

УДК 65.012.8:007+32(477)

**ОСНОВИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ОРГАНАМИ
ВЛАДИ ЩОДО ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ В
УКРАЇНІ**

DOI 10.30838/ P.ES.2224.260219.65.379

Прав Р. Ю.*Міжрегіональна Академія Управління персоналом, Київ*

У статті з'ясовано основи реалізації державної політики органами влади щодо протидії інформаційним загрозам в Україні. З'ясовано, що в умовах глобальних викликів головним стратегічним національним ресурсом, що визначає економічну і оборонну міць держави, є інформація та інформаційні технології, від яких вирішальною мірою залежать всі сфери життєдіяльності суспільства: виробництво та управління, оборона і енергетика, транспорт і зв'язок, банківська справа і фінанси, наука, освіта і багато інших. Доведено, що для власного сталого інформаційного розвитку в умовах жорсткої конкуренції з урахуванням чинників інформаційної безпеки кожна держава повинна забезпечити: розуміння інформаційних атак та протистояння ним; створення програмного забезпечення протистояння інформаційним атакам; аналіз показників інформаційних загроз з метою вдосконалення механізмів прийняття рішень в системах державного управління; забезпечення максимального захисту від зовнішніх впливів; аналіз стану і технічний аудит всіх засобів комунікації; консолідація діяльності органів державної влади та ЗМІ у сфері політичного інформування суспільства для нейтралізації негативного психологічного впливу в умовах криз та конфліктів. Інформаційна політика держави має зосередитися на віддзеркаленні нагальних питань, що сформувалися у галузі міжнародних відносин та галузі інформаційної безпеки та ін. Права та інтереси кожного суб'єкта інформаційних взаємин мають бути законодавчо захищені. Найважчим буде реалізація завдань, в межах яких планується гармонійно забезпечити інформаційну безпеку країни, індивіда і соціуму й одночасно виокремити нагальні пріоритети, а саме: створити/відновити основні захисні елементи структури інформаційної нацбезпеки, практично реалізувати зазначену раніше схему дієвого механізму інформаційного захисту країни, переглянути нові інформаційні загрози, усунути наявні, визначивши ступені імовірних результатів та рівня їхнього інтенсивного впливу. Головною інформаційною загрозою для національної безпеки є вплив, який може здійснити інша сторона на стан державної інформаційної інфраструктури, інформаційних ресурсів, на стан суспільства, свідомості, підсвідомості індивідуума задля нав'язування державі бажаної системи з відповідними цінностями, поглядами, інтересами і рішеннями щодо надважливих сфер у суспільній і державній діяльності, взяття під контроль їхньої поведінки і розвитку у потрібному іншій стороні векторі.

Ключові слова: безпека; державна політика; ефективність; інформація; інформаційна безпека; інформаційні загрози; національна безпека

UDC 65.012.8:007+32(477)

BASIS FOR THE REALIZATION OF THE STATE POLICY BY AUTHORITIES IN RESPECT TO CONTACTS TO INFORMATIONAL THREATS IN UKRAINE

DOI 10.30838/ P.ES.2224.260219.65.379

Prav R.,*Interregional Academy of Personnel Management, Kiev*

The article clarifies the basis for the implementation of state policy by authorities to counter information threats in Ukraine. It has been revealed that in the context of global challenges, the main strategic national resource defining the economic and defense power of the state is the information and information technologies, from which the vital functions of society are crucial to all sectors: production and management, defense and energy, transport and communications, banking, finance, science, education and many others. It has been proved that for the own stable information development in the conditions of strict competition taking into account factors of information security, each state should ensure: understanding of information attacks and confrontation; creation of software for confrontation with information attacks; analysis of indicators of information threats in order to improve decision-making mechanisms in public administration systems; providing maximum protection against external influences; analysis of the state and technical audit of all means of communication; consolidation of the activities of state authorities and mass media in the field of political informing of society in order to neutralize negative psychological influence in conditions of crises and conflicts. The state's information policy should focus on reflecting the urgent issues that have emerged in the field of international relations and the field of information security, etc. The rights and interests of each subject of information relations should be legally protected. The most difficult will be the implementation of tasks within which it is planned to harmonize the information security of the country, the individual and the society and simultaneously highlight the urgent priorities, namely: to create / restore the basic security elements of the information security structure, to implement the above-mentioned scheme of the effective mechanism of information protection of the country, to review new ones information threats, eliminate existing ones, identifying the degree of probable results and the level of their intensive influence. The main information threat to national security is the influence that the other party can make on the state of the state information infrastructure, information resources, on the state of society, consciousness, and subconsciousness of the individual in order to impose the state the desired system with the corresponding values, views, interests and decisions on critical areas. in social and state activities, taking control of their behavior and development in the right other side of the vector.

