УДК 351.88

Р. Ю. Прав,
аспірант, Міжрегіональна академія управління персоналом
ORCID ID: 0000-0001-8064-2836

DOI: 10.32702/2306-6814.2019.16.113

ІННОВАЦІЙНІ МЕТОДИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ПРОТИДІЇ ЗОВНІШНІМ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

R. Prav,
postgraduate student, Interregional Academy of Personnel Management

INNOVATIVE METHODS OF IMPLEMENTATION OF THE STATE POLICY FOR COUNTERACTING EXTERNAL INFORMATION THREATS

Статтю присвячено проблематиці дослідження інноваційних методів реалізації політики владних структур щодо протидії зовнішнім інформаційним загрозам. Досліджено питання сучасних інформаційних загроз та інформаційної безпеки України на сучасному етапі в рамках реалізації пріоритетних завдань державної політики забезпечення інформаційної безпеки. Виявлено особливості механізму протидії інформаційним загрозам зовнішніх джерел для забезпечення інформаційної безпеки України, наведено основні сучасні методи блокування деструктивних та стимулювання перспективних властивостей, процесів та явищ інформаційної безпеки України. Наведено методи протидії держави зовнішнім інформаційним загрозам. Наведено оперативні методи протидії зовнішнім інформаційним загрозам: 1) постійний та системний контроль вітчизняного інформаційного простору; 2) введення обмежень розмірів інформаційного простору для тих категорій населення та соціальних груп, які є найбільш вразливими до тієї чи іншої інформаційної загрози; 3) посилення авторитету та впливу власних владних структур; 4) вдалі заходи власної інформаційної політики; 5) забезпечення ефективного зворотного зв'язку з суспільством тощо.

The article is devoted to the problem of researching innovative methods for implementing the policy of governmental structures to counteract external information threats. Issues of modern information threats and information security of Ukraine at the present stage within the framework of realization of priority tasks of domestic and foreign state policy are investigated. The peculiarities of the mechanism of counteracting information threats from external sources for ensuring information security of Ukraine are revealed, the main modern methods of blocking destructive and stimulating perspective properties, processes and phenomena of information security of Ukraine are presented. The methods of counteraction of the state to external information threats are presented. The operative methods of counteracting external information threats are presented: 1) constant and systematic control of the domestic information space; 2) introducing restrictions on the size of the information space for those categories of population and social groups that are most vulnerable to a particular information threat; 3) strengthening the authority and influence of their own power structures; 4) successful measures of own information policy; 5) Ensure effective public feedback and more. Generally, there are many traditional and innovative methods of counteraction to external information threats at the state level today: methods of description and classification of information hazards; methods for investigating causal relationships (methods of divergence, similarity, accompanying changes and residuals); technical information security techniques based on the use of cryptographic approaches to ensure information security mode. The classification of information threats is given: at the location of the source of the danger; the magnitude of the likely consequences; by the degree of formation; by nature of occurrence; by the degree of subjective perception; by

sphere of activity. The analysis of the most relevant and relevant information threats to the life of the state so far shows that most of the threats, both internal and external, are interrelated, as well as the sources of their occurrence.

Ключові слова: інформаційні загрози, безпека, інформаційна безпека, інформація, методи, протидія.
Key words: information threats, security, information security, information, methods, counteraction.

