УДК: 341.5, 342; 343

https://doi.org/10.32689/2617-9660-2020-1(7)-285-296

Шемчук Віктор Вікторович,
кандидат юридичних наук, доцент кафедри конституційного та міжнародного права Навчально-наукового гуманітарного інституту Таврійського національного університету імені В. І. Вернадського, Заслужений юрист України, м. Київ, вул. Дж. Маккейна, 33, 529-05-16, vvshem.chuk@gmail.com, https//orcid.org/0000-0001-7969-6589

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ: ПРОБЛЕМИ ВИЗНАЧЕННЯ ТА ПОДОЛАННЯ

Анотація. У даній статті досліджено загрози інформаційній безпеці держави а основі існуючої доктринальної і нормативно-правової бази. Грунтовний аналіз положень Законів України «Про основи національної безпеки України» 2003 р., «Про основні засади забезпечення кібербезпеки України» 2017 р., «Про національну безпеку України» 2018 р., Стратегії національної безпеки України 2015 р., Доктрини інформаційної безпеки України 2017 р. демонструє відсутність єдиного підходу до визначення і розуміння категорії загрози інформаційній безпеці. Іноді їх трактують як загрози національній безпеці держави, як загрози національним інтересам та національній безпеці України в інформаційній сфері, кіберзагрози тощо.

У наукових виданнях подекуди їх ототожнюють або, навпаки, наводять розгалужені їх класифікації за різноманітними критеріями. Загрози інформаційній безпеці України розглядаються нами як детермінуючі фактори, що зумовлюють і породжують негативні явища, які посягають на національні інтереси в інформаційній сфері, організацію та функціонування національного інформаційного простору загалом. Вони можуть мати широкомасштабне транскордонне чи глобальне значення, пов'язані із ризиками і небезпеками в інших сферах, посягаючи на національний інформаційний простір держави або міжнародну інформаційну безпеку.

З метою попередження і протидії існуючим та ймовірним загрозам інформаційній безпеці стратегічне завдання держави потягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки. Він передбачає послідовну системну діяльність, сукупність заходів і державно-правових інституцій, що покликані гарантувати безперешкодну реалізацію національних інтересів держави в інформаційній сфері, відповідних інтересів людини і суспільства, попередження інформаційних конфліктів та оперативне їх подолання.

Ключові слова: інформаційна безпека, забезпечення, загрози, законодавство, попередження, протидія, функції держави.

Shemchuk Viktor Viktorovych,
Candidate of Law, Associate Professor of the Department of Constitutional and International Law of the VI Vernadsky Tavrida National Humanities Institute, Honored Lawyer of Ukraine, 33 John McCain street, Kyiv, Ukraine, 529-05-16, vvshem.chuk@gmail.com, https//orcid.org/0000-0001-7969-6589

INFORMATION SECURITY THREATS: PROBLEMS OF DETERMINATION AND TROUBLESHOOTING

Abstract. This article explores threats to the information security of the state and the basis of the existing doctrinal and regulatory framework. A thorough analysis of the provisions of the Laws of Ukraine «On Fundamentals of National Security of Ukraine» in 2003, «On Basic Principles of Cyber Security of Ukraine» in 2017, «On National Security of Ukraine» in 2018, National Security Strategies of Ukraine 2015, Doctrines of Information Security of Ukraine 2017 demonstrates the lack of a unified approach to identifying and understanding the category of information security threats. Sometimes they are treated as threats to the national security of the state, as threats to the national interests and national security of Ukraine in the information sphere, cyber threats, etc.

In scientific journals, they are sometimes identified or, on the contrary, categorized in various ways by their various criteria. Threats to information security of Ukraine are considered by us as determining factors that cause and create negative phenomena that affect national interests in the information sphere, organization and functioning of the national information space as a whole. They can have wide-ranging cross-border or global implications for risks and dangers in other areas, affecting the national information space of the state or international information security.