Keywords: security; state policy; efficiency; information; information security; information threats; national security

Актуальність проблеми. В умовах глобальних викликів головним стратегічним національним ресурсом, що визначає економічну і оборонну міць держави, є інформація та інформаційні технології, від яких вирішальною мірою залежать всі сфери життєдіяльності суспільства: виробництво та управління, оборона і енергетика, транспорт і зв'язок, банківська справа і фінанси, наука, освіта і багато інших. При цьому недостатня захищеність інформаційних ресурсів призводить до витоку найважливішої політичної, економічної, наукової та військової інформації.

Актуальність проблеми забезпечення інформаційної безпеки, обумовлена, крім того, необхідністю прийняття ефективних, відповідних політичним завданням, управлінських рішень. Відзначимо, що залежність від інформації та інформаційних технологій стає одним з передумов формування суспільства. Володіння своєчасними, точними, достовірними даними слугує надзвичайно важливим фактором ефективності прийняття управлінських рішень як на державному рівні, так і на рівні регіонів України. Інформація стає стратегічною цінністю як держави, так і будь-якої управлінської структури в системі політичного управління. В кінцевому рахунку, якість функціонування та безпеки інформаційної сфери, так само як і стан правового регулювання відносин у даній сфері визначають рівень розвитку держави. Як стратегічний ресурс, інформація вимагає особливих заходів не тільки в сенсі її розвитку та накопичення, але й захисту. Саме тому актуалізується необхідність дослідження моніторингу ефективності реалізації державної політики у протидії інформаційним загрозам в Україні.

Аналіз останніх досліджень та публікацій. Питанням особливостей реалізації державної інформаційної політики присвячували свої праці такі провідні науковці, як: Бондаренко В., Горбань Ю., Литвиненко В., Марутян Р., Петрик В. та інші. Проте, дані науковці досліджували лише загалом політику протидії інформаційним загрозам в Україні. Станом на сьогодні існує необхідність дослідження особливостей реалізації державної політики органами влади щодо протидії інформаційним загрозам в Україні, що зумовило вибір теми даної статті.

Мета статті – з'ясувати особливості реалізації державної політики органами влади щодо протидії інформаційним загрозам в Україні.

Виклад основного матеріалу дослідження. Інформаційна безпека є інтегрованим складником нацбезпеки, що розглядається як пріоритетна державна функція. Разом з тим, вона забезпечує якісне всебічне поінформування населення та вільний доступ до різноманітних інформаційних джерел, попереджає розповсюдження неправдивої інформації, сприяє суспільній цілісності, зберігає інформаційний суверенітет, протидіє негативному інформаційно-психологічному пропагандистському впливові та захисту національних інформаційних даних від маніпулювання, інформаційної війни та інших інформаційних операцій. Вирішення комплексних проблем, пов'язаних з інформаційною безпекою, сприятиме захисту суспільних і державних інтересів, та і гарантуванню громадянських прав на отримання всебічних, об'єктивних та якісних інформаційних даних.

Дбаючи про захист власних інформаційних інтересів, усі держави повинні забезпечувати і надійність власної інформаційної безпеки. Це необхідно і для зміцнення державності України. Збалансованість державної інформаційної політики України є складовою частиною її соціально-економічного політичного устрою, беручи до уваги пріоритетність національного інтересу та загрози державної нацбезпеки. З погляду права вона базується на положеннях правової демократичної держави і запроваджується розробкою та реалізацією державних розробок, до яких належать доктрини, стратегії, концепції та програми відповідно до чинного законодавства. На сьогодні Україна має об'єктивну потребу державно-правового регулювання науково-технологічного та інформаційного напрямку, що відповідав би сучасному світовому становищу та інформаційно-технологічному розвитку, міжнародному законодавству, та в той же час передбачала ефективний захист українських національних інтересів. Взаємини, що пов'язуються з інформаційною безпекою, як найважливіших для сучасних держави та соціуму, мають потребу у найшвидшому законодавчому регулюванні.

Проведення вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних та військових конфліктів. У ст.17. Конституції України зазначено: “Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу” [3]. Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни, її

забезпечення завдяки послідовній реалізації ефективно сформульованої національної інформаційної стратегії в значній мірі сприяло б забезпеченню досягнення успіху при вирішенні завдань у політичній, соціальній, економічній та інших сферах державної діяльності [4].

