УДК 34:351.862.2:001.102-049.5
DOI https://doi.org/10.32782/2524-0374/2023-9/65

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

CURRENT THREATS TO THE INFORMATION SECURITY OF UKRAINE IN THE CONDITIONS OF THE LEGAL REGIME OF THE MARTIAL STATE

Скочиляс-Павлів О.В., д.ю.н., професор,
професор кафедри адміністративного та інформаційного права
Інститут права, психології та інноваційної освіти Національного університету «Львівська політехніка»

У статті аналізуються сучасні загрози інформаційній безпеці України в умовах правового режиму воєнного стану. Вказується, що сьогодні, в умовах повномасштабної війни в Україні, питання інформаційної безпеки набувають особливої гостроти та актуальності, адже рівень захищеності національних інформаційних ресурсів є одним з факторів, який визначає хід воєнних дій. Розглядається поняття «загроза інформаційній безпеці» та висвітлюються підходи вчених до класифікації загроз інформаційній безпеці. Загрози інформаційній безпеці трактуються як потенційні небезпечні події або фактори, які можуть ставити під загрозу як конфіденційність, цілісність доступність інформації, так і національну безпеку держави загалом.

Сьогодні велика кількість загроз і викликів безпосередньо або опосередковано пов'язана із діяльністю російської федерації. Державою-агресором активно використовуються спеціальні методи, способи і засоби маніпулювання суспільною свідомістю, а також поглядами, цільовими установками і поведінковими стереотипами різних соціальних груп, розділених за етнічною, національною, конфесійною чи іншою ознакою, що веде до дестабілізації внутрішньополітичної та соціальної ситуації, підриву суверенітету і територіальної цілісності України. У зв'язку з цим досить актуальним є розвиток міждисциплінарного напрямку – інформаційно-психологічна безпека.

Процес прогнозування та аналізу всього спектру загроз національній безпеці, як ніколи, набув особливої актуальності. Державна інформаційна політика повинна здійснюватися послідовно з урахуванням національних інтересів нашої держави, постійно мінливих умов та нових загроз інформаційній безпеці, які походять як зі зовнішнього інформаційного простору, так і обумовлені внутрішньодержавними обставинами. Лише за наявності державного підходу до вирішення проблеми охорони та захисту інформації в інформаційних системах, телекомунікаційних мережах можна створити умови для адекватної протидії збільшенню загроз в інформаційному полі.

Ключові слова: інформаційна безпека, воєнний стан, інформаційні загрози, стратегія інформаційної безпеки, інформаційно-психологічна безпека, протидія інформаційним загрозам.

The article analyzes modern threats to Ukraine's information security in the conditions of the legal regime of martial law. It is indicated that today, in the conditions of a full-scale war in Ukraine, issues of information security are becoming particularly acute and urgent, because the level of security of national information resources is one of the factors that determines the course of military operations. The concept of "threat to information security" is considered and the approaches of scientists to the classification of threats to information security are highlighted. Threats to information security are interpreted as potential dangerous events or factors that can endanger the confidentiality, integrity, availability of information, and the national security of the state in general.

Today, a large number of threats and challenges are directly or indirectly related to the activities of the russian federation. The aggressor state actively uses special methods, methods and means of manipulating public consciousness, as well as views, target attitudes and behavioral stereotypes of various social groups, divided by ethnic, national, religious or other characteristics, which leads to destabilization of the domestic political and social situation, undermining sovereignty and territorial integrity of Ukraine. In this regard, the development of an interdisciplinary direction – informational and psychological security – is quite relevant.

The process of forecasting and analysis of the entire spectrum of threats to national security has become more relevant than ever. State information policy should be carried out consistently, taking into account the national interests of our state, constantly changing conditions and new threats to information security, which originate both from the external information space and due to domestic circumstances. Only in the presence of a state approach to solving the problem of protection and protection of information in information systems and telecommunication networks, it is possible to create conditions for adequate countermeasures against the increase in threats in the information field.

Key words: information security, martial law, information threats, information security strategy, information and psychological security, countering information threats.

