as vulnerable in this aspect [7].

The natural countermeasures are seen as investments in security technology, the development of robust cyber security policies and procedures, and the education and training of counter-cyber specialists. [8-10].

In addition, there is a clear need to develop a Single Universal Catalogue of Current IT Challenges and Threats. In addition to the description of threats and methodology of negative impacts, the Universal Catalogue should contain:

Continuously updated databases with examples of actual cybercrime; Detailed descriptions of goals achieved or not achieved by perpetrators; Methods used to disrupt and neutralise threats and subsequent investigations; Recommendations to minimise the chances of disruption to current security protocols and methodologies [11].

Such a catalogue could be the subject of several self-developing international projects running in parallel.

1. Chris Bronk (2016). Cyber Threat. The Rise of Information Geopolitics in U.S. National Security. Praeger Security International. ISBN: 978-1-4408-3498-1.

2. Jason Andress (2019). FOUNDATIONS OF INFORMATION SECURITY A Straightforward Introduction. No starch press. ISBN-10: 1-7185-0004-1 ISBN-13: 978-1-7185-0004-4.

Nurlan Karimov (2019). The European Union Cyber Security and Protection of Human Rights. DOI:10.13140/RG.2.2.26425.31841

4. Bernd W. Wirtz (2019). Digital Business Models. Concepts, Models, and the Alphabet Case Study. Springer. ISBN: 978-3-030-13004-6.

5. N. MACDONNELL ULSCH (2014). Cyber Threat! How to Manage the Growing Risk of Cyber Attacks. John Wiley & Sons, Inc. ISBN 978-1-118-935969-5.

6. Elizaveta Gaufman (2016). Security Threats and Public Perception. Digital Russia and the Ukraine Crisis. Springer. ISBN: 978-3-319-43201-4.

7. Andrew Whiting (2020). Construction Cybersecurity. Manchester University Press. ISBN: 978-1-5261-2332-.

8. Paul Rosenzweig (2013). Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare. The Great Courses. ISBN: 9781470381844.

9. https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637967/EPRS_BRI(2019)637967_EN.pdf

10. https://www.collegenp.com/technology/the-future-is-now-how-technology-is-changing-the-world/

11. https://www.law.kuleuven.be/citip/blog/should-companies-give-confidential-access-to-their-trade-secrets-part-1/

УДК 004+351.86
DOI: 10.31733/17-03-2023-555-557

Наталія ТОЛОШНА
науковий співробітник
наукової лабораторії соціологічних
та кримінально-правових досліджень
Дніпропетровського державного
університету внутрішніх справ

ВПЛИВ ІНФОРМАЦІЙНОГО ПРОСТОРУ НА НАЦІОНАЛЬНУ БЕЗПЕКУ В УМОВАХ ВОЄННОГО СТАНУ

Сьогодні як ніколи для України та її громадян потреба в безпеці стала базовою. «Посприяло» цьому повномасштабне вторгнення російської федерації та, як наслідок, реальні та потенційні загрози обстрілів, ракетних атак, наступу ворожих військ, щоденні кровопролитні бої, в яких українські захисники стримують та відбивають натиск держави-терориста.

У таких умовах держава, виконуючи свої безпосередні обов'язки перед громадянами, стоїть на захисті національної безпеки.

Відповідно до термінології закону України «Про національну безпеку України», національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Національні інтереси України, у свою чергу, – життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний

суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян [1].

Саме зараз, в цей складний час протистояння агресії з боку російської федерації, держава повинна задіяти всі можливі державні органи та системи для захисту своїх громадян, суспільства.

Як вдало зазначає А. Волянюк, з положень згаданого вище нормативно-правового акта ми можемо побачити, що національна безпека України є багатокомпонентним та багатоаспектним поняттям, і для її активної практичної реалізації повинні тісно співпрацювати майже всі внутрішні та зовнішні державні системи [2].

Одним із компонентів практичної реалізації національної безпеки є забезпечення безпеки інформаційного простору. Поряд з політичним та військовим протистоянням агресії з боку російської федерації доводиться тримати в безпеці та чистоті інформаційний простір. Ворог намагається усіма силами дестабілізувати спокій, спровокувати паніку серед громадян України, вносячи в інформаційний простір фейкові повідомлення, заяви.

В Указі Президента України від 28.12.2021 №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки» визначено, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. Стратегія інформаційної безпеки (далі – Стратегія) визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних. Метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина. Досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки.» [5].