Інформаційна безпека – це комплекс засобів, що забезпечують інформаційний суверенітет України, захист сфери інформації від загроз зовнішнього і внутрішнього типу та протистояння їх сукупностям.

Необхідність забезпечення інформаційної безпеки зумовлюється, по-перше, потребою забезпечення національної безпеки України в цілому, по-друге, існуванням таких загроз в інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам, по-третє, врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей. Завдання інформаційної безпеки - створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. При виникненні криз, загостренні конфліктів інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї. Показниками, виступають цілеспрямованість, масштабність та комплексність дій тощо [1].

Загрози національній безпеці України в інформаційній сфері це – сукупність умов та чинників, які становлять небезпеку життєво-важливим інтересам держави, суспільства і особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [6].

Як зазначає Р. Р. Марутян, найсуттєвішою загрозою національній безпеці України в інформаційній сфері є здійснення іноземними державами негативного інформаційно-психологічного впливу на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій та кампаній, спеціальних інформаційних операцій. Це відбувається через систематичне поширення тенденційної, неповної або упередженої інформації про Україну та політичні процеси, що відбуваються на її теренах. Усе це впливає на зовнішню та внутрішню політику нашої держави, знижує її міжнародний імідж, має політичне та економічне підґрунтя. Метою таких

інформаційних операцій є забезпечення власних національних інтересів інших держав [4].

Загрозами для національної безпеки української держави в сфері інформації є зокрема: обмежування свобод слова та доступу населення до інформаційних даних; перекручене, спотворене, суб'єктивне висвітлювання інформаційних даних та тенденції до їх замовчування; їх незаконне поширювання; відкрита дезінформація; інформаційна експансія іншими державами та руйнівний характер інформаційного вторгнення до національного інформаційного простору, при отриманні країнами з потужнішими інформаційними ресурсами можливості розширення свого впливу через засоби масової інформації на суспільство не таких потужних держав; поява і функціонування у межах державного національного інформаційного простору інформаційних потоків, що мають неконтрольований характер; пропагування ЗМІ агресії та насильства; повільна інтеграція нашої держави до світового інформаційного простору; невважена державна інформаційна політика та відсутня необхідна інфраструктура в інформаційній сфері; розміщування неправдивої інформації у всесвітній мережі [5].

Варто наголосити, що проти України з боку Російської федерації ведеться інформаційна війна, яка спрямована на нав'язування певних ідеологічних стереотипів, тієї чи іншої суспільної думки за допомогою засобів масової інформації, зокрема через електронні видання [5]. Війни такого типу є досить поширеними у глобальному інформаційному просторі та їх всебічно досліджують науковці та фахівці. Зокрема, Інститут національно-стратегічних досліджень США та деякі західні експерти і вчені виокремлюють кілька складових елементів інформаційної війни. Один із них – ведення психологічної війни. Головне завдання психологічної війни полягає в маніпулюванні масами. Метою такої маніпуляції є: внесення в суспільну та індивідуальну свідомість ворожих ідей та поглядів; дезорієнтація та дезінформація мас; послаблення певних переконань, залякування народу образом ворога; залякування супротивника власною могутністю [2].

У межах сучасного глобалізованого інформаційного суспільства, де кіберпростір стає полем протистояння, вагомою загрозою для інформаційної державної безпеки (і української, в тому числі) є наявність комп'ютерної злочинності, кібернетичної війни, кібернетичного тероризму, що засобами боротьби між національними інтересами в

Інтернет-мережах, використання комп'ютерної та інтернет-технології для інструменту проти опонента. Найбільш часто технологічні засоби кібернетичної війни, кібернетичного тероризму скеровані на державну безпеку й оборону і є реальною загрозою для державної незалежності.

Таким чином, на Україну часто спрямовують засоби сучасних технологій, що несуть негативні інформаційно-психологічні впливи та становлять загрозу для українського національного інформаційного середовища та державної самостійності. Інформаційна безпека України за дестабілізуючих умов, які зумовила експансіоністська агресивна інформаційна політика та негативний інформаційно-психологічний вплив з боку РФ, вимагає об'єднання сил на всіх рівнях державної влади та громадськості [6].

Те, що прийнято вважати інформаційною зброєю, зокрема, особливі операції психологічного спрямування, активно діють достатньо давно, в той час як інші засоби, наприклад, спеціальні інструменти протистояння комп'ютерного типу, утворилися тільки декілька років тому. Проте усім їм притаманна спільна риса - вони засновуються на такій ідеї, як опосередкований вплив на реальний світ.

