МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА

Правові горизонти

Legal horizons

ВИПУСК 13 (26)

Суми – 2018

DOI: http://www.doi.org/10.21272/legalhorizons.2018.i13.p79

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ВИКЛИКИ СЬОГОДЕННЯ

Чернадчук Олександр Вікторович,
кандидат юридичних наук, старший викладач кафедри кримінально-правових дисциплін та судочинства,
Навчально-науковий інститут права,
Сумський державний університет

Стаття присвячена аналізу поглядів на проблеми реалізації державної політики у сфері інформаційної безпеки держави. Доведено, що інформаційна безпека є складовою як національної безпеки в цілому, так і ключовим елементом безпеки в різних сферах життєдіяльності суспільства (політики, економіки, науки, освіти, військового управління та ін.). Аналіз поглядів науковців різних галузей знань дозволив визначити інформаційну безпеку як стан, вид діяльності або процес.

Наведено основні причини низької ефективності системи забезпечення інформаційної безпеки. У статті також висвітлено переліки загроз інформаційній безпеці, які передбачені стратегічними нормативно-правовими актами, а саме в Стратегії національної безпеки України (2015), Доктрині інформаційної безпеки України (2017), Законі України «Про національну безпеку» (2018). Висвітлено також науково-теоретичні підходи до переліку загроз інформаційній безпеці України.

Окрему увагу приділено переліку та повноваженням суб'єктів забезпечення інформаційної безпеки, що є актуальним з огляду на виклики та загрози, які постають перед державою в умовах реформ всіх сфер діяльності суспільства, обраного євроінтеграційного вектору, гібридної війни тощо. Визначено суб'єктів формування та реалізації політики інформаційної безпеки. Наведено класифікацію суб'єктів забезпечення інформаційної безпеки, запропонованої в проекті Концепції інформаційної безпеки України 2015 року. Доцільним вбачається додати до переліку суб'єктів забезпечення інформаційної безпеки міжнародні міжурядові та міжнародні неурядові організації, діяльність яких спрямована на забезпечення міжнародної інформаційної безпеки.

Ключові слова: національна безпека, інформаційна безпека, загрози інформаційній безпеці, суб'єкти забезпечення інформаційної безпеки, інформаційний суверенітет.

Chernadchuk O.V. Providing information security: challenges of the contemporaneity. The article is devoted to the analysis of the views on the problems of implementing state policy in the field of state information security. It is proved that information security is an integral part of both national security as a whole and a key element of security in various spheres of society's life (politics, economics, science, education, military management, etc.). An analysis of the views of scholars from different fields of knowledge has allowed the identification of information security as a status, type of activity or process.

The main reasons for the low efficiency of the information security system are presented. The article also lists the threats to information security that are provided by strategic regulatory acts, namely, the National Security Strategy of Ukraine (2015), the Doctrine of Information Security of Ukraine (2017), the Law of Ukraine "On National Security" (2018). The scientific-theoretical approaches to the list of threats to the information security of Ukraine are also covered.

Particular attention is paid to the list and authority of the subjects of ensuring information security, which is relevant in view of the challenges and threats faced by the state in the context of reforms in all spheres of society, chosen European integration vector, hybrid war, etc. The subjects of formation and implementation of the information security policy are determined. The classification of subjects

providing information security proposed in the draft Concept of Information Security of Ukraine 2015 is given. It is expedient to add international intergovernmental and international non-governmental organizations, whose activities are aimed at ensuring international information security, to be added to the list of subjects of information security.

Key words: national security, information security, threats to information security, subjects of information security, information sovereignty.

Постановка проблеми. Науковці, практичні працівники та законодавці все більше приділяють уваги правовому та організаційному забезпеченню інформаційної безпеки України. У 2015-2018 рр. було прийнято ряд стратегічних документів державного значення, які направлені на врегулювання безпеки в інформаційній сфері з метою досягнення максимального рівня національної безпеки.