Таким чином, як вдало вказують С. М. Матвієнків, Ю. І. Шмаленко, В. М. Кольцов, щоб бути захищеними інформаційно, необхідно мати контрольовану державою медійну структуру (Інтернет-ресурси, ЗМІ, телебачення), власну систему пропаганди та здійснення інформаційних атак та контратак стосовно спроб посилення зовнішніх впливів на суспільно-політичні обставини в країні. [3, с.226].

У сучасних умовах для людей потреба в інформації є важливою та цінною як і їх безпека. Цінність інформації та її масштабів в умовах воєнного стану для кожного своя: комусь цікава зовнішня та внутрішня політика держави, для когось важлива інформація про стан військового протистояння нашої держави (ситуація на фронті), інформація про ситуацію в економічній сфері держави, в освіті, медицині.

Маючи достатній вибір джерел та каналів інформування, у громадян є можливість критично оцінювати ситуацію, що склалася, аналізувати події, приймати ті чи інші рішення для власної безпеки.

Щодня вбиваючи українців, держава-агресор не забуває і про проведення інформаційних атак на українське населення, прагнучи за допомогою фейкової інформації посіяти в суспільстві страх та панічні настрої, дестабілізувати політичну та соціально-економічну ситуацію в Україні. Вторгаючись в український інформаційний простір, ворог робить замах на громадянську ідентичність українців [4, с. 21].

З початку повномасштабного вторгнення країни-агресора наша держава постійно адаптується та створює для своїх громадян доступні інформаційні канали (як телевізійні так і телеграм-канали). Такими з перших днів були:

- єдині новини (об'єднання каналів, які цілодобово з перших днів війни висвітлювали ситуацію в країні, наслідки атак противника тощо);
- інформаційні канали в месенджерах з поданням чітких новин про події;
- канали для виявлення фейкових новин, які активно запускає в простір російська федерація;

- додатки для смартфонів щодо оповіщення про повітряну загрозу, випуск ворогом ракет, зліт ворожої авіації;

- канали для внутрішньо переміщених осіб з інформацією про адреси, куди можливо звернутися за гуманітарною допомогою;

- оповіщення від ДСНС про можливу загрозу ракетного удару;

- заклики до громадян від державних структур таких як МВС України, ДСНС про дотримання правил особистої безпеки особливо з небезпечними предметами (найдена зброя та боєприпаси), нагадування про кібербезпеку тощо.

Важливими були заклики держави до громадян довіряти лише перевіреним джерелам інформації, адже ворог в інформаційній війні постійно намагається закидати в наш інформаційний простір фейкову інформацію, свою пропагандистські погляди, для спотворення реальності, дійсності. Вказані кроки прямо або опосередковано спрямовані на порушення національної безпеки України.

Важливим в інформаційному просторі є факт щоденного звернення Президента до своїх громадян, висвітлюючи основні події та досягнення за день цим він не тільки інформує суспільство, а й підсилює віру в перемогу, підтримує дух українського народу. Дані звернення вселяють надію в серця українців і віру в безальтернативність української перемоги над державою-терористом.

Завдяки різноманіттю джерел інформації, достовірності інформації, в українців є можливість бути проінформованими, планувати свої подальші дії, почуватися безпечніше, знаючи про реальну ситуацію в країні. Тому держава, контролюючи інформаційний простір, захищає національні інтереси, формує стан спокою, захищеності, безпеки своїх громадян.

Підсумовуючи викладене варто зазначити, що з початком широкомасштабної війни, яку розпочала сусідня держава проти України, щодня фіксують акти інформаційних атак проти нашої Батьківщини, які, в свою чергу, посягають на національну безпеку України. Для ефективного запобігання та протидії російським інформаційним атакам держава повинна вживати широкий спектр заходів (у тому числі кримінально-правового характеру).

Перспективним напрямком подальших наукових досліджень вважаємо аналіз складів кримінальних правопорушень, що посягають на інформаційну безпеку України.

1. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

2. Волянюк А. Національна безпека України: Складові елементи та виклики сьогодення. URL: https://mil.in.ua/uk/blogs/natsionalna-bezpeka-ukrayiny-skladovi-elementy-ta-vyklyky-sogodennya/.

3. Матвієнків С. М., Шмаленко Ю.І., Кольцов В.М. Опозиція «легкість-тяжкість» як метафора історичних типів суспільств. Актуальні проблеми філософії та соціології. 2022. Вип. 37. С. 223-227.

4. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах російської військової агресії. Південноукраїнський правничий часопис. 2022. № 1-2. С. 20-26.

5. Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки». URL: https://www.president.gov.ua/documents/6852021-41069.