With a view to preventing and counteracting existing and probable threats to information security, the strategic task of the state entails establishing and operating a mechanism for ensuring information security. It envisages a consistent systematic activity, a set of measures and state-legal institutions, which are designed to guarantee the smooth realization of the national interests of the state in the information sphere, the relevant interests of the individual and the society, prevention of information conflicts and their prompt resolution.

Keywords: information security, security, threats, legislation, prevention, counteraction, functions of the state.

Постановка проблеми. Сучасні інформаційні війни, поряд з іншими формами інформаційної боротьби і видами інформаційних конфліктів, є проявами більш широкої категорії – загроз національним інтересам та національній безпеці. Безумовно, предмет нашого вивчення становить не весь комплекс загроз, а власне загрози в інформаційній сфері, загрози інформаційній безпеці держави.

Аналіз останніх публікацій. Якщо поняття, сутність і зміст такого феномену як інформаційна безпека зазвичай аналізують дослідники належною мірою, то набагато менше уваги приділяється питанням небезпеки і загрозам сучасних держав. Прикметно, що не дивлячись на виокремлення самостійного напряму наукових досліджень – націобезпекознавства, порушена проблематика іноді актуалізується представниками науки міжнародного права, конституційного та адміністративного права, кримінального права, інформаційного права, державного управління, політології, історії, державної безпеки, військової науки тощо.

Так, слід згадати тих вітчизняних і зарубіжних учених, які зробили значний внесок у вивчення інформаційних впливів та небезпек, інформаційних війн і т.д.: Андрусів Г., Гафнер В., Демиденко В., Діордіца І., Забара І, Пазюк А., Почепцов Г., Камінська Н., Кормич Б., Костюк І., Кюль Д., Лібікі М., Ліпкан В., Любарський С., Моландер Р., Най Дж., Сасин Г., Сивак О., Ткачук П., Шевчук П., Цуканова О., Хорошко В., Щурко О. та ін.

Мета даної статті полягає у дослідженні загроз інформаційній безпеці держав, виокремленні їх різновидів, а також визначенні недоліків чинного законодавства України у даній сфері, ефективних шляхів їх попередження та протидії.

Виклад основного матеріалу. Враховуючи відсутність єдиного загальноприйнятого підходу до розкриття розуміння понять «інформаційна безпека»; «загрози інформаційній безпеці», а також їх активне поширення у суспільно-державному житті та на міжнародній арені з непередбачуваними переважно негативними наслідками, вважаємо доцільним привернення уваги наукової спільноти до даної проблематики. Насамперед, потребують розмежування однорідні та споріднені поняття «загроза», «ризик», «небезпека», «виклик» і т.д., а також «інформаційна загроза», інформаційний конфлікт», інформаційна війна», «інформаційне протистояння», «інформаційне протиборство», «інформаційний тероризм» тощо.

Звісно, першочергово слід звернутись до існуючих нормативно-правових актів у даній сфері. І протягом тривалого часу у полі зору законодавців перебували ці питання.

Ще Законом України «Про основи національної безпеки України» у ст. 7 (втратив чинність на підставі Закону № 2469-VIII від 21.06.2018) до загроз національним інтересам і національній безпеці в інформаційній сфері було віднесено наступні:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;

• розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

• намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [1].

У даному законі відсутнє трактування загроз інформаційній безпеці, але було визначено поняття «загрози національній безпеці» як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України (ст. 1); З огляду на врегулювання завдань забезпечення свободи слова та інформаційної безпеки, кібербезпеки та кіберзахисту, можна зробити висновок, що це одно порядкові і відмінні категорії, як і відповідні їм загрози.

У свою чергу, у Законі України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. Закріплено визначення «загрози національній безпеці України» –явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України. Вони згідно п. 5. ст. 3, як і 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 [2].

Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII більше уваги приділяє питаню гагроз у даній сфері. Зокрема, індикатори кіберзагроз визначаються як показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози. Кіберзагроза –наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. Тут розкриваються поняття кіберінцидентів та кібератак, кіберзлочинів (комп'ютерних злочинів), кібертероризму і- кібершпигунства тощо. [3].

У Доктрині інформаційної безпеки України», затвердженій Указом Президента України №47/2017 від 25 лютого 2017 року перелічено актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері.:

• 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 . [4].