ПОСТАНОВКА ПРОБЛЕМИ ТА ЇЇ ЗВ'ЯЗОК З ВАЖЛИВИМИ АКТУАЛЬНИМИ ЗАВДАННЯМИ

Тотальна зміна всіх сфер життєдіяльності сучасного суспільства, швидке розповсюдження інформації є сьогодні найвагомішим чинником динамічного політичного соціально-економічного, інтелектуального, культурного життя держави. Інформаційна сфера стала відігравати вкрай важливу роль у зв'язку з динамічністю розвитку інформаційної інфраструктури, розвитку інформаційно-комунікаційних технологій, поширення інформатизації бізнес-процесів, розвитком нових технологій та інновацій, у тому числі у секторі ІТ, загальним розвитком індустрії інформатизації. Звідси випливає, що питання інформаційної безпеки сьогодні набувають підвищеної значимості та актуальності. Інформаційна безпека є невід'ємною частиною національної безпеки, яка в умовах посилення зовнішніх інформаційних загроз, особливо в умовах ведення кібервійни в Україні та посиленням впливу інформаційних загроз, набуває виняткового значення. Саме державою затверджується та реалізовується державна політика, механізми протидії цим загрозам, які включають і впровадження оптимальних та ефективних методів, важелів та інструментів забезпечення інформаційної безпеки.

Питань аналізу державної політики в сфері протидії зовнішнім інформаційним загрозам та пошук інноваційних методів цієї протидії в своїх наукових дослідженнях торкалися відомі вітчизняні вчені: В. Антонюк, І. Арістова, О. Бандурка, В. Брижко, В. Бут, В. Горбулін, В. Домарєв, З. Живко, І. Івченко, Р. Калюжний, А. Качинський, О. Куцька, М. Литвин, В. Ліпкан, О. Орєхов, Г. Сащук, О. Снитко, Т. Ткачук, Г. Новицький, В. Пилипчук, М. Стрельбицький, Р. Хмелевський, В. Цимбалюк та інші. Проте вони переважно розглядали теоретичні питання розвитку сучасного інформаційного суспільства, правового регулювання інформаційної сфери, а також державної політики в сфері інформаційної безпеки. Варто зазначити, що сьогодні недостатньо опрацьованими є питання застосування сучасних методів протидії інформаційним загрозам, що й визначає необхідність подальших досліджень у цьому напрямку.

МЕТА ТА ЗАВДАННЯ СТАТТІ

Метою статті є здійснення грунтовного аналізу інноваційних методів реалізації політики держави в сфері протидії зовнішнім інформаційним загрозам та особливостей їх застосування в сучасних умовах.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

На сьогодні інформація, без перебільшення, є визначальним і найвагомішим ресурсом розвитку сучасного суспільства. Вона активно впливає на всі сфери життєдіяльності як окремих країн, так і всього світового співтовариства завдяки бурхливому розвитку ІКТ — інформаційно-комунікаційних технологій. Проте разом з корисними інтересами та спрямованістю інформація може використовуватися і на шкоду окремим індивідам, суспільству і державі. ІКТ стала найважливішим чинником сучасних світових інтеграційних процесів та найсильнішим каталізаторам інформаційного обміну, тому може нести і як явні, так і приховані загрози. Тому забезпечення інформаційної безпеки на міжнаціональному на національному рівні є надзвичайно важливим, оскільки рішення та механізми державного впливу в системі ІКТ безпосередньо впливають на подальші дії держави в зовнішній та внутрішній політиці.

У цьому контексті визначальним є поняття "інформаційна загроза". Яке визначається сучасними вченими як сукупність певних інформаційних чинників та негативних умов, які створюють небезпеку певному об'єкту, структурі або всьому суспільству. Як вважають В. Горбулін та Т. Ткачук, під такими загрозами слід розуміти певні родові ознаки небезпеки у вигляді можливості чи неминучості виникнення різнопланових соціо-технічних чи природних явищ чи неконтрольованих подій, які можуть статися в певний момент часу на певній території і можуть призвести до людських, економічних, фінансових втрат. Безпека ж визначається вченими як нульовий, початковий варіант небезпеки [5, с. 17].

Виняткову небезпечність загроз інформаційній безпеці держави підкреслює Г. Сащук: "...Ураховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд і мораль як окремих осіб, так і суспільства загалом, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності й форм виявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які суперечать інтересам національної безпеки..." [13].

Відповідно до цього інформаційні загрози можна класифікувати за різними підставами та підходами, що пояснює їх складну, різнопланову, багатоаспектну сутність та зміст. Так, основні види інформаційних загроз наведені в таблиці 1.

