

УДК 351.746

DOI: <https://doi.org/10.32782/2224-6282/176-28>**Дикий А. П.**

к.е.н., доцент кафедри національної безпеки,
публічного управління та адміністрування,
Державний університет «Житомирська політехніка»
ORCID: <https://orcid.org/000-0002-5819-0236>

Научук К. М.

доктор філософії, асистент кафедри національної безпеки,
публічного управління та адміністрування,
Державний університет «Житомирська політехніка»
ORCID: <https://orcid.org/0000-0002-4195-5124>

Тростенюк Т. М.

доктор філософії, доцент кафедри національної безпеки,
публічного управління та адміністрування,
Державний університет «Житомирська політехніка»
ORCID: <https://orcid.org/0000-0001-7130-7454>

Dykyi Anatolii, Naumchuk Kateryna, Trosteniuk Tetiana
Zhytomyr Polytechnic State University

АНАЛІЗ СУЧАСНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ

В сучасному світі досить складно уявити людину, яка була б позбавлена доступу до інформативних ресурсів, адже інформатизація проникла абсолютно у всі сфери суспільного життя, є одним із чинників ефективного соціально-економічного, культурного та духовного розвитку кожного в майбутньому. Разом з розвитком, інформаційній сфері притаманно нести й загрозу, яка є ключовим елементом в гібридній війні проти України, реальною загрозою якої є не лише підбурювання громадян, але й створення реальних загроз національній безпеці всієї країни. Наступні десятиріччя для всіх держав світу будуть обумовлені специфічними випробуваннями та розвитком інформаційно-комунікаційних технологій. Для кожної країни характерні свої закони, звичаї, традиції, норми поведінки та ідеологічні цінності. Тому, одним з основних завдань серед людей, організацій та її в межах всієї країни захист національної безпеки держави та захист інформаційного простору є основою гарантування інформаційної безпеки. Швидше формування інформатизованого суспільства, його поширення та укорінення набуває особливого значення при вирішенні проблем інформаційної безпеки. На відміну від інших сфер життєдіяльності, інформаційна існує не з метою потенційного заробітку, оскільки сфера потребує значних інвестицій з метою захисту установ від втрат, які пов'язані з витоком інформаційних ресурсів. Враховуючи всі чинники – загрози інформаційній безпеці зустрічаються досить часто, що пов'язано з знаходженням зловмисниками слабких місць, завдяки яким можна пошкодити інформаційні ресурси. Мобільність громадян є щоденною, але не всі користувачі піклуються про захист персональних даних, їх збереженість та недоторканість. Дослідження існуючих загроз займалися вчені з різних країн світу, проте не кожен зміг зробити чіткий поділ загроз та їх попередження, саме тому, обрана тема дослідження є актуальною та потребує детального вивчення та практичного вирішення. Розробка та реалізація практичних заходів протидії загрозам інформаційної безпеки є можливою завдяки постійній взаємодії усіх суб'єктів інформаційної взаємодії з органами державної влади, про що йдеться у статті. Метою статті є здійснення аналізу сучасних загроз інформаційній безпеці держави в контексті забезпечення національної безпеки України.

Ключові слова: інформація, інформаційна сфера, інформаційна безпека, національна безпека, загроза, держава, національна інформаційна безпека.