Постановка проблеми. Науково-технічний прогрес і пов'язана з ним інтеграція людської діяльності привели до виникнення глобальних проблем сучасності, які гостро поставили перед людською цивілізацією проблему виживання, безпеки її розвитку. Залежно від загроз людському існуванню можна розглядати такі складові безпеки людського суспільства: ядерну, екологічну, політичну, технологічну, економічну та інші. Основою цих складових є інформаційна безпека. І сьогодні, в умовах повномасштабної війни в Україні, питання інформаційної безпеки набувають особливої гостроти та актуальності, адже рівень захищеності національних інформаційних ресурсів є одним з факторів, який визначає хід воєнних дій. Сучасні загрози інформаційній безпеці постали як нові виклики, які потребують як вдосконалення державної політики, так і конкретних, практичних дій для їх нейтралізації.

В. Артемов, В. Хорошко, Ю. Хохлачова, В. Погорелов, підкреслюючи суперечливості сучасного світу, вважають, що найважливіше значення для більшості держав має інформаційна та воєнна небезпека, саме тому важливою підсистемою загальної системи забезпечення національної безпеки України називають забезпечення інформаційно-воєнної безпеки [1, с. 23, 24].

Стан опрацювання проблематики. Вивченню різних аспектів у сфері інформаційної безпеки присвячені роботи українських вчених: В. Антонюка, І. Арістової, І. Березовської, М. Биченка, Н. Бортник, В. Грищенка, М. Гуцалюка, Б. Демидова, О. Довгань, Я. Жаркова, В. Зайцева. І. Замаруєва, С. Єсімова, Р. Калюжного, Б. Кормича, О. Кохановської, В. Ліпкан, Г. Линник, О. Литвиненка, П. Мельника, В. Негодченка, О. Олійника, Д. Русака, Т. Перуна, Т. Слінько, Д. Федченка, В. Цимбалюка, В. Шамрая, М. Швеця, Ю. Яцишина та багатьох інших.

Запровадження в Україні воєнного стану поставило перед науковцями нові завдання та виклики. В. Артемов, О. Александров, В. Алещенко, О. Звоздецька, О. Кантур, Д. Камак, Є. Курінний, Ю. Кучеренко, А. Носик, С. Онопрієнко, В. Погорелов, В. Хорошко, Ю. Хохлачова у своїх дослідженнях звертаються до теми інформаційної безпеки в умовах повномасштабної збройної агресії.

Мета дослідження полягає в тому, щоб визначити сучасні загрози та виклики інформаційній безпеці в умо-

вах воєнного стану та окреслити відповідні шляхи протидії збільшенню загроз в інформаційному полі.

Виклад основного матеріалу. Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. І це недарма, адже інформаційна безпека держави є постійним об'єктом посягань, якому протистоять різноманітні інформаційні загрози, особливо це проявляється під час воєнного стану, коли держава-агресор активно використовує такі інструменти як масове, щоденне поширення фейкової інформації про хід воєнних дій, пропаганду своїх викривлених цінностей, маніпулювання громадською думкою, заборону українських каналів на окупованих територіях, психологічний та моральний тиск на населення підконтрольних територій.

Стратегія інформаційної безпеки від 28 грудня 2021 року трактує інформаційні загрози як потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні [2].

В. В. Антонюк трактує загрозу інформаційній безпеці наступним чином: це умови та фактори, існування яких здатне спричинити порушення параметрів інформації (включаючи інформацію, що присутня в інформаційних системах), які використовуються для задоволення інтересів громадян, громадянського суспільства, людей, органів та організацій, що здійснюють комерційну діяльність, державного управління [3].

Таким чином, можемо підсумувати, що загрози інформаційній безпеці – це потенційні небезпечні події або фактори, які можуть ставити під загрозу як конфіденційність, цілісність доступність інформації, так і національну безпеку держави загалом.