Як бачимо, автори Доктрини, при виділенні загроз інформаційній безпеці держави, використали той самий підхід, що і до визначення національних інтересів в інформаційній сфері, тобто наявні повторення, неповнота переліку, термінологічна невизначеність, донесення однієї думки за рахунок різних формулювань тощо. Наприклад, декілька разів використовується поняття спеціальних інформаційних операцій, при цьому у національному законодавстві це поняття не розкривається і стає незрозумілим, чому загрозою визнаються лише спеціальні інформаційні операції. Крім того, при характеристиці першої загрози, розробники Доктрини не вказали від кого вона походить, напевно, мається на увазі РФ, однак при констатації наявності загрози, особливо у доктринальному документі, бажано чітко вказувати джерело її походження. Те саме стосується і формулювання загрози – «поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій», не уточнюється від кого походить ця загроза. В цілому ж закріплені у Доктрині положення щодо спеціальних інформаційних операції описують одну і ту саму загрозу – перманентну інформаційну війну РФ проти України, що здійснюється різними засобами як в українському національному інформаційному просторі так і в глобальному.

Що стосується термінологічної невизначеності, то розробники Доктрини інформаційної безпеки України дуже вільно оперують поняттями, зміст яких у законодавчих актах не розкривається. Зокрема використовуються поняття інформаційної експансії та інформаційного домінування без врахування особливостей їх співвідношення, яке наявне у науковій літературі.

Так, інформаційна експансія – це діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу а метою:

• поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії;

• витіснення положень національної ідеології і національної системи цін-

ностей і заміщення їх власними цінностями й ідеологічними установками;

• збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ;

• нарощування присутності власних ЗМІ в інформаційній сфері об'єкта проникнення і тому подібне [5].

При цьому, за критеріями масштабності, інтенсивності та характеру засобів, інформаційна експансія займає найнижчий рівень інформаційного протиборства, тоді як до найвищого рівня відносять інформаційну війну.

Водночас, як випливає з наведеного визначення інформаційної експансії, саме інформаційне домінування є однією з її цілей, і, відповідно, наслідком такої експансії. Таким чином, інформаційне домінування є складовою інформаційної експансії, тому є невірним виділення інформаційної експансії та інформаційного домінування як окремих загроз.

Певні питання викликає і віднесення авторами Доктрини до загроз таких проблем, як недосконалі законодавство та інформаційна інфраструктура, неефективність державної інформаційної політики та недостатній рівень медіа-культури суспільства. Враховуючи те, що мова йде про загрози інформаційній безпеці держави, яка є складовою національної безпеки, то в умовах гібридної війни з РФ, особи, які відповідальні за виникнення вказаних загроз, вочевидь, мають нести і кримінальну відповідальність. Однак, на практиці закріплення вказаних загроз у Доктрині інформаційної безпеки України не викликало належної реакції ані з боку громадянського суспільства, ані з боку державних органів.

На наш погляд, недоліки аналізу загроз інформаційної безпеки, що викладені у Доктрині, також зумовлені відсутністю відповідного переліку загроз у профільному законі. На сьогодні, більш детальний перелік загроз в інформаційній сфері, представлений у Стратегії національної безпеки України (далі – Стратегія), яка була введена у дію Указом Президента № 287/2015 від 26.05.2015 р.

Відповідно до п. 3.6. Стратегії загрозами інформаційній безпеці є: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Згідно з п. 3.7. Стратегії загрозами кібербезпеці і безпеці інформаційних ресурсів виступають: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом. Пунктом 3.8. Стратегії визначені загрози безпеці критичної інфраструктури, а саме: критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення [6].

