України, є: виявлення представників екстремістської спрямованості у вітчизняних засобах масової інформації та недопущення їх використання іноземними організаціями та їх філіями для підриву безпеки України, здійснення заходів, спрямованих на запобігання та протидії таким загрозам на території України, система додаткових заходів, спрямованих на недопущення розповсюдження в засобах масової інформації та мережі Інтернет контенту, що порушує національний суверенітет та територіальну цілісність України, розпалює міжнаціональні та релігійні конфлікти, пропагандує війну тощо.

Тому очікуваними результатами реалізації Стратегії є: захищений інформаційний простір України; ефективне функціонування системи стратегічних комунікацій; здійснення ефективної протидії поширенню незаконного контенту; забезпечення сталого процесу інформаційної реінтеграції громадян України, які проживають на тимчасово окупованих територіях України, та поширення українського телерадіомовлення на територіях України, прилеглих до тимчасово окупованих територій; суттєве підвищення рівня медіакультури та медіаграмотності населення; дотримання конституційних прав особи на вільне вираження своїх поглядів і переконань, захист приватного життя; забезпечення захисту прав журналістів; формування української громадянської ідентичності [1].

Отже, реальна реалізація цієї стратегії посилить здатність Української нації забезпечувати власну інформаційну безпеку та захист свого інформаційного простору в умовах режиму воєнного стану в Україні, де росія є основною загрозою безпеці України.

1. Стратегія інформаційної безпеки: Указ Президента України від 28.12.2021р.№685/2021.URL :https://zakon.rada.gov.ua/laws/show/685/2021# Text

2. Конституція України від 28.06.1996 р. URL https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

3. Про Національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text

4. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. № 1(24)/2018. С. 89-103.

5. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 411 с.

УДК 35.078.7/759.6
DOI: 10.31733/15-03-2024/2/326-328

Олександра
НЕСТЕРЦОВА-СОБАКАРЬ
доцент кафедри
цивільно-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ УКРАЇНИ

Зростання інформаційної інфраструктури, що виникає у суспільних відносинах, призводить до того, що національна безпека має суттєву залежність від забезпечення інформаційної стійкості та надійності основних її компонентів. Ця проблема має системотворче значення для розвитку держави у всіх сферах життєдіяльності суспільства, так і щодо забезпечення безпеки країни в цілому.

Основною проблемою є забезпечення інформаційної безпеки, яка сприяє захищеності інформації від несанкціонованого доступу, використання, розкриття, зміни, знищення, а також від випадкового чи навмисного впливу, що може призвести до втрати, крадіжки, пошкодження, модифікації чи недоступності інформації. Інформаційна безпека має велике значення для забезпечення захисту державних таємниць, а також інформаційних систем та ресурсів державних органів; захисту конфіденційної інформації, комерційної таємниці, а також інформаційних систем та бізнес-ресурсів, захисту персональних даних, доступності інформації та її незмінності; контролю за доступом до інформації та її

використанням тощо.

Із розвитком інформаційних технологій та появою нових загроз інформаційна безпека стає дедалі важливішою, у тому числі щодо захисту від неправомірних дій інформаційного характеру щодо об'єктів критичної інфраструктури.

Інформаційна безпека критичної інфраструктури України є сукупністю систем державного управління, спрямованих на забезпечення обороноздатності об'єктів, порушення функціонування яких призводить до втрати управління та незворотного руйнування інфраструктури економіки країни, суб'єкта або адміністративно-територіальної одиниці України, зниження безпеки населення держави на тривалий період.

Як відомо, первинна класифікація основних джерел загроз інформаційній безпеці передбачає їх поділ на зовнішні та внутрішні. Аналіз показує, що найбільш актуальними, у зв'язку з ситуацією, що склалася на міжнародній арені, є зовнішні передумови, а саме діяльність зарубіжних розвідувальних та інформаційних підрозділів, спрямована проти інтересів країни в інформаційній сфері через створення умов, що передбачають утиск інтересів України у світовому інформаційному просторі та розробка концепцій інформаційних війн.

