

IEEE Region 10 Conference (TENCON), 2019, стр. 1564–1571, doi: 10.1109 / TENCON.2019.8929316.

6. Bots in libr Bots in libraries: The aries: They're coming for coming for your jobs (or is it?) our jobs (or is it?). URL: https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=1142&context=library_research. (Дата звернення 5.06.2022).
7. Cdns' dark side: identifying security problems in cdn-to-origin connections. URL: <https://users.encs.concordia.ca/~mmannan/student-resources/Thesis-MASc-Shobiri-2021.pdf>. (accessed 5.06.2022). (Дата звернення 5.06.2022).
8. Abegaz B. W. DNS Services, alternative ways of using DNS infrastructures. – Delft: TNO, 2011. URL: <https://repository.tudelft.nl/islandora/object/uuid:1e0114b7-d907-499e-bb20-fa83753d8067/datastream/URL/download>. (Дата звернення 5.06.2022).
9. Задерейко О. В., Трофименко О. Г., Прокоп Ю. В., Логінова Н. І., Кухаренко С. В. Аналіз витоків даних у інформаційних системах. Сучасна спеціальна техніка. № 3 (66), 2021. С. 16-30.
10. NoRoot Firewall. URL: <https://play.google.com/store/apps/details?hl=en&id=app.greyshirts.firewall>. (Дата звернення 5.06.2022).
11. Windows Firewall Control. URL: <https://binisoft.org/wfc>. (Дата звернення 5.06.2022).

Ключові слова: месенджер Telegram, витoki метаданих в Telegram, вихідні мережеві з'єднання Telegram, конфіденційність месенджера Telegram.

Key words: Telegram messenger, Telegram metadata leaks, Telegram outgoing network connections, Telegram messenger privacy.

ТОМА МАРІАНА ГЕОРГІЙВНА

*Чернівецький національний університет імені Юрія Федьковича,
асистент кафедри кримінального права, кандидат юридичних наук*

БАЗАРНИЙ СЕРГІЙ ВАСИЛЬОВИЧ

*Національний університет оборони України імені Івана Черняхівського,
підполковник, ад'юнкт кафедри застосування інформаційних технологій
та інформаційної безпеки*

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В РЕАЛІЯХ МАСШТАБНОЇ ВІЙСЬКОВОЇ АГРЕСІЇ

Жахлива реальність сьогодення постає перед нашою країною з новими викликами та надскладними завданнями, які Україна зобов'язана виконати. Даючи гідну відсіч окупантам та різноплановим проявам гібридної війни, розпочатої Російською Федерацією ще у 2014 році, стає очевидним, що сьогодні Україна як суверенна держава зіштовхнулася з гострою нагальною необхідністю захисту фундаментальних націона-

льних цінностей – незалежності, територіальної цілісності й суверенітету держави, свободи, прав людини, добробуту, миру й безпеки, верховенства права – а також забезпечення ефективного функціонування сектору безпеки й оборони в умовах обмежених ресурсів. Інструментом успішної протидії широкомасштабній зовнішній агресії та розвитку інформаційного суспільства в Україні стає актуальним не лише ефективне зростання технологічних можливостей здійснення інформаційного обміну, а й всебічне розуміння та усвідомлення усіма суб'єктами інформаційних відносин необхідності здійснення усіх можливих та доступних заходів захисту інформаційних ресурсів та забезпечення інформаційної національної безпеки України [1, с. 45–46].

На початках XXI століття у світі активно спостерігається хвиля зростання та розповсюдження інформаційних мереж які на нашу думку є ідеальним поєднанням електро обчислювальних машин та комунікацій соціуму. Цивілізований світ вступив в еру інформаційного суспільства тим самим інформація стає центральним ядром рушійною силою у багатьох сферах життєдіяльності як окремого індивіда так і світу в цілому.

Під поняттям інформаційної безпеки як правило розуміють зазвичай необхідність протидії витоку інформації з обмеженим доступом, а також розповсюдження та поширення недостовірної інформації, однак застосування системного підходу дає можливість побачити відмінність наукового розуміння цієї проблеми від побутового [2, с. 174]. Нагадаємо, що положення стаття 17 Конституції України говорить, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [3], що свідчить про поняття «інформаційна безпека» в нормативно-правовому аспекті конституційного статусу [4, с. 30].