Отже, п.п. 3.6., 3.7, та 3.8. Стратегії присвячені загрозам інформаційній безпеці, загрозам кібербезпеці і безпе-

ці інформаційних ресурсів та загрозам безпеці критичної інфраструктури. На наш погляд, поділ загроз на вказані групи не є вдалим, оскільки не враховано структуру механізму забезпечення інформаційної безпеки держави та місце елементів у ньому. Зокрема, загрози інформаційній безпеці є широким поняттям, яке включає загрози кібербезпеки, інформаційної інфраструктури тощо. Водночас складовою інформаційної інфраструктури є критично важлива інформаційна інфраструктура. Разом з тим, аналіз загроз в інформаційній сфері, закріплений у Стратегії, є більш ґрунтовним. На наш погляд, доцільно було б його врахувати при розробці Доктрини інформаційної безпеки України. Адже, враховуючи принцип загального і спеціального нормативного акту, спеціальний, доктринальний документ повинен містити всебічний та повний аналіз стану інформаційної безпеки, в тому числі і в аспекті існуючих загроз.

Таким чином, на підставі вивчення положень Доктрини інформаційної безпеки України, закріплені у ній загрози інформаційної сфери можна класифікувати за джерелом походження на зовнішні та внутрішні.

Зовнішні загрози: – проведення державою-агресором спеціальних інформаційних операції проти України, як на її території, так і поза її межами; – інформаційна експансія та інформаційне домінування держави-агресора.

Внутрішні загрози включають : недостатню розвиненість національної інформаційної інфраструктури; неефективність державної інформаційної політики; недосконаліть законодавства; невизначеність стратегічного наративу; недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Наведена класифікації загроз чітко вказує на помилковий аналіз ситуації у сфері інформаційної безпеки держави, що був проведений авторами Доктрини інформаційної безпеки України. В умовах гібридної війни, не є правильним у профільному доктринальному документі зазначати лише про дві загрози, що походять з боку держави-агресора, та зазначати про шість внутрішніх загроз, які створюються самим органами державної влади та суспільством. Така оцінка ситуації знижує ефективність механізму забезпечення інформаційної безпеки.

Не можна не згадати суб'єктів механізму забезпечення інформаційної безпеки, якими виступає особа, суспільство (його певні групи чи об'єднання) та держава (в цілому, окремі державні органи та органи місцевого самоврядування). У Доктрині інформаційної безпеки України суб'єкти прямо не визначаються, але аналіз Розділу Доктрини щодо механізму її реалізації дозволяє виділити таких суб'єктів забезпечення інформаційної безпеки держави, як-то: Рада національної безпеки і оборони України; Кабінет Міністрів України; Міністерство інформаційної політики України; Міністерство закордонних справ України; Міністерство оборони України; Міністерство культури України; Державне агентство України з питань кіно; Національна рада України з питань телебачення і радіомовлення; Державний комітет телебачення і ра-

діомовлення України; Служба безпеки України; Розвідувальні органи України; Державна служба спеціального зв'язку та захисту інформації України; Національний інститут стратегічних досліджень.

Зокрема, на Міністерство інформаційної політики України покладені в установленому порядку організація та забезпечення моніторингу загроз національним інтересам і національній безпеці в інформаційній сфері тощо [5].

З наведеного переліку випливає, що у Доктрині визначені суб'єкти забезпечення інформаційної безпеки – державні органи, а відповідні суб'єкти на рівні суспільства та особи не згадуються. Прикметно, що у Доктрині інформаційної безпеки РФ окремий пункт присвячений переліку суб'єктів, які складають організаційну основу системи забезпечення інформаційної безпеки, зокрема визначено 12 таких суб'єктів та 12 учасників системи у цій сфері [7].

Можна погодитись з В.О. Демиденко, Н.В. Камінською у тому, що важливим є покладення відповідних повноважень, а також відповідальності на інші органи публічної влади центрального, регіонального і локального рівнів, зокрема, органи місцевого самоврядування у законодавстві України в даній сфері [8-9]. На наш погляд, чим чіткіше встановлено коло суб'єктів забезпечення інформаційної безпеки, тим краще розуміння уповноваженими суб'єктами механізму такого забезпечення, і, як наслідок, підвищення його ефективності.