Наявна ситуація в світовому інформаційному просторі характеризується наступним: більшість країн світу зіштовхнулася з проблемами кібертероризму, кіберзлочинності та іншими проблемами інформаційної безпеки; протягом останніх десятиліть спостерігається тенденція до поширення інформаційної агресії і насилля; набувають поширення агресивна реклама, спроби маніпуляції свідомістю людини, періодично проводяться інформаційно-психологічні операції; майже у 120 країнах світу (за оцінками американських експертів) ведуться розробки інформаційної зброї або її елементів (для порівняння – розробки зброї масового знищення здійснюються у близько 20 країнах); наслідки використання сучасної інформаційної зброї (згідно з висновками вчених та експертів європейських країн, України, РФ і США) можуть бути зіставленими із застосуванням зброї масового ураження; новітні виклики і загрози в інформаційній сфері становлять реальну загрозу безпеці людства та міжнародному правопорядку [1].

2017 та 2018 роки стали періодом позитивних кроків в питанні утвердження засад інформаційної безпеки та інформаційного суверенітету держави.

Прийняття у 2017 році Доктрини інформаційної безпеки України стало фундаментом, на якому держава змогла почати перебудовувати свою діяльність у цій царині на базі підпорядкованості єдиному стратегічному задуму та узгодженості дій різних органів державної влади. Водночас залишається значна кількість стратегічних викликів та загроз у сфері інформаційної безпеки, які потребують першочергового вирішення [2].

Аналіз останніх досліджень і публікацій. Теоретико-правові основи інформаційної безпеки держави взагалі та в окремих органах виконавчої влади, зокрема, були предметом наукових досліджень В. Б. Авер'янова, А. Б. Агапова, О. М. Адрєєвої, І. В. Арістової, О. М. Бандурки, І. Р. Березовської, Р. А. Калюжний, Б. А. Кормича, В. А. Ліпкан, Г. М. Линник, О. В. Логінова, Ю. Є. Максименко, О. В. Олійника, В. М. Петрик, Т. В. Субіної, В. М. Супрун, О. О. Тихомирова та ін.

Цілі і завдання. Метою статті є аналіз поглядів на реалізацію державної політики у сфері інформаційної безпеки держави, загрози інформаційній безпеці, характеристику суб'єктів забезпечення інформаційної безпеки.

Виклад основного матеріалу. Інформаційна безпека України тісно пов'язана з національною, регіональною та глобальною безпекою. Особливо актуальними питання інформаційної безпеки і її нормативно-правового регулювання є для пострадянських країн, громадяни яких після тривалої ізоляції у закритому суспільстві стикнулися з раніше не відомими їм викликами сучасного світового інформаційного простору, причому не лише позитивними, а й негативними. На тлі несформованого «інформаційного імунітету» такі негативні чинники створюють «непрозорі», зрозумілі лише експертам у відповідних галузях, загрози маніпулювання індивідуальною й масовою свідомістю. Варто також зауважити, що пострадянські країни поки що виступають у ролі не стільки суб'єктів, скільки об'єктів інформаційних впливів через відставання у сфері сучасних інформаційних технологій. Останнє ставить під сумнів не тільки їхнє входження до числа постіндустріальних (інформаційних) суспільств, а й ефективний захист власних інформаційних ресурсів [3].

Інформаційна безпека є не лише складовою національної, але й невід'ємною складовою економічної, екологічної, соціальної, оборонної, політичної безпеки. Інформаційна безпека є багатогранним соціальним «явищем», «станом», «видом діяльності», здійснюється на міжнародному, національному та галузевому рівнях, одночасно являючись стратегічно важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності держави, суспільства і особи в інформаційній сфері від зовнішніх та внутрішніх загроз [4].

Безсумнівним є твердження, що інформаційна безпека є елементом національної безпеки і тісно пов'язана з політичною, економічною, науковою, освітньою, військовою, правоохоронною та іншими сферами життєдіяльності суспільства. Дійсно, науковці визначають її як стан, вид діяльності або процес.

Системний характер інформаційної безпеки дозволяє визначити її забезпечення як складний, комплексний вид діяльності, що висуває особливі вимоги до його структурної характеристики. Ґрунтуючись на цьому, забезпечення інформаційної безпеки доцільно розглядати як цілеспрямовану діяльність, провідним, але не єдиним елементом об'єктно-суб'єктного складу якої є держава [5]. Отже, О.О. Тихомиров визначає інформаційну безпеку як вид діяльності.