ANALYSIS OF CURRENT THREATS TO THE INFORMATION SECURITY OF THE STATE

In today's world it is difficult to imagine a person who would be deprived of access to information resources, because informatization has penetrated into all spheres of public life, is one of the factors of effective socio-economic, cultural and spiritual development of everyone in the future. Along with development, the information sphere also has a threat, which is a key element in the hybrid war against Ukraine, the real threat of which is not only inciting citizens, but also creating real threats to national security throughout the country. The next decades for all countries of the world will be conditioned by specific tests and development of information and communication technologies. Each country has its own laws, customs, traditions, norms of behavior and ideological values. Therefore, one of the main tasks among people, organizations and throughout the country is the protection of national security and protection of the information space is the basis for ensuring information security. Faster formation of an informatized society, its spread and rooting becomes especially important in solving information security problems. Unlike other spheres of life, information does not exist for the purpose of potential earnings, as the sphere needs significant investments to protect institutions from losses associated with the leakage of information resources. Given all the factors – threats to information security are quite common, due to the fact that criminals find vulnerabilities that can damage information resources. Citizens' mobility is daily, but not all users care about the protection of personal data, their safety and inviolability. Scientists from around the world have studied existing threats, but not everyone has been able to make a clear division of threats and their prevention, which is why the chosen research topic is relevant and needs detailed study and practical solutions. The development

and implementation of practical measures to combat information security threats is possible through the constant interaction of all subjects of information interaction with public authorities, as discussed in the article. The purpose of the article is to analyze the current threats to information security of the state in the context of ensuring the national security of Ukraine.

Keywords: information, information sphere, information security, national security, threat, state, national information security.

JEL classification: C41, F52, J28

Постановка проблеми. Основним фактором, який впливає на здатність держави протистояти загрозам проявляється у встановленні взаємодії країни та її відкритістю до зовнішніх впливів. В такому випадку держава втрачає свій монополізм на території, політичні сили стають обмеженими адже відбувається корегування в залежності від впливу країн – сусідів.

Глобалізаційний розвиток більшості процесів відбувається завдяки всеосяжній інформатизації та різноманітності можливих загроз внутрішнього та зовнішнього середовища.

Аналіз останніх досліджень і публікацій. Питання інформаційної безпеки та захисту національного інформаційного простору досліджували як вітчизняні так і зарубіжні вчені, зокрема: В. Гафнер [2], І. Діордіца [6], Б. Кормич [4], В. Ліпкан [6], А. Марущак [7], Г. Сашук [11], В. Петрик [8], Г. Почепцов [9] та ін. Однак питання аналізу сучасних загроз інформаційній безпеці держави залишаються дослідженими фрагментно і потребують глибокого дослідження даного питання.

Мета статті полягає в здійсненні аналізу сучасних загроз інформаційній безпеці держави в контексті забезпечення національної безпеки України.

Вклад основного матеріалу. Для більш детальної класифікації можливих загроз необхідно розглянути поняття, які безпосередньо стосуються інформаційної сфери та інформаційної безпеки.

Першим поняттям є поняття інформаційної безпеки, яка відображає стан захищеності найбільш важливих інтересів громадян, держави та суспільства, завдяки якому необхідно запобігати завданню шкоди інформації, її неякісному, недобросовісному та несвоєчасному поширенню.

Наступним є поняття загроза інформаційній безпеці – це явища та чинники наявного та потенційного характеру, які за збігом певних обставин створюють небезпеку для життєво важливих інтересів людини та громадяни, суспільства, держави.

Інформаційний продукт – це візуальний (аудіо чи друкований) продукт, який призначено для задоволення існуючих інформаційно-комунікативних потреб громадського суспільства, який створено громадянами відповідно до чинного законодавства.

Інформаційна політика держави – діяльність, спрямована на формування та регулювання інформаційного середовища в якому відбувається задоволення потреб комунікативного характеру громадян країни.

Національним інформаційним простором є сукупність інформаційних потоків різного характеру (національного та іноземного походження), які є доступними на всій території країни.

Інформаційною сферою є сукупність технологій, ресурсів, послуг та продуктів інформаційного характеру між суб'єктами інформаційної діяльності щодо регулювання відносин інформаційного характеру.

Спільною рисою усіх складових інформаційного простору є інформація, яка потребує захисту від внутрішніх та зовнішніх загроз.