Якщо наноситься удар через недосконалість інформаційних взаємин, використання інформації неякісного характеру та ін., це говорить про послаблення інформаційної безпеки. Це трактування дає можливість розглянути як нагальні питання гарантії інформаційної безпеки нашої держави такі:

- недосконала інформаційна політика та політика державної інформаційної безпеки;
- недосконала нормативно-правова база інформаційних співзв'язків та інформаційної безпеки;
- недостатньо розвинена державна інформаційна інфраструктура;
- обмеження іноземних держав щодо України розповсюдження інформаційних даних та отримання новітніх інформаційних технологічних засобів;
- несанкціоновані дії посадовців, різноманітних об'єднань та угруповань у межах інформаційного інтересу населення та країни в цілому;
- недосконала державна система забезпечування інформаційної безпеки;

– ймовірність виникнення нештатної, непередбаченої ситуації у рамках систем, процесів, основою яких є інформаційні технології та ін.

Для забезпечення ефективності реалізації державної політики органами влади щодо протидії інформаційним загрозам в Україні необхідне забезпечення наступних умов [6]:

1. Усвідомлення безперервної роботи системи забезпечування державної інформаційної безпеки. Ця стадія пов'язується з ідентифікуванням надважливих точок, що є об'єктами, на які скерований захист. Мова йде також про основні внутрішні та зовнішні загрози, що можуть мати критичний вплив на системи.

2. Стратегії забезпечування безперервної діяльності системи. В такому разі робота передбачає визначення та добір альтернативного рішення про відновлювання системи задля зведення загроз до мінімуму. Рішення повинні зважати на собівартість захисних систем та їх результативність.

3. Розроблення та впровадження. Ця стадія містить структурування та документування Програми безперервності державного управління.

4. Прогрес культури державної інформаційної безпеки спрямований на розробку інтегральної системи задля захисту інформаційних даних держави.

5. Виконання, допомога та аудит процесу врегулювання безперервної роботи системи державної інформаційної безпеки при умові різних кризових та конфліктних ситуацій.

6. Керування системами державної інформаційної безпеки статусним та рольовим розподілом і перерозподілом, що передбачають наявність відповідальності, підзвітності, страхування (гарантування) та управління щодо безперервної діяльності системи, що забезпечує державну інформаційну безпеку.

Головною інформаційною загрозою для національної безпеки є вплив, який може здійснити інша сторона на стан державної інформаційної інфраструктури, інформаційних ресурсів, на стан суспільства, свідомості, підсвідомості індивідуума задля нав'язування державі бажаної (іншій стороні) системи з відповідними цінностями, поглядами, інтересами і рішеннями щодо надважливих сфер у суспільній і державній діяльності, взяття під контроль їхньої поведінки і розвитку у потрібному іншій стороні векторі. Саме це – загроза українській

незалежності у суспільній і державній роботі, котра реалізується в інформаційній площині. Стратегічна інформаційна конфронтація є прикладом самостійного і абсолютно нового виду протистоянь, що здатний до вирішення конфліктів, не застосовуючи збройні сили в усталеному значенні. Щоб вивчити закономірності, які діють в інформаційному протистоянні, та проаналізувати його кількісні характеристики, варто вдатися до формалізації як ступеня інформаційної озброєності країни, так і механізму розвитку ресурсної бази в конкретній державі та впливу, який має зовнішнє оточення. У цьому випадку інформаційне становище України лежить в основі аналізу.

Для того, щоб нівелювати негативний ефект масштабних негативних інформаційно-психологічних впливів, операцій та війн, мають бути визначені пріоритетні напрямки держполітики в інформаційній сфері та здійснені важливі кроки владними органами України, а саме:

- 1) інтегрувати Україну до інформаційного простору на світовому та регіональному європейському рівні;
- 2) інтегрувати до міжнародних інформаційних та інформаційно-телекомунікаційних систем та організацій;
- 3) створити власний національний інформаційний простір та забезпечити розвиток інформаційного суспільства;
- 4) модернізувати усю систему інформаційного захисту країни та сформувати й реалізувати ефективну інформаційну політику;
- 5) удосконалити законодавство щодо інформаційної безпеки, узгодити національне законодавство з рядом відповідних міжнародних стандартів та ефективно врегульовувати інформаційні процеси в правовій площині;
- 6) розвивати національну інформаційну інфраструктуру;
- 7) підвищити конкурентоспроможність вітчизняного інформаційного продукту та послуг інформаційного характеру;
- 8) впровадити сучасні інформаційно-комунікативні технології у процес держуправління;
- 9) налагодити ефективну взаємодію між владними структурами та інститутами громадянського суспільства під час створення, здійснення та коригування держполітики в інформаційному питанні.

