокувальників контрабанди Донбасу [6].

Поняття «стратегічний наратив» є ключовим контентним елементом всієї інформаційної (в т.ч. пропагандистської) діяльності держави, і на його утвердження в цільових аудиторіях і спрямовується діяльність усіх комунікативних можливостей держави. Проблемою залишається те, що дотепер відсутнє єдине розуміння самої концепції стратегічного наративу.

Однак і досі не вирішеними залишаються питання: якою мірою має бути викладений стратегічний наратив, наскільки він має бути конкретний та в якій формі зафіксований (а також – в якому типі документу має відбутись таке фіксування) [7].

Також треба відзначити, що, розбираючи поняття та ознаки стратегічного наративу, постає все більше не юридичних питань, а суто філософських. Оскільки в другому пункті «Мета та принципи Доктрини» сказано, що «метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни», то виникає питання: чому Доктрина спрямована тільки проти певної держави, хоч вона і проголошується державою-агресором? На наш погляд, доктрина повинна застосовуватися не до конкретної держави або події, а бути універсальним інструментом. В умовах глобалізації інформаційного простору і прагнення України формувати інформаційне громадянське суспільство не може ідея протидії інформаційному впливу Російської Федерації підміняти собою весь обсяг спрямування інформаційної безпеки України. Існують й інші держави, з якими ми маємо будувати партнерські інформаційні за змістом стосунки задля самовизначення України як рівних з іншими державами в інформаційному «полі» цивілізованих сучасних правовідносин, де саме вітчизняна Доктрина інформаційної безпеки має визначати прагнення України до досягнення високого рівня інформаційного суверенітету. І хоч цей термін неодноразово відкидався і парламентом, і президентом у минулі роки, до початку агресивних закидів Російської Федерації, однак сьогодні питання впровадження його в нормативно-правовий обіг постає з новою силою і в більшому обсязі, ніж раніше [8, с. 206–208].

Самі автори Доктрини стверджують, що вона базується на принципах додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України. І таке декларування засад Доктрини найкраще ілюструє, що інформаційний суверенітет як невід'ємна складова частина державного суверенітету і має стати об'єктовим складником заявлених у Доктрині відносин. У такому випадку засадничі положення, що визначають спрямованість волі народу, а отже, й органів державної влади в напрямі здійснення державної політики у сфері інформаційної безпеки, не будуть залежати від того, яка саме організація прагне завдати шкоди інформаційному простору України і інформаційним правам українців.

У пункті 2 «Мета та принципи» вказано таке: «метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформа-

ційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни». Це класичний приклад того, як не потрібно ставити в Доктрині цілі стратегічного характеру. Не можна будувати інформаційну політику на протидії кому-небудь чи чому-небудь. Це реакційний підхід, тобто позиція упосліджена, безперспективна і провальна. Доктрина інформаційної безпеки повинна формулювати виклики набагато більш далекоглядні та масштабні за своєю суттю.

Неефективно повсякденним наративом з елементами української пропаганди воювати з повсякденним наративом з елементами російської пропаганди. Це мало що дасть. Лише краща структурна організація повсякденного наративу, вища інтелектуалізація цього наративу і насичення його елементами стратегічного дискурсу дає нам шанс на перемогу в інформаційній війні (про яку в тексті Доктрини є згадка, але серед понять означення «інформаційної війни» відсутнє).

Успіх російської пропаганди полягає в тому, що в неї є довгострокова стратегія, що робити з Україною, а в України такої довгострокової стратегії немає, що є головною проблемою інформаційної безпеки для України.

Доктрина у своїх засновках першого та другого розділу написана так, ніби десь уже є якась державна стратегія, а професійні інструменти роботи з інформаційним простором мають її просунути та відстояти перед російською пропагандою. Тобто найголовніший виклик – відсутність стратегії в української влади. Стратегічні комунікації є там, де є стратегія. Коли немає стратегії, то не може бути ніяких стратегічних комунікацій [8, с. 207–209].

У п. 3 Доктрини «Національні інтереси України в інформаційній сфері» сформульовані Національні інтереси України в інформаційній сфері. Отже, Національними інтересами України в інформаційній сфері є:

1. Життєво важливі інтереси особи:

– забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

– забезпечення конституційних прав людини на захист приватного життя;

– захищеність від руйнівних інформаційно-психологічних впливів [3].

Доцільно звернути увагу на те, що автори Доктрини характеризують «скорочений» обсяг змісту конституційних інформаційних прав і свобод, зосереджуючись лише на збиранні, зберіганні, використанні та поширенні інформації. Тут слід наголосити, що це суттєво звужена конструкція, адже тільки законодавчо закріплене право на інформацію [9] передбачає, окрім визначених вище змістових складників також: пошук, виготовлення (що дуже актуально для інформаційної незалежності), захист (який не може бути охоплений поняттям зберігання) інформації.