Проте деякі вчені виділяють свої власні класифікації інформаційних загроз. Так, В. Кохан і М. Литвин, вивчаючи проблематику інформаційної безпеки всередині держави, вирізняють загрози в політико-економічній, соціокультурній, військовій, екологічній, освітній, криміногенній та просвітницькій сферах, а також інформаційні загрози виникнення надзвичайних ситуацій природного, соціального та техногенного характеру [9]. В. Хусаінов, згоджуючись загалом з вищенаведеною класифікацією, вказує на трансформацію домінуючій загрозі світу та державі на велику кількість менших за масштабами потенційних загроз. А В. Ліпкан вважає, що саме джерела інформаційних загроз є зовнішніми та внутрішніми.

Традиційно вчені виділяють такі основні зовнішні джерела інформаційної небезпеки [3, с. 105]:

— негативні наслідки діяльності іноземних політико-економічних, військових, розвідувальних, інформаційних та ін. структур, які спрямовані проти національних інтересів України, а також ймовірного послаблення можливостей їх реалізації;

— діяльність або прагнення державних та приватних структур іноземних держав до ущемлення національних інтересів на міжнародній арені, нанесення потенційної та реальної шкоди такими діями;

— посилення конкурентної боротьби на міждержавному та транснаціональному рівні за володіння та користування новітніми технологіями, засобами, системами;

— загострення енергетичних проблем;

— терористична, екстремістська та інша злочинна діяльність міжнародних злочинних угруповань;

— діяльність наземних, повітряних, космічних, морських технічних засобів та приладів (супутників, радіоелектронного обладнання, інтернет-ресурсів та ін.) іноземних розвідувальних служб, яке наносить шкоду інтересам України;

— розробка іншими країнами стратегій війн малої інтенсивності у інформаційній, технологічній, економічній та ін. сферах життєдіяльності, які передбачають суттєву дестабілізацію державної і недержавної складових у загальній системі забезпечення національної безпеки України.

Аналізуючи найбільш актуальні та значимі для сьогодення інформаційні загрози життєдіяльності держави та суспільства, зазначимо, що більшість загроз і внутрішнього, і зовнішнього характеру взаємопов'язані між собою, як і джерела їх виникнення. Тому сьогодні вчені пропонують виділяти особливий тип транскордонних інформаційних загроз, які мають глобальний характер і несуть у собі ознаки як зовнішніх, так і внутрішніх інформаційних загроз. При цьому форма їх вияву — внутрішня, а сутність (джерела виникнення, стимуляція та склад можливих учасників) — зовнішня [8, с. 182].

Розглянемо питання сутності поняття "інформаційної безпеки". В вузькому розумінні, на думку В.М. Брижка, вона трактується як результат інтеграції змісту понять "національна безпека" та "безпека інформації" і ототожнюється з інститутом таємниці та суто технологічною інформаційною сферою. В широкому розумінні сьогодні інформаційна безпека трактується як стан захищеності інформаційного середовища, що повністю відповідає інтересам держави та забезпечує формування та можливості розвитку в умовах існування зовнішніх та внутрішніх загроз [4, с. 75].

На сьогодні в державі розроблена та затверджена Стратегія національної безпеки України (прийнята і затверджена Указом Президента України від 26 травня 2015 року № 287 "Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України"), яка основним видом інформаційних загроз національній безпеці нашої держави визначає агресивні дії Російської Федерації в інформаційному просторі [12]. Стратегія розмежовує поняття інформаційно-психологічної війни, загрози кібербезпеці України та безпеці її інформаційних ресурсів. Проте негативним явищем, на думку Т. Ткачука, є відмежування цих понять від суто загроз інформаційній безпеці держави.