Отже, аналіз деяких нормативно-правових актів демонструє відсутність на законодавчому рівні поняття загроз інформаційній безпеці держав. Тому варто звернутись до доктринальних джерел, енциклопедичних та інших наукових видань. Найбільш широко загрози інформаційним ресурсам розглядають як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, що зберігається в ній. Виникнення загрози, тобто віднаходження джерела актуалізації певних подій у загрози характеризується таким елементом як уразливість. Саме за наявності вразливості як певної характеристики системи і відбувається активізація загроз. А самі загрози за своєю суттю відповідно до теорії множин є невичерпними, а отже й не можуть бути піддані повному описові у будь-якому дослідженні [10].

Загроза (англ. *threat*) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають «атакою». Загроза безпеці інформації (англ. *security threat*) – загрози викрадення, зміни або знищення інформації. Вони бувають випадковими або навмисними. [11]. До загроз інформаційній безпеці системі управління національною безпекою належать: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання. Через їх чисельність відповідно до загальної класифікації загроз національній безпеці, виокремлюють загрози інформаційній безпеці за різними критеріями.

За джерелами походження: – природного походження (масове руйнування через природні катаклізми

каналів зв'язку), – техногенного походження (аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів системи управління національною безпекою тощо) – антропогенного походження (помилковий запуск програми, (не)навмисне допущення через недотримання правил безпеки роботи в Інтернеті інсталяції закладок тощо).

За характером реалізації: – реальні (активізація шляхів дестабілізації є неминучою і не обмежена часом і простором); – потенційні (шляхи дестабілізації можливі за певних умов середовища функціонування органів публічної влади); – здійснені (загрози втілені у життя); – уявні (умовні чи схожі з існуючими, але такими не є).

За ступенем гіпотетичної шкоди: – загроза (явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів у інформаційній сфері і створюють небезпеку для системи управління національною безпекою, життєзабезпечення її системостворюючих елементів); – небезпека (безпосередня дестабілізація функціонування системи управління національною безпекою).

За ймовірністю реалізації: – вірогідні (за виконання певного комплексу умов обов'язково настануть., наприклад, оголошення атаки інформаційних ресурсів, що передує власне атаці); – неможливі (за виконання певного комплексу умов ніколи не настануть, переважно мають більш декларативний характер, не підкріплений реальною і навіть потенційною можливістю здійснити проголошені наміри, вони здебільшого мають залякуючий характер); – випадкові (за виконання певного комплексу умов протікають по-різному, їх аналізують за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах).

За рівнем детермінізму: випадкові (загрози, які можуть трапитися або не трапитися – загрози хакерів дестабілізувати інформаційній системи органів влади), закономірні (загрози стійкого, повторюваного характеру, зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки, – численні атаки хакерів на офіційні сайти ФБР, ЦРУ США) [10-12].

Цей перелік, звісно, можна продовжувати, але очевидний наступний висновок. Так, поняття загрози розглядаються переважно абстрактно або спрощено, подекуди звужено, відірвано від контексту поняття «інформаційна безпека» і майже не пов'язано із контекстом родового поняття «загроза».

Загрози інформаційній безпеці України розглядаються нами як детермінуючі фактори, що зумовлюють і породжують негативні явища, які посягають на національні інтереси в інформаційній сфері, організацію та функціонування національного інформаційного простору загалом. Вони мають або можуть мати широкомасштабне значення, пов'язані із ризиками і небезпеками в інших сферах.

Так, у законодавстві України регламентовані загрози національній безпеці України на сучасному етапі розвитку нашого суспільства і держави існують у зовнішньополітичній сфері, у сфері державної безпеки, у воєнній сфері та сфері безпеки державного кордону України, у внутрішньополітичній сфері, в економічній сфері, у соціальній та гуманітарній сферах, у

науково-технологічній сфері, у сфері цивільного захисту, в екологічній сфері, в інформаційній сфері. Безпосередньо детермінують посягання на інформаційну безпеку, так само як і на державний суверенітет і територіальну цілісність держави України такі загрози як претензії з боку інших держав світу, глобалізація світових відносин і зосередження важелів впливу на світові процеси в руках окремих осіб або груп, прояв сепаратизму і намагання автономізації за етнічною ознакою окремих регіонів України/ Усі інші загрози національній безпеці України можуть прямо і не створювати небезпеку посягання, але тією чи іншою мірою підривають ці фундаментальні цінності держави та суспільства [13].