В науковій літературі представлена велика кількість класифікацій загроз інформаційній безпеці за різними ознаками. Наприклад, О. М. Шевчук пропонує класифікацію загроз інформаційній безпеці за походженням джерела загроз: антропогенні, техногенні, стихійні [4, с. 155]. А. В. Войціховський класифікує загрози інформаційній безпеці за цілями впливу: загрози конфіденційності інформації, цілісності інформації, доступність інформації, витік інформації, незаконний вплив на інформацію [5, с. 18].

Т. Ткачук наводить таку типологію загроз національній безпеці у світовому інформаційному просторі: – за місцем розташування джерела загрози: внутрішні джерела (національна інформаційна сфера) та зовнішні джерела (глобальний інформаційний простір); – за компонентами інформаційної сфери: інформаційно-політичні, інформаційно-технологічні та інформаційно-психологічні компоненти; – за характером руйнівної дії: явні, приховані і комбіновані; – за масштабом прояву: місцеві, регіональні, національні та глобальні [6, с. 184].

О. А. Ніщименко виділяє класифікацію загроз забезпеченню інформаційної безпеки за способом впливу:

– інформаційні способи, що являють собою не дозволений доступ до інформації з метою її викрадення, спотворення, видалення тощо;

– програмно-математичні способи досягаються за допомогою установки в програмно-апаратних системах, засобів обробки інформації, засобів забезпечення безпеки інформації від прихованого обладнання або компонентів, які виконують функції, не описані у відповідній документації на це обладнання, і які допомагають поширювати вірусні програми, які здатні нанести шкоду інформаційним ресурсам;

– фізичні методи – прямий вплив на інформаційні системи, засоби обробки та захисту інформації, пов'язані із фізичним пошкодженням, викраденням та видаленням інформаційних ресурсів;

– організаційно-правові методи забезпечують, насамперед, слабкий розвиток нормативної бази у сфері інформаційної безпеки, а також недотримання законодавчих вимог, перешкоди при прийнятті нормативно-правових актів у галузі інформації; закупівлю та використання застарілого обладнання та засобів захисту інформації; незаконне обмеження доступу громадян до інформації [7, с. 18–19].

Окремі дослідники серед основних небезпек розглядають можливість використання інформаційних технологій для необґрунтованих вторгнень у духовно-моральну сферу людей та соціальних організацій. Банки даних, які накопичують інформацію про здоров'я, працю, підприємницьку діяльність, рахунки у фінансових установах, є потенційною загрозою вторгнення у приватне життя громадян. І вважають, що ніхто не має права застосовувати комп'ютер та науку, щоб знищити духовне життя людини і людства загалом. Як засіб вирішення цих проблем вчені вказують на вкорінення демократичних ідей та цінностей, захист громадян державою, постійну діяльність щодо попередження злочинних вторгнень в галузі інформації із застосуванням комп'ютерних технологій [8, с. 35].

В державному аспекті загрози та виклики інформаційній безпеці розписані у Стратегії інформаційної безпеки та поділені на дві групи: глобальні та національні. Отже, глобальними викликами та загрозами загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

– збільшення кількості глобальних дезінформаційних кампаній;

– інформаційна політика російської федерації – загроза не лише для України, але й для інших демократичних держав;

– соціальні мережі як суб'єкти впливу в інформаційному просторі;

– недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій.

До національних викликів та загроз відносяться:

– інформаційний вплив російської федерації як держави-агресора на населення України;

– інформаційне домінування російської федерації як держави-агресора на тимчасово окупованих територіях України;

– обмежені можливості реагувати на дезінформаційні кампанії;

– несформованість системи стратегічних комунікацій;

– недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів;

– спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України;

– доступ до інформації на місцевому рівні;

– недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам [2].

Вважаємо, що до числа загроз можна додати і той факт, що зарубіжні країни давно здійснили стрімкий розвиток можливостей інформаційно-технічного впливу на інформаційну структуру, тоді, коли українська інформаційна інфраструктура в значній мірі залежить від зарубіжних інформаційних технологій.