Таблиця 1. Класифікація видів інформаційних загроз

№ з/п	Вид класифікації	Вид інформаційної загрози
1	За місцем знаходження джерела небезпеки	Зовнішні Внутрішні
2	За масштабами ймовірних наслідків	Глобальні Загальнонаціональні Регіональні Локальні поодинокі
3	За ступенем сформованості	Потенційні Реальні
4	За характером виникнення	Природні Техногенні Соціальні
5	За за ступенем суб'єктивного сприйняття	Завищені Занижені Мінімальні Умовні Адекватні
6	За сферами життєдіяльності	Політичні Економічні Соціальні Науково-технічні Екологічні Культурні Духовні та ін.

Джерело: узагальнено автором на основі [1—6].

Безпосередньо для нормативно-правового регулювання забезпечення інформаційної безпеки держави було прийнято Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України", який затвердив основні положення забезпечення інформаційної безпеки держави в умовах ведення гібридної війни з Росією. Ця Доктрина визначила основні інтереси та прагнення України в інформаційному середовищі, основні загрози їх практичній реалізації та пріоритети і напрями державної політики в інформаційній сфері. Вона також розмежувала основні види зовнішніх інформаційних загроз, передусім з боку РФ, а саме [11]:

— проведення інформаційних операцій, які спрямовані на зниження та підрив обороноздатності держави, ЗСУ, інших військових та воєнізованих формувань, посилення панічних, екстремістських настроїв серед населення, часткову чи повну дестабілізацію політичного чи соціально-економічного життя, провокування та розгортання міжетнічних, міжконфесійних і соціальних конфліктів [11];

— створення засобами інформаційного впливу негативного іміджу України на міжнародній арені [11];

— проведення інформаційної експансії державою-агресором та структурами, які їй підконтрольні [11];

— домінування держав-агресора в інформаційному середовищі на тимчасово окупованих територіях [11];

— обмеження можливостей України, окремих структур та органів ефективно протидіяти зовнішнім інформаційним загрозам [11];

— пропаганда в світі та Україні автономістських, федералістських та ізоляціоністських настроїв і концепцій існування [11].

Для ефективної протидії зовнішнім інформаційним загрозам розроблено комплексний системний механізм протидії, який включає в себе такі елементи: мету забезпечення безпеки; система моніторингу та оцінки зовнішніх джерел інформаційної небезпеки; сфери безпеки; параметри інформаційної безпеки; перелік інформаційних загроз та наслідки їх реалізації для України;