Як базовою скористаємося моделлю врегулювання інформаційного протистояння між двома країнами, яку склали, взявши за основу модель Річардсона-Каспарова. Базується модель на наступних гіпотезах:

– під час обміну інформаційними атаками обидві країни прагнуть покращити свою інформаційну зброю в плані ефективності пропорційно до рівня інформаційності супротивника;

– фактор економічного потенціалу кожної з держав може надати/обмежити впливовість щодо темпу збільшення інформаційної потужності держави;

– країни збільшують свої інформаційні потужності згідно зі своїми цілями.

Позначимо рівні інформаційних потужностей кожного учасника протистояння як $N_1(t)$, $N_2(t)$, де t – час. Тоді зазначений перелік умов, за яких модель діятиме, можна формалізувати у систему, яку складають два диференціальних рівняння:

$$\begin{aligned} N_1 &= M_1 (L_1 - N_1) [1 - \exp(-p_1(k_1 N_2 - a_1 N_1 + g_1))] \\ N_2 &= M_2 (L_2 - N_2) [1 - \exp(-p_2(k_2 N_1 - a_2 N_2 + g_2))], \end{aligned} \quad (1)$$

де $M_1, M_2, L_1, L_2, p_1, p_2, a_1, a_2, k_1, k_2$ є позитивними коефіцієнтами, що не залежать від часу.

Параметри моделі (1) за аналогією Т. Сааті [7] визначені наступним чином:

k_1, k_2 – коефіцієнти реакції на інформаційні атаки;

a_1, a_2 – показники витрат на генерацію інформаційної зброї;

g_1, g_2 – коефіцієнти претензії (агресивності), якщо вони позитивні, або коефіцієнти доброї волі, якщо вони негативні;

M_1, M_2 – вартість наявного інформаційного забезпечення;

L_1, L_2 – граничні значення рівнів інформаційних потужностей;

p_1, p_2 – коефіцієнти ступеня важливості інформаційних витрат.

Модель (1) допускає існування чотирьох особливих розв'язків, що визначають координати положень рівноваги:

$$\begin{aligned} \text{а) } N_1^p &= N_1^*, N_2^p = N_2^* & \text{б) } N_1^p &= N_1^*, N_2^p = L_2 \\ \text{в) } N_1^p &= L_1, N_2^p = N_2^* & \text{г) } N_1^p &= N_2^*, N_2^p = L_2, \end{aligned} \quad (2)$$

де N_1^*, N_2^* – є рішення системи лінійних алгебраїчних рівнянь.

Нехай функції $u_1 = r_1^0(x_1 - x_2)$ і $u_2 = r_2^0(x_2 - x_1)$ характеризують політику кожної країни в сфері інформаційного протистояння, де змінні $x_1 = N_1 - N_1^*$, $x_2 = N_2 - N_2^*$ мають значення відхилень від рівноважних рівнів інформаційної потужності. Тут r_1^0, r_2^0 – стаціонарні параметри

управління. З врахуванням вигляду функції u_1 , u_2 система (1) набуває вигляду:

$$\begin{aligned}x_1 &= M_1 (\delta_1 - x_1) [1 - \exp(-p_1(a_1 x_1 - k_1 x_2))] + r_1^0 (x_1 - x_2) \\x_2 &= M_2 (\delta_2 - x_2) [1 - \exp(-p_2(a_2 x_2 - k_2 x_1))] + r_2^0 (x_2 - x_1),\end{aligned}\quad (3)$$

Можемо дійти таких такого висновку: у кожній державі, що існує у світовому інформаційному просторі як його частина, має бути напрацьований перелік дій для свого стабільного прогресу в інформаційній площині в обставинах жорсткого конкурування, враховуючи чинники інформаційної безпеки. Для цього варто [1]:

- розуміти інформаційні атаки та засобів протидії;
- створити програмне забезпечення для протидії нападам інформаційного характеру;
- аналізувати показники інформаційних небезпек з метою вдосконалити механізми, згідно з якими приймаються рішення в системі держуправління;
- забезпечити максимальний захист від зовнішнього впливу;
- аналізувати стан і вдаватися до технічного аудиту всіх комунікаційних засобів;
- консолідувати діяльність владних структур та засобів масової інформації у галузі донесення політичної інформації до суспільства, щоб нейтралізувати негативний психологічний вплив в кризових та конфліктних обставинах.