Інформаційному суспільству притаманний свій розвиток, який має низку проблем організаційно-правового характеру до якого відносять [10]:

- відсутність стратегічного рівня забезпечення інформаційної безпеки;

- неналежний рівень супроводження зовнішньої та внутрішньої інформаційної політики України;

- автономність державних установ, основне завдання яких є забезпечення інформаційної безпеки України, дублювання їх повноважень та недостатня якість наявної координаційної складової;

- відсутність дієвих механізмів експертної оцінки інформаційної продукції, поширення якої створює загрозу інформаційній безпеці щодо прав людини, інтересам суспільства та держави;

- відсутність ефективних механізмів залучення громадськості та приватного сектору України до протидії негативним інформаційним впливам, міжнародної співпраці у цій сфері;

- наявність законодавчих та організаційних прогалин у сфері обігу інформації з обмеженим доступом.

При цьому сучасні виклики інформаційній безпеці України зумовлені як внутрішніми, так і зовнішніми чинниками [10]:

- внутрішніми є чинники, які виникають в межах однієї країни. Характерною ознакою є: відсталість інформаційних технологій в Україні від провідних країн світу, низький рівень інформатизації, розпорошеність повноважень органів державної влади та законодавства в інформаційній сфері;

- зовнішніми є загальносвітові тенденції щодо створення та застосування технологій інформаційного характеру та намаганнями іноземних суб'єктів впливати на вітчизняний інформаційний простір з метою забезпечення власних інтересів.

Отже, на сучасному етапі становлення та укріплення позицій Україні слід зосередитись на двох пріоритетних напрямках:

- першим напрямом є необхідність оновлення внутрішнього українського простору задля підвищення його конкурентоспроможності;

- другим напрямом є необхідність забезпечення інформаційної присутності держави та просування її.

Таким чином, враховуючи вищезазначений матеріал слід зауважити, що загрози інформаційної безпеки мають комплексний характер та включають в себе такі види загроз як:

- загрози безпеки інформації та всієї інформаційної структури;

- загрози суб'єктів інформаційної сфери;

- загрози реалізації прав та усіх інтересів учасників.

Доцільно погодитись, що сукупність умов та факторів загроз інформаційній безпеці держав несуть небезпеку найбільш важливим інтересам суспільства.

Якщо враховувати політичну ситуацію між країнами, на сьогоднішній день найбільш небезпечними загрозами інформаційній безпеці є транскордонний вплив, яких проявляється в рамках інформаційної

війни. Станом на сьогодні інформаційною війною прийнято вважати цілеспрямований вплив інформаційного характеру в якому відбувається не опосередковане використання та заволодіння інформацією яка не перебуває в загальному доступі.

Інформаційна війна є найвищим ступенем інформаційного протиборства яка повинна розв'язати суспільно – політичних, ідеологічних та інформаційних протистоянь.

Для України основною загрозою є віртуалізація, яка є соціальним відчуженням людини, зміною її свідомості, переходом до віртуального світу їх перебування. Прискорені темпи інформатизації породжують виникнення ще однієї загрози, яка перетворить людину на додаток до існуючих інформаційних технологій. Саме тому, виникає необхідність забезпечувати не лише безпеку інформації але й усього суспільства, яке є носієм усіх глобальних загроз.

Безпека інформаційної сфери України, враховуючи всі основні чинники та можливі прояви складається з таких основних складових як:

- персональної, що відображає власне ставлення особи до захисту інформаційних даних;
- публічної, яка відображає ставлення суспільства до важливості збереження даних;
- комерційної – ставлення організацій до захисту своїх таємниць;
- державної – ставлення держави до захисту інформації яка відповідає за національні цінності та інтереси.

Тому, визначення характеру ризиків передбачає врахування таких елементів як:

- врахування концепцій політичної безпеки;
- відповідність чинному законодавству;
- конкретизація об'єктів та цілей;
- оцінка можливих ризиків.

Інформаційна політика держави повинна оцінювати основні елементи та відповідати на їх ключові питання задля забезпечення законних прав та захисту інтересів.