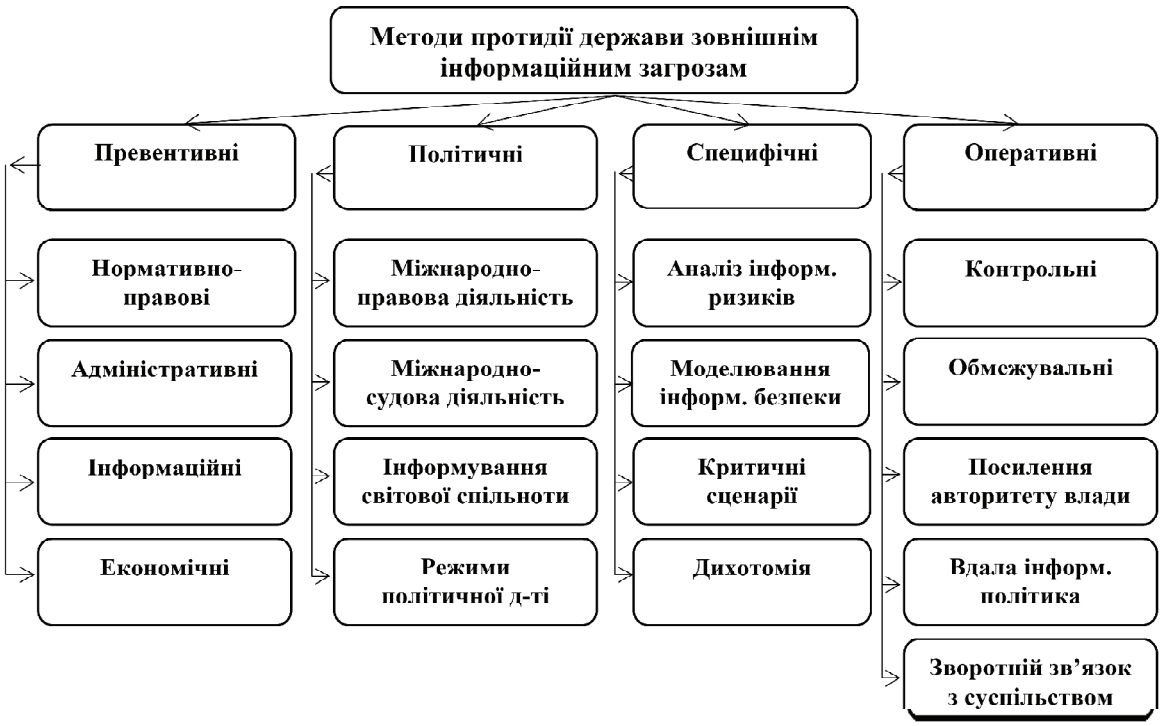

Рис. 1. Методи протидії держави зовнішнім інформаційним загрозам

Джерело: узагальнено автором на основі [1—6].

методи протидії зовнішнім інформаційним загрозам з боку державних структур [15, с. 182].

У сучасних реаліях застосування цих традиційних методів є недостатнім для боротьби із усім спектром гібридних загроз, які стоять перед Україною, тому спектр методів може бути розширено і новими підходами. Розподіл загальних методів можемо здійснювати на превентивні та оперативні; політичні та специфічні (рис. 1) [7, с. 117]:

1) превентивні (профілактичні) — спрямовані на недопущення розгортання інформаційних загроз на території України та запобігання появі нових інформаційних ризиків та якомога більш ранньому етапі їх виникнення [7, с. 117; 15];

2) оперативні — спрямовані на безпосередні дії у відповідь на вже здійснені агресивні кроки від зовнішніх інформаційних джерел [2; 15];

3) політичні — засновані на діяльності вищих державних органів та посадових осіб на міжнародній арені [2];

4) специфічні.

Превентивні методи класифікуються на 4 основні групи — нормативно-правові, адміністративні, інформаційні, економічні [15]. Так, наприклад, нормативно-правові методи грунтуються на вдосконалення існуючої нормативно-правової бази забезпечення інформаційної безпеки України. На сьогодні основою нормативно-правового регулювання в цій сфері є:

— перший рівень: Конституція України, Концепція національної безпеки України, Доктрина інформаційної безпеки України та Закон України "Про основи національної безпеки України";

— другий рівень: закони, які визначають важливі напрямки забезпечення інформаційної безпеки в державі ("Про державну таємницю", "Про Основні засади розвитку інформаційного суспільства в Україні на 2007—2015 роки", "Про інформацію", "Про Концепцію Національної програми інформатизації", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про Національну програму інформатизації", "Про телекомунікації", "Про радіочастотний ресурс", "Про захист суспільної моралі" та ін.);

— третій рівень: закони, що визначають компетенції державних органів у сфері інформаційної безпеки — "Про СБУ", "Про Кабінет Міністрів України", "Про прокуратуру", "Про надзвичайний стан" та ін.;

— укази та розпорядження Президента України, акти КМУ в цій сфері;

— міністерські та відомчі нормативні акти.

До оперативних методів протидії зовнішнім інформаційним загрозам слід віднести такі:

1) постійний та системний контроль вітчизняного інформаційного простору; щоправда, є деякі загрози політичного диктату та розгортання цензури в цьому випадку, тому контроль має бути не жорстким, погодженим та врівноваженим;

2) введення обмежень розмірів інформаційного простору для тих категорій населення та соціальних груп, які є найбільш вразливими до тієї чи іншої інформаційної загрози;

3) посилення авторитету та впливу власних владних структур, ЗСУ серед населення;

4) вдалі заходи власної інформаційної політики;

5) забезпечення ефективного зворотного зв'язку з суспільством тощо.