Розглядаючи інформаційну безпеку з філософської точки зору дослідник Триняк В.Ю. розкриває подвійну сутність інформаційної безпеки: як стан та як процес. Інформаційна безпека, на думку Триняка В.Ю.:

- це стан захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері від внутрішніх та зовнішніх загроз, що забезпечує стійкий розвиток, а також стан стабільності основних сфер життєдіяльності (політики, економіки, науки, сфери державного управління, військової справи тощо) стосовно небезпечних інформаційних впливів (як упровадження, так і вилучення інформації);

- процес, оскільки вона є невід'ємною частиною соціокультурного життя суспільства, в якому діють політична влада, суспільно-політичні сили і течії, особи, соціальні групи, рухомі економічними та соціально-політичними потребами, інтересами і цілями [5].

Процесам, що відбуваються в глобальному інформаційному просторі, притаманні певні тенденції та особливості, які Довгань О.М. характеризує наступним чином: по-перше, уроки інформаційної агресії, які пережила і переживає Україна, змінюють традиційні уявлення про символи могутності й способи досягнення світового панування. .... По-друге, як показує практика, інформаційна перевага надає можливість випередити суперника у прийнятті рішень, у тому числі військово-політичних, і є запорукою успіху у воєнних діях. Оскільки, як зазначалося вище, завдяки глобальному розвитку в перспективі виникне нове протистояння у світі за контроль над інформаційним простором і «транспортуванням інформації», що в свою чергу порушить проблему будівництва нової системи європейської та міжнародної безпеки. По-третє, самі по собі геополітичні трансформації нинішнього століття зумовлюють характер відносин співробітництва і протиборства. Однією із головних сфер такого суперництва виступатиме інформаційний простір на різних його рівнях (глобальному, регіональному, можливо, субрегіональному і національному). В умовах інформаційної глобалізації жодна держава світу, незалежно від рівня економічного, воєнного чи інформаційного потенціалу, нездатна самостійно забезпечити власну інформаційну безпеку. По-четверте, володіння інформаційними ресурсами стає одним із головних факторів геополітичної конкуренції. Формування глобальної інформаційної інфраструктури на основі мережі Інтернет може привести до посилення просторової взаємозалежності держав. ... По-п'яте, у різних країнах світу активно розробляються технології та психологічні засоби ведення інформаційної війни й інформаційного протиборства, спрямовані на використання інформації проти людського інтелекту. І насамкінець, по-шосте, поряд із відомими засобами впливу (дезінформація, чутки, пропаганда, агітація, міфи тощо) на перший план виходять засоби одержання й доставки інформації. Це насамперед системи глобального телерадіомовлення, за допомогою яких реальні події з відповідними коментарями та спеціально підібрані факти й аргументи стають доступними аудиторії в багатьох країнах світу [6].

До основних причин низької ефективності системи забезпечення інформаційної безпеки відносять:

1. високу корумпованість та недостатній фаховий рівень керівників державних суб'єктів згаданої системи;

2. відсутність суспільного консенсусу з ключових питань державного будівництва, а також належної взаємодії та координації дій між органами виконавчої влади і силовими структурами, в тому числі при проведенні комплексного огляду сектору безпеки і оборони;

3. виконання окремими органами державної влади невластивих для них функцій, дублювання їхніх повноважень, розпорошення сил та засобів, відсутність їх консолідації;

4. невідповідність правового регулювання дій суб'єктів забезпечення національної безпеки особливостям ситуації у безпековій сфері;

5. незадовільні якість та рівень ресурсного забезпечення суб'єктів системи забезпечення національної безпеки [7].

Розглянемо погляди законодавця на загрози інформаційній безпеці України. Адже виходячи із загроз формується державна політика забезпечення інформаційної безпеки України та напрями її реалізації.

Стратегією національної безпеки України (2015) загрозами інформаційній безпеці України визначено ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства (п. 3.6) [8].

У Законі України «Про національну безпеку» (2018) [9] натомість не конкретизовано загрози інформаційній безпеці, а лише узагальнено загрозами визнано явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України. Крім того, в новому законодавчому акті з питань забезпечення національної безпеки визначено, що державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо, а загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України.