Інтегрованою складовою національної безпеки є інформаційна безпека яку розглядають як пріоритетну функцію держави. Проблема гарантування інформаційної безпеки України викликана антиукраїнськими впливами, які розповсюджують ідеї сепаратизму, насильства, національної ворожнечі і є каталізаторами знищення національної ідентичності України, знищення міжнаціональної узгодженості, посягання на конституційний лад України, територіальну цілісність та недоторканність держави. Проблема забезпечення та гарантування інформаційної безпеки України стає актуальнішою в умовах війни, коли з боку Російської Федерації відбувається інформаційна експансія, агресивно упереджене розповсюдження фактів та явищ, а технології рашистських інформаційно-психологічних операцій спрямовані на домінування в українському та глобальному інформаційному просторі та утримання на рівні mass media першості.

Результатом розповсюдження вищезазначеної інформації – інформаційна безпека України опинилась під загрозою та стала об'єктом інформаційно-психологічних впливів. Констатуючи факти на нашу думку по-перше український інформаційний простір є незахищеним

від зовнішніх негативних пропагандистських впливів в результаті чого стає об'єктом інформаційної експансії, а по-друге у глобальному медіа-просторі відсутній український національний інформаційний продукт. Як наслідок – світова спільнота відчуває брак інформації або отримує її з різноманітних джерел, які часом дезінформують, або ж надають викривлену, спотворену, неповну чи недостовірну інформацію.

Ступінь інформаційної безпеки держави як складової національної безпеки, чимало, зумовлена рівнем її інформаційної інфраструктури, в наслідку чого ми спостерігаємо сприятливі умови експансії іноземними компаніями ринку інформаційних послуг. Низький професійний рівень національного виробника інформаційного продукту, звичайно його неконкурентоспроможність не лише на світовому ринку, а й вітчизняного, призвів до того, що українська аудиторія, свідомо, надає перевагу зарубіжним інформаційним програмам [5].

Модернізоване інформаційне суспільство, де кіберпростір обернувся полем бою, загрозами інформаційній безпеці держави є комп'ютерна злочинність, кібертероризм, кібервійни, які передбачають протистояння національних інтересів у просторі Internet із застосування комп'ютерних та інтернет-технологій для знищення супротивника. Здебільшого технології кібервійни, кібертероризму цілеспрямовані на сферу державної безпеки й оборони і становлять реальну загрозу суверенітету держави [6].

Кіберпростір – сфера діяльності утворена за допомогою сукупності комунікаційних каналів мережі Internet та інших телекомунікаційних мереж, технологічної інфраструктури, яка забезпечує їх функціонування, у будь-яких формі за допомогою людської активності.



Інформаційно-технічні загрози, хоча і являють собою відносно нові види інформаційних загроз, становлять надзвичайно високу небезпеку, серед іншого й через доволі швидкі темпи розвитку даного напрямку.

Отже, державна інформаційна політика є важливою ланкою зовнішньої і внутрішньої політики країни яка беззаперечно охоплює всі сфери життєдіяльності суспільства. Стрімкий розвиток інформаційних технологій супроводжується проявом принципово нових загроз інтересам особистості, суспільства, держави та її національній безпеці. Вітчизняний інформаційний простір України є недостатньо захищеним від зовнішніх руйнівних пропагандистських інформаційно-психологічних впливів та загроз. Тому захист інформаційного суверенітету, створення надпотужної системи інформаційної безпеки України, розроблення дієвих стратегій і тактик протидії медіазагрозам мають бути пріоритетними завданнями державної політики її влади та недержавних інститутів.

Список використаних джерел:

1. Присяжнюк М. М. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 42–46.
2. Рубан В. Я. Інформаційна безпека України: сутність та проблеми. *Стратегічна панорама*. 1998. № 3-4. С. 170–175.
3. Конституція України: Основний Закон України від 28.06.96 р. № 254к/96-ВР. URL: <http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>
4. Цимбалюк В. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. Правове, нормативне та методологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. Київ, 2004. С. 30–33.
5. Про Стратегічний оборонний бюлетень України: указ Президента України від 17 вересня 2021 року № 473/2021. URL: <https://www.president.gov.ua/documents/4732021-40121>
6. Про стратегію воєнної безпеки України: указ Президента України від 25 березня 2021 року № 121/2021. URL: <https://zakon.rada.gov.ua/laws/show/121/2021>

Ключові слова: інформаційна безпека України, національна безпека, інформаційні технології, кіберпростір, кіберзлочинність, mass media, інформаційна загроза, інформаційна війна.

Key words: information security of Ukraine, national security, information technologies, cyberspace, cybercrime, mass media, information threat, information war.