Окремо виділимо методи протидії зовнішнім інформаційним загрозам, які мають політичну складову [11]:

1) розробка і подання на розгляд міжнародних інституцій (ООН, Ради безпеки ООН, Ради Європи, ОБСЄ та ін.) резолюцій та ін. документів в даній сфері [11];

2) уведення спеціальних адміністративно-правових режимів, режимів діяльності політичних партій та рухів [11];

3) доведення до міжнародної спільноти достовірної та своєчасної інформації про ситуацію в Україні [11];

4) міжнародні економіко-політичні методи, вперед усім арбітражі в Міжнародний та Європейський суд проти держави-агресора [11].

Окремо відзначимо ще новітні специфічні методи — наприклад, метод дихотомії, який грунтується на одночасному проведенні відповідних заходів як щодо джерела загрози, так і щодо укріплення об'єкту небезпеки. Виділяють дві предметні складові протидії зовнішній загрозі: 1) визначення джерела загрози та можливий вплив на нього; 2) проведення відповідних заходів по забезпеченню інформаційної безпеки об'єкту [16, с. 66].

Відзначимо, що на сьогодні існує чимало як традиційних, так і інноваційних методів протидії зовнішнім інформаційним загрозам на державному рівні. До традиційних методів слід віднести такі:

— методи опису та класифікацій інформаційних небезпек (для формулювання адекватних заходів по здійсненню попередження чи усунення негативних наслідків інформаційних загроз);

— методи дослідження причинних зв'язків (методи розбіжності, схожості, супроводжувальних змін та залишків), які спрямовані на визначення причинно-наслідкових зв'язків між загрозами та наслідками їх реалізації та розробку на цій основі заходів по їх нейтралізації;

— технічні методи захисту інформації, які грунтуються на використанні криптографічних підходів для забезпечення режиму секретності інформації; проте виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них через те, що користувач буде позбавлений можливості своєчасного і швидкого доступу до цих даних та інформації, тому забезпечення конфіденційності інформації має відповідати можливості доступу до неї [4].

Зрозуміло також, що вичерпний перелік методів реалізації державної політики протидії зовнішнім інформаційним загрозам скласти фактично нереально, оскільки механізм їх реалізації створюється фактично після кожної появи нової зовнішньої інформаційної загрози, тим більше що вони є дуже мінливими в сучасному динамічному середовищі. Тому у разі вибору адекватних методів реагування спостерігаємо зміщення акцентів із загроз на ризики. У такому разі можна відійти від розуміння загроз інформаційній безпеці як усталених явищ та впроваджувати різноманітні новітні підходи їх нейтралізації, особливо в умовах невизначеності політичного та соціально-економічного життя. Тому сучасні методи базуються насамперед на принципах управління ризиками, оскільки дозволяють впливати на ті керовані елементи загроз, у разі нівелювання яких буде забезпечено оптимальний стан інформаційного простору держави якомога менше затраченими зусиллями [16].

Для того щоб ефективно протистояти інформаційним впливам, попереджувати негативні наслідки від впливу пропаганди, необхідним є боротьба із інформаційними загрозами на стратегічному і тактичному рівнях, що може включати наступні напрями:

1. Ефективна реалізація положень інформаційної доктрини в Україні.

2. Активізація виробництва власного інформаційного продукту та його поширення у Європі і світі.

3. Зміцнення співпраці щодо протидії пропагандистським впливам з іноземними державами.

4. Удосконалення нормативно-правового регулювання інформаційної безпеки, зокрема прийняття стратегії інформаційної безпеки на основі діючої доктрини.

5. Формування та зміцнення інформаційного простору держави, в якому циркулюватиме достовірна, неупереджена інформація.

6. Активізація громадських об'єднань та інших зацікавлених сторін до виявлення неправдивої інформації, що пришвидшить її нейтралізацію.