Слід підкреслити, що загрози інформаційній безпеці держави виходять за межі географічних кордонів держав, посягають на національний інформаційний простір, але можуть мати транскордонні чи глобальні негативні наслідки.

Висновки. Необхідність подальшого вивчення і розроблення чіткого поняття «загроза» є нагальною і має бути спрямована на формування ефективної і реальної системи моніторингу та управління загрозами, та іншими ризиками для інформаційної безпеки держави.

З метою попередження і протидії існуючим та ймовірним загрозам інформаційній безпеці стратегічне завдання держави потягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки. Він передбачає послідовну системну діяльність, сукупність заходів і державно-правових інституцій, що покликані гарантувати безперешкодну реалізацію національних інтересів держави в інформаційній сфері, відповідних інтересів людини і суспільства, попередження інформаційних конфліктів та оперативне їх подолання. Враховуючи активну глобалізацію інформаційно-комунікаційних мереж важливо не тільки державам, а й міжнародним організаціям долучатись до співпраці у напрямі протидії різноманітним видам інформаційної агресії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про основи національної безпеки України: Закон України від 19 червня 2003 року № 964-IV URL:https://zakon.rada.gov.ua/laws/show/964-15

2. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/

3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. *Офіційний вісник України.* 2017. № 91. Ст. 2765.

4. Доктрина інформаційної безпеки України: Затверджена указом Президента України від 25 лютого 2017 року №47/2017. Київ: *Офіційний вісник України*, 2017. № 20.

5. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с.

6. Стратегія національної безпеки України: введена у дію Указом Президента від 26.05.2015 р. № 287/2015. *Офіційний вісник України*, 2015. № 43, Ст. 1353.

7. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646. *Собрание законодательства РФ.* 2016. № 50. Ст. 7074.

8. Демиденко В.О. Принципи застосування органами місцевого самоврядування законодавства України в сфері кібербез-

пеки. *Юридичний часопис НАВС*. 2018. №1. С. 141-153.

9. Камінська Н.В. Проблеми імплементації міжнародно-правових стандартів у сфері кібербезпеки. *Розвиток науки і практики міжнародного права: матеріали м*іжнар. науково-практ. конфер., присвяченій 25-річчю УАМП. К., 2018.

10. Політологія URL:.https://pidruchniki.com/15341220/politologiya/ponyattya_vidi_zagroz_natsionalnim_interesam_natsionalniy_bezpetsi_informatsiyniy_sferi

11. Інформаційна_загроза. URL:https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B0

12. Богуш В. М., Кривуца В. Г., Кудін А. М., Інформаційна безпека: Термінологічний навчальний довідник/ За ред. Кривуци В. Г. К., 2004. 508 с.

13. Носач А.В. Загрози національній безпеці як обов'язкова ознака злочинності, що посягає на державний суверенітет і територіальну цілісність України. *Право і суспільство*. 2019. №3. С. 50–56.

14. Ткачук П.П., Гула Р.В., Сивак О.І., Щурко О.М., Шемчук В.В. Інформаційна війна і національна безпека: монографія. Л.: НАСВ, 2015. 265 с.

15. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посіб. К.: Кондор, 2008. 382 с.

REFERENCTES:

1. Pro osnovy nacional`noyi bezpeky Ukrayiny: Zakon Ukrayiny vid 19 cherv. 2003 roku № 964-IV [The Law of Ukraine «On the basics of Ukraine's national security»]. (2003 June 19) zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/964-15 [in Ukrainian].

2. Pro nacional`nu bezpeku Ukrayiny: Zakon Ukrayiny vid 21 cherv. 2018 roku № 2469-VIII [The Law of Ukraine «On the of Ukraine's national security»] (2018 June 21) zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/ [in Ukrainian].

3. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny: Zakon Ukrayiny vid 5 zhovt. 2017 roku № 2163-VIII [The Law of Ukraine «On the basic principles of cyber security in Ukraine»] (2017 October 5). *Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine,* 91, pp. 2765 [in Ukrainian].