2. Серед життєво важливих інтересів суспільства і держави в інформаційній сфері Доктриною визначені:

– захист українського суспільства від агресивного впливу деструктивної пропаганди;

– захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

– всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності в доступі до достовірної та об'єктивної інформації;

– забезпечення вільного обігу інформації;

– розвиток та захист національної інформаційної інфраструктури;

– збереження і примноження духовних, культурних і моральних цінностей Українського народу;

– забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;

– вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;

– зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;

– розвиток медіакультури суспільства та соціально відповідального медіасередовища;

– формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;

– створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;

– розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;

– безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;

– розвиток системи стратегічних комунікацій України;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;

– забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

– захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;

– формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти;

– розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та в супутниковому мовленні за межами України.

Загалом перераховані елементи, що становлять життєво важливі інтереси суспільства і держави в інформаційній сфері, не викликають сумнівів у їх актуальності й потребі захисту. Однак знову ж таки згадування в цих положеннях про інформаційний простір, про інформаційну самостійність, інформаційну незалежність, та, за ідейним навантаженням, і національний інформаційний продукт, говорить про «підсвідоме» прагнення авторів Доктрини до ймовірності потреби оперування в цьому документі категорією «інформаційний суверенітет» [3, п. 3].

Четвертий пункт Доктрини «Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері» розвиває ідеї, що повністю «зав'язані» на інформаційному суверенітеті. Узагальнюючи підходи до особливостей сучасного розуміння інформаційного суверенітету та пристосовуючи ці положення до України, можна окреслити такі основні його складники:

1) законодавче визначення та забезпечення стратегічних напрямів розвитку і захисту національного інформаційного простору;

2) визначення норм, засад і меж діяльності зарубіжних та міжнародних суб'єктів у національному інформаційному просторі України;

3) формування та захист інтересів України у світовому інформаційному просторі, міжнародних інформаційних відносинах;

4) участь у заходах, що сприяють сталому розвитку національного інформаційного простору України та зміцненню її суверенітету;

5) гарантування інформаційної безпеки України [10, с. 119].

Враховуючи, що в прикінцевих положеннях Доктрини передбачається можливість реалізації Доктрини лише за умови належної координації заходів, здійснюваних усіма державними органами, а суб'єкти реалізації державної інформаційної політики у взаємодії з інститутами громадянського суспільства в межах компетенції повинні забезпечувати реалізацію Доктрини, а також за необхідності вносити обґрунтовані пропозиції щодо корегування її положень, то має сенс звернути увагу і на певні протиріччя ідейно-категоріального характеру в Доктрині.

До інструментальної частини Доктрини, тобто до тієї частини, де пропонуються ті чи інші інструменти, найменше претензій. З огляду на деяку журналістську та експертну критику з цього приводу можна зауважити, що під час війни такі дії в інформаційному просторі можуть бути виправдані [3].

Крім того, є декілька неточностей в Доктрині. Перша проблема – у самій назві Доктрини. Якщо ми говоримо про інформацію, то це повідомчий монолог – журналістів, експертів. Якщо про комунікацію, то це значно ширше, ніж інформація, бо тут діє політолог, причому з останніми телекомунікаційними досягненнями – інтерактивний політолог.

Не може в інформаційному просторі виникати ніякої комунікації, якщо ми його не розглядаємо як комунікаційний простір. Тобто право вживати термін «комунікація» з'являється лише в інакше поіменованій Доктрині – «Доктрині комунікаційної безпеки».

У сучасному світі інформація вже не є основою безпеки. Основою безпеки є комунікація людей між собою, представниками влади та недержавними установами з приводу інформації.

Доктрина такої ситуації не передбачає. Отже, ніякої інформаційної безпеки така Доктрина у своїх засновках не пропонує – вона лише закріплює проблему стратегічного протистояння, надаючи владно-олігархічній стратегічній установці преференції. Тому Доктрина у своїх засновках – це маніпуляція на користь захисту провладної цензури у ЗМІ, яка прикривається війною Росії проти України.

Отже, правильні інструменти, що запропоновані в Доктрині, нівелюються засадничими двома розділами. Не можуть бути ефективно задіяні навіть дуже професіональні інструменти, якщо в стратегічному плані понятійні уявлення та цілі сформульовані невірно [6].

Слід відзначити, що до прийняття Закону України «Про основні засади забезпечення кібербезпеки України» в національному законодавстві щодо кібербезпеки не було профільного Закону, регулювання відносин у даній сфері відбувалося численними нормами загального характеру. Відповідно до преамбули Закон визначає сферу регулювання суспільних відносин у чотирьох напрямах:

1) правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі;

2) основні цілі, напрями та принципи державної політики у сфері кібербезпеки;

3) повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері;

4) основні засади координації їхньої діяльності із забезпечення кібербезпеки [11].