Висновки. Інформаційна політика держави має зосередитися на віддзеркаленні нагальних питань, що сформувалися у галузі міжнародних відносин та галузі інформаційної безпеки та ін. Права та інтереси кожного суб'єкта інформаційних взаємин мають бути законодавчо захищені. Найважчим буде реалізація завдань, в межах яких планується гармонійно забезпечити інформаційну безпеку країни, індивіда і соціуму й одночасно виокремити нагальні пріоритети, а саме: створити/відновити основні захисні елементи структури інформаційної нацбезпеки, практично реалізувати зазначену раніше схему дієвого механізму інформаційного захисту країни, переглянути нові інформаційні загрози, усунути наявні, визначивши ступені імовірних результатів та рівня їхнього інтенсивного впливу. Державна інформаційна політика повинна акцентовано забезпечувати право на своєчасне отримання достовірної і повної інформації, утвердження свободи слова та інформаційної

діяльності, перешкоджання втручанню до змісту та внутрішньої організації інформаційного процесу, крім моментів, що визначені у законодавстві згідно з Конституцією України; збереження та вдосконалення вітчизняних національних інформаційних технологій, забезпечувати інформаційну та національно-культурну ідентифікацію української держави у межах світового інформаційного простору; гарантувати державну підтримку та розвиток ресурсної бази, науково-технічного продукту та технологій інформаційного характеру.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бондаренко В.О., Литвиненко В.О. Інформаційна безпека сучасної держави: концептуальні роздуми. / [Електронний ресурс] - Режим доступу: www.crimeresearch.ru/library/strateg.html
2. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення [Електронний ресурс] / Ю. О. Горбань. – Режим доступу: <http://www.visnyk.academy.gov.ua/wpcontent/uploads/2015/04/20.pdf>
3. Закон України «Про інформацію». / [Електронний ресурс] - Режим доступу: <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12>
4. Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України [Електронний ресурс] / Р. Р. Марутян. – Режим доступу: http://www.dsaua.org/index.php?option=com_content&view=article&id=198%3A2014-08-13-12-5548&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk
5. Методи інформаційного захисту простору. Інформаційна безпека України [Електронний ресурс]. – Режим доступу: <http://www.ua.textreferat.com/referat-7471.html>
6. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: <http://www.justinian.com.ua/article.php?id=3222>
7. Саати Т. Л. Математические модели конфликтных ситуаций. - М. : “Сов. Радио”, 1977. - 304 с
8. Фурман І. О. Інформаційна безпека в комп'ютерних програмах та системах, 2015.–2с.

REFERENCES:

1. Bondarenko V.O., Lytvynenko V.O. Informatsiina bezpeka suchasnoi derzhavy: kontseptualni rozdumy [Information security of the modern state: conceptual reflections]. Retrieved from www.crimeresearch.ru/library/strateg.html [in Ukrainian].

2. Horban Yu. O. Informatsiina viina proty Ukrainy ta zasoby yii vedennia [Information war against Ukraine and means of its conduct] Retrieved from <http://www.visnyk.academy.gov.ua/wpcontent/uploads/2015/04/20.pdf> [in Ukrainian].
3. Zakon Ukrainy «Pro informatsiiu» [The Law of Ukraine "On Information"]. Retrieved from <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12> [in Ukrainian].
4. Marutian R. R. Rekomendatsii shchodo vdoskonalennia polityky zabezpechennia informatsiinoi bezpeky Ukrainy [Recommendations for improving the policy of ensuring information security of Ukraine] Retrieved from http://www.dsaua.org/index.php?option=com_content&view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk [in Ukrainian].
5. Metody informatsiinoho zakhystu prostoru. Informatsiina bezpeka Ukrainy [Methods of information protection of space. Information security of Ukraine] Retrieved from <http://www.ua.textreferat.com/referat-7471.html> [in Ukrainian].
6. Petryk V. Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby [The essence of information security of the state, society and person] Retrieved from <http://www.justinian.com.ua/article.php?id=3222> [in Ukrainian].
7. Saaty T. L. (1997) Matematicheskie modeli konfliktnyih situatsiy [Mathematical models of conflict situations]. Moskva : “Sov. Radio” [in Russian].
8. Furman I.O. (2015) Informatsiyna bezpeka v komp"yuternykh prohramakh ta systemakh [in Ukrainian].