Доктрина інформаційної безпеки України виділяє як одну з актуальних загроз національним інтересам та національній безпеці України в інформаційній сфері проблему поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні. Упродовж останнього року ці тенденції місцями посилювались, часто – за прямої чи опосередкованої інформаційної, політичної, фінансової підтримки агресора. Ця проблема потребує постійної уваги та системного моніторингу регіональних інформаційних загроз, одним із завдань якого є визначення рівня загроз політичній стабільності регіону, а також оцінка впливу третіх сторін на посилення цих загроз [2].

Доктриною інформаційної безпеки (2017 рік) [10] наведено дещо розширений перелік актуальних загроз національним інтересам та національній безпеці України в інформаційній сфері, а саме: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні; проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах; інформаційне домінування держави-агресора на тимчасово окупованих територіях; недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України; неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Поряд з поглядами законодавця, вважаємо за доцільне звернутися до науково-теоретичних підходів до загроз інформаційній безпеці України.

Триняк В.Ю. розглядаючи інформаційну безпека як соціокультурний феномен виділяє зовнішні та внутрішні загрози інформаційній безпеці України. До зовнішніх загроз найбільшу небезпеку представляють: інформаційний вплив іноземних політичних, економічних, військових та інформаційних структур на розробку і реалізацію стратегії зовнішньої політики України; поширення за кордоном дезінформації про зовнішню політику України; порушення прав громадян України і юридичних осіб в інформаційній сфері за кордоном; спроби несанкціонованого доступу до інформації і впливу на інформаційні ресурси, інформаційну інфраструктуру органів державної влади, що реалізують зовнішню політику України, українських представництв і організацій за кордоном, представництв України при міжнародних організаціях. Основними внутрішніми загрозами інформаційній безпеці України є: корупція; порушення з боку органів державної влади та органів місцевого самоврядування Конституції й законів держави, прав і свобод людини й громадянина; перевага в діяльності управлінських структур особистих, корпоративних, регіональних інтересів над загальнонаціональними; вияви моральної та духовної деградації суспільства; науково-технологічне відставання від розвинених країн; нерозвиненість внутрішнього ринку

високотехнологічної продукції та відсутність його ефективного захисту від іноземної технічної і технологічної експансії; від'їзд учених, фахівців, кваліфікованої робочої сили за межі країни; вияви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; прагнення маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [6].

Заслуговує на увагу більш конкретизований підхід на ключові загрози в інформаційній сфері, сформульований Власюком О.С.: 1. Проведення інформаційних спецоперацій з метою формування негативного міжнародного іміджу України. 2. У зв'язку з посиленням уваги у всьому світі до забезпечення кібербезпеки держави, що не в останню чергу пов'язано з активізацією хакерської діяльності з боку Росії та Китаю, вбачається доцільним зосередження діяльності на протидії новітнім засобам ведення наступальної та оборонної кібервійни. 3. В Україні, судячи з матеріалів відкритої преси, "вузьким місцем" є аналітична підготовка співробітників у сфері автоматизації процесів збору інформації та необхідності її аналітичного згортання. 4. У зв'язку з певним загостренням українсько-російських та українсько-румунських відносин у рік президентських виборів в Україні та постійним впливом з боку Росії та Румунії на інформаційний простір України, на особливу увагу заслуговує питання моніторингу відповідних Інтернет-сайтів, соціальних мереж, форумів, чатів тощо з яскраво вираженою проросійською та прорумунською тематикою.

Вважаємо за доцільне приділити увагу переліку та повноваженням суб'єктів забезпечення інформаційної безпеки, що є актуальним з огляду на виклики та загрози, які постають перед державою в умовах реформ всіх сфер діяльності суспільства, обраного євроінтеграційного вектору, гібридної війни тощо.

Суб'єкт забезпечення безпеки – одна з основних категорій, що використовується для розкриття змісту системи забезпечення як національної, так і інформаційної безпеки. Традиційно йому приділяється багато уваги на нормативно-правовому рівні, загальнотеоретичні аспекти державного забезпечення інформаційної безпеки оскільки саме право в сучасній правовій державі є засобом визначення повноважень суб'єктів державної діяльності та окреслення сфери їх компетенції [5].

Усі суб'єкти забезпечення національної безпеки є одночасно суб'єктами забезпечення інформаційної безпеки та формально поділяються на державні та недержавні.