4. Doktryna informacijnoyi bezpeky Ukrayiny: Zatverdzhena ukazom Prezydenta Ukrayiny vid 25 lyut. 2017 roku № 47/2017 [Doctrine of Information Security of Ukraine: Approved by the decree of the President of Ukraine] (2017 February 25). *Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine*, 20 [in Ukrainian].

5. Lipkan V.A., Maksymenko Y.Y., Zhelixovs`kyj V.M. (2006). Informacijna bezpeka Ukrayiny v umovax yevrointegraciyi: Navchal`nyj posibnyk [Information Security of Ukraine in the Context of European Integration: A textbook]. K.: KNT. [in Ukrainian].

6. Strategiya nacional`noyi bezpeky Ukrayiny: vvedena u diyu Ukazom Prezydenta vid 26 trav. 2015 roku № 287/2015 [Ukraine's National Security Strategy: Enacted by Presidential Decree] (2015 May 26). *Oficijnyj visnyk Ukrayiny – Official Bulletin of Ukraine,* 43, pp. 1353 [in Ukrainian].

7. Ob utverzhdeny`y Doktryny nformacyonnoj bezopasnosty Rossyjskoj Federacy`y: Ukaz Prezydenta RF ot 05 dek. 2016 № 646 [On approval of the Information Security Doctrine of the Russian Federation: Presidential Decree]. (2016 December 5). *Sobranye zakonodatel`stva RF – Legislative vault RF*, 50, pp. 7074. [in Russian].

8. Demydenko, V.O. (2018). Pryncypy zastosuvannya organamy miscevogo samovryaduvannya zakonodavstva Ukrayiny v sferi kiberbezpeky [Principles of local self-government enforcement in the field of cybersecurity legislation]. *Yurydychnyj chasopys NAVS – Law magazine NAVS*, №1, 141-153. [in Ukrainian].

9. Kamins`ka, N.V. (2018). Problemy implementaciyi mizhnarodno-pravovy`x standartiv u sferi kiberbezpeky [Problems of implementation of international legal standards in cybersecurity]. Materialy mizhnar. naukovo-prakt. konfer., prysvyachenij 25-richchyu UAMP «Rozvytok nauky i praktyky mizhnarodnogo prava» – Materials international scientific-practice. conference dedicated to the 25th anniversary of UAMP «The development of the science and practice of international law».[in Ukrainian].

10. Politologiya [Politology]. Retrieved from https://pidruchniki.com/15341220/politologiya/ponyattya_ vidi_zagroz_ natsionalnim_interesam_natsionalniy_ bezpetsi_informatsiyniy_sferi [in Ukrainian].

11. Informacijna_zagroza [Information threat]. Retrieved from https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B0. [in Ukrainian].

12. Bogush, V.M., Kryvucza, V.G., Kudin, A.M. (2004). Informacijna bezpeka: Terminologichnyj navchalnyj dovidnyk/ Za red. Kryvucy V.G. [Information Security: A Terminological Training Handbook]. K., 508 p. [in Ukrainian].

13. Nosach, A.V. (2019). Zagrozy nacional`nij bezpeci yak obov'yazkova oznaka zlochynnosti, shho posyagaye na derzhavnyj suverenitet i terytorial`nu cilisnist` Ukrayiny [Threats to national security as a mandatory feature of crime that impinges on the state sovereignty and territorial integrity of Ukraine]. *Pravo i suspil`stvo – Law and Society,* №3, pp. 50–56. [in Ukrainian].

14. Tkachuk, P.P., Gula, R.V., Sy`vak, O.I., Shhurko, O.M., Shemchuk, V.V. (2015). Informacijna vijna i nacional`na bezpeka: monografiya. [Information warfare and national security]. L.: NASV. [in Ukrainian].

15. Kormych, B.A. (2008). Informacijna bezpeka: organizacijno-pravovi osnovy: navch. posib. [Information Security: Organizational and Legal Basis]. K.: Kondor. [in Ukrainian].