Як випливає зі Стратегії інформаційної безпеки, велика кількість загроз і викликів безпосередньо або опосередковано пов'язана із діяльністю країни-агресора. Військово-політичні цілі російської федерації досягаються за допомогою інформаційного протиборства з використанням психологічних операцій і активних інформаційних заходів. Інформаційна безпека суспільства повинна забезпечувати безпеку індивідуальної, групової і масової свідомості громадян в рамках інформаційних загроз, які виражаються в інформаційно-психологічному впливі. Сьогодні державою-агресором активно використовуються

спеціальні методи, способи і засоби маніпулювання суспільною свідомістю, а також поглядами, цільовими установками і поведінковими стереотипами різних соціальних груп, розділених за етнічною, національною, конфесійною чи іншою ознакою, що веде до дестабілізації внутрішньополітичної та соціальної ситуації, підриву суверенітету і територіальної цілісності України.

Новітні інформаційні технології різко підвищили ефективність засобів впливу на психічний стан особистості і суспільства. Подальший розвиток інформаційно-комунікаційних технологій лише розширить можливості засобів масової інформації. У зв'язку з цим досить актуальним є розвиток міждисциплінарного напрямку – інформаційно-психологічна безпека. Активно розвиваються засоби і форми не відкритого маніпулювання індивідуальною і груповою свідомістю. До числа таких форм можна віднести нові технології засобів масової інформації, мереживні технології та багато іншого, за допомогою якого можна отримувати доступ до інформації різного негативного характеру. На цьому наголошують Ю. Кучеренко, О. Александров, А. Носик, Д. Камак і вважають, що в методологічному аспекті інформаційну безпеку можливо представити двома складовими: інформаційно-психологічною та інформаційно-технічною, що направлені на захист інформаційної сфери та населення держави від дії інформаційних сил і засобів інших країн (організацій, груп). Інформаційно-психологічна безпека визначає стан захищеності громадян, окремих груп та населення країни від негативних інформаційно-психологічних впливів. Інформаційно-технічна безпека визначає стан захищеності інформаційно-технічного середовища від програмних, силових, розвідувальних, радіоелектронних та інших впливів, що направлені на знищення, спотворення (втрату) інформації, вивід з ладу інформаційно-технічних об'єктів, інформаційної інфраструктури держави, включаючи систему державного та воєнного управління [9, с. 103].

На даний момент засоби масової інформації є цілодобовим джерелом отримання будь-якого роду інформації. Населення країни отримує відомості про процеси, що відбуваються в країні і світі, в різних сферах. Не завжди інформація, що висвітлюється є достовірною та повною. В більшості випадків російські засоби масової інформації подають інформацію про події в Україні у викривленому стані, що негативно позначається на сприйнятті реальної ситуації в державі та створення негативного образу України у свідомості громадян [10, с. 137]. Як влучно зазначає І. Б. Котерлін, «інформація є зброєю «масового ураження» [11, с. 154], саме тому система захисту інформаційної сфери повинна бути адаптована до сучасних загроз з тим, щоб мінімізувати деструктивні інформаційні впливи.

У світлі напруженої міжнародної обстановки інформація про політику окремих держав також висвітлюється російськими засобами масової інформації спотворено, що позначається на взаємовідносинах між конкретними державами. Разом з тим, будь-які, навіть обґрунтовані і доведені свідчення, про хакерські атаки російської федерації на інформаційні системи окремих країн світу, державою-агресором категорично відкидаються.

Сучасні можливості інформаційно-комунікаційних технологій виводять засоби масової інформації на перший план як стратегічний елемент здійснення впливу лідируючих країн на міжнародну громадськість і розв'язання інформаційних війн.

Спеціальні служби держави-агресора здійснюють збір інформації, проводять заходи, спрямовані на здобуття відомостей, що становлять державну таємницю, а також наукових розробок. Комп'ютерна розвідка з використанням програмних закладок в технічні засоби, спеціальних програмних засобів доступу і сканерів мереж забезпечує несанкціонований доступ до баз даних і до інформаційної системи, в тому числі в обхід малоефективних засобів захисту, а також перехоплення трафіку інформаційно-телекомунікаційних мереж для отримання повідомлень, що передаються. До традиційних завдань цього виду розвідки відноситься здобування інформації про економічний, військово-технічний, науковий потенціал нашої країни. Можливості комп'ютерної розвідки доповнюються іншими глобальними розвідувальними системами, які переорієнтовуються на вирішення нових завдань [12, с. 122–123].