У юридичній літературі зустрічається визначення системи органів державної влади у сфері національної інформаційної безпеки як сукупність взаємовідносин суб'єктів державного управління (органів державної влади), які проводять державно-управлінську діяльність на основі розмежування компетенції між ними щодо об'єктів державного управління (сфери суспільного життя) з метою гарантування конституційних прав та свобод людини і громадянина, розвитку громадянського суспільства та захищеності інформаційного суверенітету держави [12, с. 29], та яка включає в себе дві складові: систему органів законодавчої влади, що здійснюють функцію нормативно-правового регулювання загальнодержавного керівництва у сфері забезпечення інформаційної безпеки, та систему органів виконавчої влади, які виконують функцію часткового формування у межах наданих повноважень та реалізації державної політики інформаційної безпеки у сучасних умовах [13].

В свою чергу дослідник М. Б. Левицька дає наступну класифікацію суб'єктам забезпечення інформаційної безпеки: 1) суб'єкти, діяльність яких безпосередньо підпорядкована завданням забезпечення національної безпеки, як у комплексі, так і окремим із них (Рада національної безпеки й оборони України, правоохоронні та інші державні виконавчі органи спеціальної компетенції); 2) суб'єкти, для яких така діяльність є одним з основних, але не єдиним напрямом (вищі органи законодавчої, виконавчої та державної влади); 3) суб'єкти, для яких участь у забезпеченні національної безпеки не є основною діяльністю (всі інші державні й громадські організації) [14].

Суб'єктам забезпечення інформаційної безпе¬ки відповідає окрема специфічна функція – функція розробки або функція реалізації політики інформац¬ійної безпеки. Функція розробки державної політики інформаційної безпеки включає в себе діяльність ком¬петентних органів держави щодо встановлення стра¬тегічних цілей, завдань, основних принципів та на¬прямів державної діяльності в цій сфері, розробку концепцій та рішень загальнодержавного довгостро¬кового значення. Функція реалізації політики інфор¬маційної безпеки спрямована на досягнення тактич¬них та оперативних цілей, забезпечує вирішення кон¬кретних завдань, застосування відповідних засобів, форм та методів державного впливу на суспільні відносини в цій сфері [15].

Функцію розробки державної політики інформаційної безпеки покладено на Президента України, Верховну Раду України, Раду національної безпеки і оборони, їх дорадчі та консультаційні органи та ін. Проте не варто забувати, що участь у розробці державної політики інформаційної безпеки можуть брати міністерства, органи виконавчої влади, а також громадяни, надаючи свої пропозиції у вигляді конкретних планів, заходів, концепцій, проектів або зауважень до вже існуючих.

Так, наприклад, сучасний підхід до класифікації суб'єктів забезпечення інформаційної безпеки запропоновано в проекті Концепції інформаційної безпеки України 2015 року [16], розробленої Міністерством інформаційної політики України. У концепції суб'єктів розподілено за суб'єкти забезпечення та суб'єктів реалізації державної політики в сфері інформаційної безпеки.

Суб'єктами забезпечення інформаційної безпеки проекті концепції визначено:

1. громадян України, об'єднання громадян, громадські організації та інші інститути громадянського суспільства;

2. Президент України, Верховна Рада України, Кабінет Міністрів України, інші центральні органи виконавчої влади та органи сектору безпеки і оборони України;

3. засоби масової інформації та комунікації різних форм власності, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність;

4. наукові установи, освітні і навчальні заклади України, які, зокрема, здійснюють наукові дослідження та підготовку фахівців за різними напрямами інформаційної діяльності, в галузі інформаційної безпеки.

Крім того, у проекті концепції конкретизовано суб'єктів реалізації державної політики в сфері інформаційної безпеки, та визначено, що такими суб'єктами є: Служба безпеки України; Міністерство внутрішніх справ України; Міністерство оборони України; Служба зовнішньої розвідки України; Центральний орган виконавчої влади із спеціальним статусом, який забезпечує формування та реалізує державну політику у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій і користування радіочастотним ресурсом України.

Висновки. Варто звернути увагу на позитивні та стратегічно важливі норми, передбачені проектом Концепції інформаційної безпеки України 2015 року. Так, на концептуальному рівні здійснюється спроба закріпити поняття інформаційної безпеки, національного інформаційного простору, визначено основи державної політики у сфері інформаційної безпеки, здійснення громадського контролю та державно-громадське партнерство в сфері реалізації державної інформаційної політики та забезпечення інформаційної безпеки.