Для вирішення загроз, які існують в сфері інформаційної безпеки першочерговими напрямками ми пропонуємо:

- удосконалити правове забезпечення інформаційної безпеки. Реалізувати це можливо шляхом визначення нових або уточнення існуючих завдань, функцій і повноважень суб'єктів забезпечення інформаційної безпеки України;
- забезпечити інформаційний суверенітет України.

Основна мета цього напрямку проявляється у недопущення будь якої інформаційної залежності та інформаційної експансії з боку інших держав чи міжнародних структур;

- сприяти розвитку міжнародного співробітництва інформаційної сфери в умовах перегляду його основних принципів і механізмів. Є необхідним для посилення міжнародно-правової відповідальності за використання сил і засобів, які негативно впливають або створюють загрози людині, суспільству, державі;

- зміцнити організаційні основи забезпечення інформаційної безпеки шляхом: вирішення основного питання координації діяльності суб'єктів які забезпечують інформаційну безпеку що стосується сфери протидії інформаційної агресії, забезпечення кібернетичної безпеки України;

- налагодити систему державно-приватного партнерства сфери забезпечення інформаційної безпеки;

- запровадити систему контролю демократичного характеру за діяльністю державних суб'єктів забезпечення інформаційної безпеки;

- модернізувати комунікаційну політику у стосунках “державо-суспільство”.

Разом з зазначеними напрямками, необхідною є розробка програм освітньо-виховного впливу, яка була б спрямована на формування основних властивостей забезпечення власної інформаційної безпеки, зокрема підвищення рівня культури використання засобів оброблення інформації, оприлюднення власної інформації та способів її захисту, критичного ставлення до інформації [1; 3; 5; 12; 13].

Для вирішення існуючих загроз державна інформаційна політика повинна базуватись на забезпеченні прав на надання достовірної, повної та своєчасної інформації кожному громадянину а також забезпечувати їх свободу щодо вираження думок, недопущення втручання третіх осіб у внутрішнє середовище інформаційних процесів, крім випадків, які можуть передбачатись чинним законодавством України.

Висновки. Отже, інформаційна безпека є складним, системним та багаторівневим явищем, яке перебуває під впливом постійного впливу чинників внутрішнього та зовнішнього середовища, з врахуванням політичної світової обстановки, мікроклімату в середині самої держави, стану та рівня інформацій-комунікаційної обстановки держав світу.

Наявність загроз, які стосуються інформаційної безпеки більшою мірою супроводжуються існуванням загроз в економічній, політичній, державно-управлінській та інших сферах. Загрози, які виникають в інформаційній сфері зумовлені загрозами, які інших сфер, які мають дотичний характер до інформації, і за рахунок інформаційних ресурсів несуть руйнівні наслідки.

Список використаних джерел:

1. Боднар І.Р. Роль держави у формуванні інформаційної політики. *Вісник ЛКА*. 2011. № 34. С. 291–296.
2. Гафнер В.В. Информационная безопасность : учебное пособие в 2 ч.; ГОУ ВПО «Урал. гос. пед. ун-т». Екатеринбург, 2009. Ч. 1. 155 с.
3. Державна інформаційна політика. URL: <http://mereg.org.ua/law/projects/derzhpolityka>
4. Кормич Б.А. Інформаційна безпека: організаційно-правові основи : навч. посібник. Київ : Кондор, 2004. 384 с. С. 67–401.
5. Куцька О.М. Особливості інформаційно-психологічного впливу Російської Федерації напередодні та початковому етапі антитерористичної операції на сході України. *Інформаційна безпека людини, суспільства, держави*. 2017. № 1(21). С. 180–190.
6. Ліпкан В.А., Діордіца І.В. Національна безпека України: кримінально-правова охорона : навчальний посібник. Київ : КНТ, 2007. 227 с.
7. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України*. 2011. № 21. С. 92–95.
8. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. № 5. С. 122–134.
9. Почепцов Г. Сучасні інформаційні війни. Київ : Вид. дім “Кисево-Могілянська академія”, 2015. 497 с.

10. Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964-IV (втратив чинність). URL: <https://zakon.rada.gov.ua/laws/show/964-15#Text>
11. Сашук Г. Інформаційна безпека в системі забезпечення національної безпеки. *Бизнес и безопасность*. 2014. № 1. С. 46–50.
12. Сопілко І.М. Інформаційні загрози та безпека сучасного українського суспільства. *Юридичний вісник*. 2015. № 1(34). С. 75–80.
13. Thor Olavsrud. 4 information security threats that will dominate 2017. CIO (December 29, 2016). URL: <https://cio.com/article/3153706/security/4-information-security-threats-thatwill-dominate-2017.html>

References:

1. Bodnar, I.R. (2011) *Rol'derzhavy u formuvanni informacijnoi' polityky* [The role of the state in shaping information policy]. *Visnyk LKA*, no. 34, pp. 291–296.
2. Gafner, V.V. (2009) *Informatsionnaya bezopasnost'* [Information Security]; GOU VPO «Ural. gos. ped. un-t». Ekaterinburg, ch. 1, 155 p. (in Russian)
3. Derzhavna informacijna polityka [State information policy]. Available at: <http://merega.org.ua/law/projects/derzhpolityka> (accessed 23 November 2021).
4. Kormych, B.A. (2004) *Informacijna bezpeka: organizacijno-pravovi osnovy* [Information security: organizational and legal bases]. Kyiv: Kondor, 384 p., pp. 67–401. (in Ukrainian)
5. Kuc'ka, O.M. (2017) Osoblyvosti informacijno-psyhologichnogo vplyvu Rosijs'koi' Federacii' naperedodni ta pochatkovomu etapi antyterrorystychnoi' operacii' na shodi Ukrainy [Features of information and psychological influence of the Russian Federation on the eve and the initial stage of the anti-terrorist operation in eastern Ukraine]. *Informacijna bezpeka ljudyny, suspil'stva, derzhavy*, no. 1(21), pp. 180–190.
6. Lipkan, V.A. and Diordica, I.V. (2007) *Nacional'na bezpeka Ukrainy: kryminal'no-pravova ohorona* [National Security of Ukraine: Criminal Protection]. Kyiv: KNT, 227 p. (in Ukrainian)
7. Marushhak, A.I. (2011) Informacijno-pravovi naprjamy doslidzhennja problem informacijnoi' bezpeky [Information and legal directions of research of information security problems]. *Derzhavna bezpeka Ukrainy*, no. 21, pp. 92–95.
8. Petryk, V. (2009) Sutnist' informacijnoi' bezpeky derzhavy, suspil'stva ta osoby [The essence of information security of the state, society and the individual]. *Jurydychnyj zhurnal*, no. 5, pp. 122–134.
9. Pohepcov, G. (2015) *Suchasni informacijni vijny* [Modern information wars]. Kyiv: Vyd.dim “Kyjevo-Mogyljans'ka akademija”, 497 p. (in Ukrainian)
10. Pro osnovy nacional'noi' bezpeky Ukrainy [On the foundations of national security of Ukraine]: Zakon Ukrainy vid 19.06.2003 r. № 964-IV (vtratyv chynnist'). Available at: <https://zakon.rada.gov.ua/laws/show/964-15#Text> (accessed 23 November 2021).
11. Sashhuk, G. (2014) Informacijna bezpeka v systemi zabezpechennja nacional'noi' bezpeky [Information security in the system of national security]. *Biznes i bezopasnost'*, no. 1, pp. 46–50.
12. Sopilko, I.M. (2015) Informacijni zagrozy ta bezpeka suchasnogo ukrai'ns'kogo suspil'stva [Information threats and security of modern Ukrainian society]. *Jurydychnyj visnyk*, no. 1(34), pp. 75–80.
13. Thor Olavsrud (2016) 4 information security threats that will dominate 2017. CIO. Available at: <https://cio.com/article/3153706/security/4-information-security-threats-thatwill-dominate-2017.html> (accessed 23 November 2021).