Суттєвого негативного впливу на інформаційну безпеку додає широке використання терористичними і екстремістськими організаціями світових інформаційних ресурсів і механізмів інформаційного впливу для поширення ідеології тероризму, нагнітання міжнаціональної і соціальної напруженості і т. д. Діяльність терористів також перемістилася в інформаційний простір, дане напрямок названо «інформаційний тероризм», або «кібертероризм». Інформаційний тероризм грунтується, в першу чергу, на використанні інформаційних технологій.

Поняття кібертерроризму було введено в науковий обіг в середині вісімдесятих років минулого століття Б. Коліном, співробітником Інституту безпеки і розвідки (США). Зазначеним терміном були позначені прояви терористичного характеру в рамках віртуального простору. Дане поняття застосовувалося при прогнозуванні можливих майбутніх ситуацій. Б. Колін вважав, що виникнення реальних проявів кібертероризму відбудеться лише в першій третині XXI століття [13].

Інформаційний вплив почав використовувати нові способи і механізми на технічні та віртуальні системи. Треба зауважити, що активізувалися процеси застосування і поширення інформаційної зброї, тому виникає загроза інформаційних війн та інформаційного тероризму, як якісно нового типу впливу на геополітичну обстановку. Основною метою застосування інформаційної зброї є порушення функціонування інформаційної структури суспільства, підрив авторитету органів державної влади та недовіра до політики, що проводить держава.

Новою загрозою інформаційної безпеки України є загроза комп'ютерних атак на промислову сферу. Зросла кількість комп'ютерних атак (хакерських операцій) на інформаційні мережі, інформаційні державні системи та інформаційні системи персональних даних, кредитно-фінансову сферу. В органах влади досі здійснюється функціонування зарубіжного програмного забезпечення, засобів і систем обробки інформації. У зв'язку з цим можна відзначити гостру необхідність постійного оновлення систем забезпечення інформаційної безпеки, а також розвитку вітчизняної продукції і програмного забезпечення [14].

Створення, використання та розповсюдження вірусів і програм, які можуть знищити систему, пошкодити її, незаконно знищити, блокувати або змінювати інформацію є також досить актуальною проблемою в сучасному суспільстві. Діяльність хакерів, які можуть знаходитися в будь-якій точці світу, може завдати значної шкоди економіці будь-якої країни, підірвати авторитет керівництва держави, через розповсюдження листування, телефонних розмов тощо. Варто згадати одну з найпотужніших і небезпечних кібератак, яка трапилася в Україні влітку 2017 році, коли на декілька банків та підприємств (Укрпошта, Нова Пошта) було здійснено хакерську атаку та несанкціоноване втручання в операційні системи за допомогою комп'ютерного вірусу. Це відчули і клієнти банків та підприємств, які в цей час не змогли скористатися їхніми послугами. Під час війни кібератаки посилились у сфері публічного адміністрування і об'єктами атак часто стають офіційні сайти державних установ.

Однією з проблем інформаційної безпеки, на думку Н. С. Грабар, є кіберзлочини на внутрішньому ринку. Значної шкоди завдають комп'ютерні злочини, спрямовані на мережі банків і кредитних організацій. Основною метою зловмисників є не самі банки, а їх клієнти, і злочинець може викорис-

товувати їх некомпетентність, придбати дані в корисливих цілях. Загрози також можуть виходити і від персоналу організації або фірми. Наприклад, у деяких організаціях у співробітників є доступ до Інтернету для виконання своїх посадових обов'язків, але працівник використовує глобальну мережу в особистих цілях і запускає на робочому комп'ютері файли, які згодом ведуть до збитків. Серед основних цілей захисту України від інформаційно-психологічних загроз можна назвати захист від руйнівних інформаційних впливів суспільства і соціальних груп громадян, відстоювання національних інтересів і цілей України в інформаційному просторі, а також протидію спробам маніпулювання за рахунок інформації з боку ворожих Україні політичних сил [15, с. 170].