ВИСНОВКИ

Таким чином, під поняттям методів реалізації державної політики протидії зовнішнім інформаційним загрозам слід розуміти сукупність різнопланових видів та способів діяльності державних структур та інституцій і способів їх взаємодії, які дають змогу найбільш ефективно та оперативно реагувати відповідним чином на зовнішні інформаційні загрози або управляти тими ризиками, що їх зумовили для подальшої їх нейтралізації. На відміну від традиційних методів нейтралізації інформаційних загроз, інноваційні методи базуються на принципах управління ризиками і можуть ефективно блокувати деструктивні елементи та властивості загроз, а також дати стимул розгортанню та реалізації конструктивних елементів, властивостей та процесів в інформаційному просторі України. Для подолання інформаційних загроз нагально-необхідним є ефективно реалізовувати державну доктрину інформаційної безпеки, посилювати координацію та співпрацю з іншими державами та з громадянським суспільством для виявлення інформаційних загроз; формування власного інформаційного простору з поширенням достовірної інформації. Перспективними з точки зору подальших досліджень може бути науковий пошук найбільш ефективних інструментів застосування методів протидії інформаційних загроз.

Література:

1. Аналітичний огляд проблем інформаційного й електронного права в Україні [Електронний ресурс] // Сайт "AMB" group. — Режим доступу: http://www.its-way.kiev.ua/index.php?language=ru&main_managemen=about&mana gemen=eGov_Zak

2. Антонюк В.В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України // Дисертація на здобуття наукового ступеня кандидата наук з державного управління // НАДУ при Президентові України. — К., 2017. — 218 с.

3. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: монографія / За загальною редакцією д-ра юрид. наук, проф. Бандурки О.М. — Харків: Вид-во Ун-ту внутр. Справ, 2000. — 368 с.

4. Брижко В.М. Інформаційне суспільство. Дефініції / В.М. Брижко, О.М. Гальченко, В.С. Цимбалюк, О.А. Орєхов, А.М. Чорнобров. — К., 2002. — 220 с.

5. Горбулін В.П. Засади національної безпеки України / В. Горбулін, А. Качинський. — К.: Інтертехнологія, 2009. — 272 с.

6. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки / В. Дереко // Інформаційна безпека людини, суспільства, держави. — 2015. — № 2 (18). — С. 16—22.

7. Живко З. Інформаційні загрози: суть і проблеми / З. Живко, М. Живко // Безпека та захист інформації в інформаційних системах: тези доповідей II Міжнародної НПК. — К., 2017. — С. 116—118.

8. Куцька О.М. Особливості інформаційно-психологічного впливу Російської Федерації напередодні та початковому етапі антитерористичної операції на сході України / О. Куцька // Інформаційна безпека людини, суспільства, держави. — 2017. — № 1 (21). — С. 180—190.

9. Литвин М.М. Умови та фактори внутрішньої загрози національній безпеці України / М. Литвин, В. Кохан [Електронний ресурс]. — Режим доступу: plesetsk-info.ru/uchebnoe-posobie/umovi-ta-faktorivnutrshno-zagrozi-natconalni-bez

10. Про основи національної безпеки України: Закон України від 19.06.2003 [Електронний ресурс]. — Режим доступу: http://zakon2.rada.gov.ua/ laws/ show/964-15

11. 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 № 47/2017 [Електронний ресурс]. — Режим доступу: www.president.gov.ua/ documents/ 472017-21374

12. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про національну безпеку України": Указ Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. — Режим доступу: www.president.gov.ua/ documents/ 2872015-190

13. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки / Г. Сащук [Електронний ресурс]. — Режим доступу: http:// journ. univ.kiev.ua/ trk/publikacii/satshuk_publ.php

14. Снитко О.С. Проекти тотального зомбування в інформаційному просторі України / О. Снитко // Інформаційна безпека людини, суспільства, держави. — 2017. — № 1 (21). — С. 207—215.

15. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз // Підприємництво, господарство і право. — № 10. — 2017. — С. 182—189.

16. Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності / Р. Хмелевський // Сучасний захист інформації. — 2016. — № 4. — С. 65—70.

References:

1. "AMB" group (2018), "Analytical review of problems of information and electronic law in Ukraine", available at: http://www.itsway.kiev.ua/index.php?-language=ru&main_managemen=about&managemen=-eGov_Zak, (Accessed 11 August 2019).

2. Antoniuk, V.V. (2017), "Organizational and legal bases of formation and realization of the state information security policy of Ukraine", Abstract of Ph.D. dissertation, State administration, The National Academy for Public Administration under the President of Ukraine, Kyiv, Ukraine.

3. Aristova, I.V. (2000), Derzhavna informatsijna politika: orhanizatsijno-pravovi aspekty [State information policy: organizational and legal aspects], Kharkiv National University of Internal Affairs, Kharkiv, Ukraine.

4. Bryzhko, V. M. Hal'chenko, O.M. Tsymbaliuk, V.S. Oriekhov, O.A. атв Chornobrov, A.M. (2002), Informatsijne suspil'stvo. Definitsii [Information Society. Definitions], Integral, Kyiv, Ukraine.

5. Horbulin, V.P. Kachyns'kyj, A.B. (2009), Zasady natsional'noi bezpeky Ukrainy [National security principles of Ukraine], Intertekhnolohiia, Kyiv, Ukraine.

6. Dereko, V.N. (2015), "Theoretical and methodological principles of information security threat classification", Information Security of the Person, Society and State, vol. 2 (18), pp. 16—22.

7. Zhyvko, Z.B. and Zhyvko M.O. (2009), "Information threats: the essence and problems", Information Security of the Person, Society and State, vol. 7 (81), pp. 116—118.

8. Kuts'ka, O.M. (2017), "Features of information-psychological impact of the Russian Federation on the eve and initial stage of the anti-terrorist operation in eastern Ukraine", Information Security of the Person, Society and State, vol. 1 (21), pp. 180—190.

9. Lytvyn, M. and Kokhan, V. (2017), "Conditions and factors of internal threat to Ukraine's national security", available at: http://plesetsk-info.ru/uchebnoe-posobie/umovi-ta-faktorivnutrshno-zagrozi-natconalni-bez, (Accessed 11 August 2019).

10. The Verkhovna Rada of Ukraine (2003), The Law of Ukraine "On the Fundamentals of National Security of Ukraine", available at: https://zakon2.rada.gov.ua/laws/show/964-15?lang=en (Accessed 11 August 2019).

11. President of Ukraine (2017) Decree "On the decision of the National Security and Defense Council of Ukraine of December 29, 2016 "On the Doctrine of Information Security of Ukraine", available at: https://www.president.gov.ua/documents/472017-21374 (Accessed 11 August 2019).

12. President of Ukraine (2015) Decree "On the decision of the National Security and Defense Council of Ukraine of 6 May 2015 "On National Security of Ukraine", available at: https://www.president.gov.ua/documents/2872015-190 (Accessed 11 August 2019).

13. Press Office "TroubleShooter" (2014), "Information security in the national security system", available at: http://troubleshooter.com.ua/ru/inform-bezopasnost/52-informatsijna-bezpeka-v-sistemi-zabezpechennya-natsionalnoji-bezpeki (Accessed 11 August 2019).

14. Snytko, O.S. (2017), "Total zombie projects in the information space of Ukraine", Information Security of the Person, Society and State , vol. 1 (21), pp. 207—215.

15. Tkachuk, T.Yu. (2017), "Modern threats to the information security of the state: a theoretical and legal analysis", Entrepreneurship, Economy and Law, vol. 10, pp. 182—189.

16. Khmelevs'kyj, R.M. (2016), "Research of information security threats assessment of information objects", Modern Information Security, vol. 4, pp. 65—70.

Стаття надійшла до редакції 12.08.2019 р.