Доцільним, на нашу думку, додати до вказаного переліку міжнародні міжурядові та міжнародні неурядові організації, діяльність яких спрямована на забезпечення міжнародної інформаційної безпеки, а саме її вій¬ськового, терористичного і кримінального аспектів. Це зумовлено тим, що рішення та рекомендації міжнародних організацій (Європейський Союз (ЄС); Організацію Об'єднаних Націй (ООН); Організацію Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО); Шанхайську організацію співробітництва (ШОС); Євразійське економічне співтовариство (ЄврАзЕС); Північноатлантичний Альянс (НАТО); Співдружність Незалежності Держав (СНД); Рада Європи; Організації економічного співробітництва і розвитку (ОЕСР) та ін.) відіграють важливу роль у формуванні національної правової доктрини та безпосередньо у формуванні системи забезпечення інформаційної безпеки як державного та світового масштабу.

Література :

1. Пилипчук В.Г. Системні правові проблеми формування інформаційного суспільства : зб. наук. ст. та тез ; "Інформаційне суспільство і держава : проблеми взаємодії на сучасному етапі". Х. : НДІ державного будівництва та місцевого самоврядування, 2012. С. 3-7

2. Офіційний сайт Національного інституту стратегічних досліджень / Послання Президента України / Аналітична доповідь до щорічного послання Президента України до Верховної ради України «про внутрішнє та зовнішнє становище України в 2018 році / Наукові видання. URL : http://www.niss.gov.ua/public/File/analit_dopovid_POSLANNYA_2018_FINAL_Oct_02.pdf

3. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики : Вибр. наук. Праці. К. : НІСД, 2016. 528 с.

4. Косиця О.О. Інституціональний механізм системи інформаційної безпеки. Порівняльно-аналітичне право. 2016. № 4. С. 150-153

5. Тихомиров О. О. Класифікації забезпечення інформаційної безпеки / Вісник Запорізького національного університету. 2011. № 1. С. 164–168.

6. Триняк В.Ю. Інформаційна безпека як соціокультурний феномен : автореф. Канд.. філос. наук за спец. 09.00.03 – соціальна філософія та філософія історії. Дніпропетровськ. 2009, 22 с..

7. Концептуальні засади розвитку системи забезпечення національної безпеки України : аналіт. доп. / О. О. Резнікова, В. Ю. Цюкало, В. О. Паливода та ін. К. : НІСД, 2015. 58 с.

8. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року № 287/2015. URL : http://zakon.rada.gov.ua/laws/show/287/2015

9. Про національну безпеку: Закон України від 21 червня 2018 року

№ 2469-VIII. URL : http://zakon.rada.gov.ua/laws/show/2469-19

10. Про Доктрину інформаційної безпеки України: рішення Ради національної безпеки і оборони України від 29 грудня 2016 року, введене в дію Указом Президента України від 25 лютого 2017 року №47/2017. URL : https://www.president.gov.ua/documents/472017-21374

11. Максименко Ю.Є. Плюралізм загроз інформаційної безпеки України \ Імперативи розвитку цивілізації : Матеріали міжвідомчої науково-практичної конференції «Інформаційна безпека у воєнній сфері. Сучасний стан та перспективи розвитку» (Київ, 31 березня 2015 року). № 2. 2015. К. : ФОП О. С. Ліпкан, 2015. С.82-83

12. Взаємовідносини органів державної влади у сфері забезпечення інформаційної безпеки України: організаційно-правові питання / Вісник УАДУ: Наук. журн. 2002. № 3. С. 27-31

13. Березовська І.Р. Суб'єкти у сфері забезпечення інформаційної безпеки в Україні // Наукові записки Львівського університету бізнесу та права. 2013. Вип. 10. С. 148-153

14. Левицька М. Б. Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України : дис. … канд. юрид. наук : 12.00.01. К., 2002. 206 с.

15. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: дис. … доктора юрид. наук: спец. 12.00.07. Одеса, 2004. 427 с.

16. Концепція інформаційної безпеки України : проект // Міністерство інформаційної політики України. 2015. URL : http://mip.gov.ua/done_img/d/30-project_08_06_15. pdf.