Висновки. Процес прогнозування та аналізу всього спектру загроз національній безпеці, як ніколи, набув особливої актуальності. Державна інформаційна політика повинна здійснюватися послідовно з урахуванням національних інтересів нашої держави, постійно мінливих умов та нових загроз інформаційній безпеці, які походять як зі зовнішнього інформаційного простору, так і обумовлені внутрішньодержавними обставинами. Лише за наявності державного підходу до вирішення проблеми охорони та захисту інформації в інформаційних системах, телекомунікаційних мережах можна створити умови для адекватної протидії збільшенню загроз в інформаційному полі. В першу чергу це передбачає вдосконалення національної інформаційної інфраструктури, включаючи електронні засоби масової інформації, банківські системи, системи зв'язку, транспорт, енергетику, промисловість та сферу послуг. Крім того, ця інфраструктура доповнюється Інтернетом, який постійно розширює нові можливості, які несуть нові загрози та виклики.

Розробка державної політики у сфері забезпечення інформаційної безпеки, що відповідає ситуації внутрішньої та зовнішньої політики, а також організації процесів державного регулювання видається складним і нагальним завданням для негайного вирішення відповідними державними органами.

ЛІТЕРАТУРА

1. Артемов В. Ю., Хорошко В. О., Хохлачова Ю. Є., Погорелов В. В. Інформайційно-воєнна безпека як елемент національної безпеки України. *Захист інформації*. 2022. Т. 24, № 1. С. 21–29.
2. Стратегія інформаційної безпеки від 28 грудня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7.
3. Антонюк В.В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці. *Державне управління: удосконалення та розвиток*. 2014. № 8. С. 22–27.
4. Шевчук О.М. Адміністративно-правове регулювання у сфері забезпечення інформаційної безпеки: дис. …канд. юрид. наук : спец. 12.00.07. Київ, 2011. 210 с.
5. Войціховський А. В. Питання інформаційної безпеки України на сучасному етапі. *Право і безпека*. 2015. № 3 (58). С. 15–20.
6. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182–186.
7. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. № 1. С. 17–23.
8. Бортник Н. П., Пєтков С. В. Загрози інформаційному ресурсу держави в контексті інформаційної та національної безпеки. *ІТ право: проблеми і перспективи розвитку в Україні*: збірник матеріалів науково-практичної конференції (Львів, 18 листопада 2016 р). Львів, 2016. С. 34–36.
9. Кучеренко Ю. Ф., Александров О. В., Носик А. М., Камак Д. О. Методологічні основи інформаційної безпеки країни з урахуванням умов сучасного періоду її державотворення. *Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*. 2022. Вип. 4 (14). С. 99–109.
10. Мосов С. П., Уханова Н. С. Протидія негативним інформаційним впливам на людину і суспільство в умовах гібридної війни. *Інформація і право*. 2018. № 2 (25). С. 134–141.
11. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. Актуальні проблеми вітчизняної юриспруденції 2022. № 1. С. 150–155.
12. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту: дис. … канд. політичних наук: 23.00.04. Київ, 2018. 210 с.
13. Климчук О. Інформаційна та кібербезпека в сучасному світі: досвід СБУ. 12.07.2018. Ліга net. URL: http://ua.news.liga.net/politics/opinion/informatsiyna-ta-kiberbezpeka-vsuchasnomu – sviti-dosvid-sbu.
14. Дмитренко М. А. Проблемні питання інформаційної безпеки України. 2018. URL: journals.iir.kiev.ua/index.php/pol_n/article/download/3318/2997.
15. Грабар Н.С. Механізми інформаційної безпеки України в умовах інформаційного глобалізму. *Право та державне управління*. 2019. № 7. С. 168–73.