Підводячи підсумок усьому вищенаведеному, доцільно зробити такі висновки:

1. Суверенітет держави та його окремі аспекти, зокрема інформаційний суверенітет, не повинен перетворюватися на самоціль.

2. Кіберзлочинність вимагає комплексного підходу до вирішення існуючих проблем як з боку органів державної влади, місцевого самоврядування, правоохоронних органів, так і з боку інших зацікавлених суб'єктів.

3. Соціальною цінністю суверенітету є юридична самостійність держави, котра виявляється в непідкоренні іншій державі або групі держав, тобто незалежність від чужої волі. Однак ця незалежність не означає непідкорення міжнародному праву та не повинна бути теоретичним обґрунтуванням самоізоляції, відокремлення та автаркії. У цьому контексті прагнення українського законодавця до реалізації інформаційного суверенітету в тому вигляді й розумінні, в якому це поняття закріплене в законодавстві, може призвести до випадіння України з міжнародного інформаційного простору.

4. Для виправлення неприпустимого становища, що утворилося в інформаційній сфері, необхідно чітко визначити законом інформацію, доступ до якої обмежується, і мету обмеження. При цьому перелік відомостей, які входять до кола обмежень, має бути вичерпано визначеним і систематично оприлюдненим.

5. У зазначеному випадку необхідно також дотримуватися двох принципів. Перший – це принцип максимального оприлюднення: вся інформація, яку зберігають державні органи влади, підлягає оприлюдненню, винятки можуть бути тільки для дуже обмеженого числа випадків. Другий принцип характеризує вимоги щодо обмежень: а) винятки повинні бути зрозумілими, б) описуватися вузько, в) підлягати контролю на предмет наявності «шкоди» і впливу на «суспільні інтереси». А саме: рішення державного органу обмежити доступ до інформації є виправданим, якщо, по-перше, інформація має відношення до легітимної мети, передбаченої законом; по-друге, її оприлюднення має дійсно загрожувати спричиненням суттєвої шкоди легітимній меті; по-третє, шкода, яка може бути заподіяна вказаній меті, повинна бути вагомішою, ніж суспільний інтерес в отриманні інформації.

6. Вочевидь, проголошення законодавцем інформаційного суверенітету та захист інформації з обмеженим доступом як елемент інформаційної безпеки певною мірою перехрещуються з принципом інформаційної свободи, що передбачає апріорі весь соціальний інформаційний загал як такий, що є загально доступним. Тобто доступність інформації має переважати над виправданням в обмеженні такої доступності [8, с. 209].

Література

1. Гібридна війна. URL: https://uk.wikipedia.org/wiki/Гібридна_війна

2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ Президента України від 25.02.2017 р. № 47/2017. URL: http://zakon3.rada.gov.ua/laws/show/47/2017

3. Про Доктрину інформаційної безпеки України. Рішення РНБО від 29.12.2016 р. URL: http://zakon3.rada.gov.ua/laws/show/n0016525-16/paran2#n2

4. Про основні засади забезпечення кібербезпеки України : Закон України від 21.06.2018 р. №2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

5. Закон про дезінформацію: як влада хоче боротися з фейками, соцмережами і журналістами. URL: https://www.bbc.com/ukrainian/features-51268503

6. Дацюк С. Проблеми інформаційної безпеки, які ігноруються. *«Украинская правда»* від 28.02.2017. URL: https://www.facenews.ua/columns/2017/312448/

7. Мандзюк О. Засади розроблення стратегічного наративу. URL: http://goal-int.org/zasadi-rozroblennya-strategichnogo-narativu/

8. Ісмайлов К.Ю., Бєлих Д.В. Інформаційний суверенітет та доктрина інформаційної безпеки України. *Електронне наукове видання «Порівняльно-аналітичне право»*. 2019. № 1. С. 206–209.

9. Про інформацію : Закон України від 02.10.1992 р. № 2658-XII. URL: http://zakon2.rada.gov.ua/laws/show/2657-12

10. Ісмайлов К.Ю. Юридичні тенденції та концептуальні підходи до інформаційного суверенітету в Україні. *International Scientific-Practical Conference Development of legal regulation in East Europe: experience of Poland and Ukraine* : Conference Proceedings, January 27-28, 2017. Sandomierz. P. 117-119.

11. Науково-практичний коментар до Закону України «Про основні засади забезпечення кібербезпеки України» / В.Л. Грохольський та ін. ; за заг. ред. д.ю.н., проф. В.Л. Грохольського ; Одеський держ. унів-т внутр. Справ. Одеса, 2020. 173 с.

Михальський Я. В.,
аспірант
Одеського державного університету
внутрішніх справ

Пишна А. Г.,
кандидат юридичних наук,
доцент кафедри адміністративної
діяльності поліції
Одеського державного університету
внутрішніх справ