До внутрішніх джерел належать несприятливий стан галузей промисловості, тенденція об'єднання державних та кримінальних структур в інформаційній сфері, а також зниження ступеня захищеності конституційних інтересів громадян та суспільства загалом в інформаційній сфері. Вплив наведених загроз на критичну інформаційну інфраструктуру України може призвести до порушення їхнього функціонування та стати причиною настання тяжких наслідків для держави як в економічній, так і в політичній сферах.

Як показує практичний досвід, найбільшу вагу у сучасному стані захищеності інформаційного суверенітету України займають зовнішні чинники, перш за все засновані на інформаційній збройній агресії російської федерації та планомірному використанні сучасних концепцій інформаційних воєн. Тому пріоритетними на даний час є дослідження, спрямовані на вдосконалення та розробку нових підходів до функціонування системи інформаційної безпеки критичної інфраструктури України.

Оцінка безпеки критичної інформаційної інфраструктури здійснюється з метою виявлення, попередження та ліквідації наслідків комп'ютерних атак на інформаційні ресурси, з метою прогнозування виникнення можливих загроз безпеки критичної інформаційної інфраструктури та вироблення заходів щодо підвищення стійкості під час проведення щодо її комп'ютерних атак [1, с. 34-39].

Найбільшу загрозу безпеці об'єктів критичної інфраструктури становлять саме скоординовані атаки з використанням програмних вірусів. Такий вид атаки поєднує підготовчий етап (дії, що створюють на об'єкті нові уразливі місця) та атакуючі дії (використання уразливих місць). Водночас, підготовчі дії можуть здійснюватися значно раніше, ніж сама атака, можуть бути задіяні працівники (інсайдери) підприємства, що є об'єктом нападу, та здійснені різноманітні відволікаючі маневри [2, с. 19].

Як показує досвід розвинених країн, дослідження механізмів захисту інформації об'єктів критичної інфраструктури передбачає на перших кроках етап ідентифікації (визначення) елементів, які повинні розглядатися як об'єкти критичної інфраструктури. Разом з тим важливим напрямом забезпечення захисту інформації на об'єктах критичної інфраструктури є запровадження відповідного управлінського впливу, який передбачається здійснювати в декілька етапів, одним із головних мають стати моніторинг, спостереження та контроль [3].

Підсумовуючи викладене, забезпечення інформаційної безпеки об'єктів критичної інфраструктури потребує цілеспрямованого вжиття комплексу заходів, спрямованих на: розробку і вдосконалення основних положень, що ідентифікують кіберзлочини, кібертероризм та інформаційні війни; створення взаємопов'язаного, систематизованого набору моделей та сценаріїв реалізації комп'ютерних атак на об'єкти, потенційно вразливі з погляду кіберзлочинів, а також розробка та впровадження ефективного комплексу механізмів, моделей та сценаріїв організації протидії подібним явищам; підготовку пропозицій щодо вдосконалення на законодавчому, організаційному та операційному рівнях реалізації інформаційної безпеки, а також правових та нормативних актів для ефективної протидії проявам кіберзагроз.

---

1. Гончар С. Ф. Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури / С. Ф. Гончар, Г. П. Леоненко, О. Ю. Юдін // *Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі*. 2014. №

806. С. 34-39.

2. Русецький А.А., Марков В.В. Аналіз стану загроз критичній інфраструктурі в Харківській області. *Актуальні проблеми вітчизняної юриспруденції*. № 1. Том 2. 2017. С. 18-20.

3. Шевченко М. М. Методика системно-комплексного дослідження державного управління забезпеченням національної безпеки / М. М. Шевченко // *Вісник Національної академії оборони України*. 2010. № 4. С. 235–240.

УДК 321.011:341.211:342.3
DOI: 10.31733/15-03-2024/2/328-329

Олександр ТАЛДИКІН
доцент кафедри
загальноправових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

КІБЕРВІЙНА В КОНТЕКСТІ ЗАГРОЗИ ІНФОРМАЦІЙНОМУ СУВЕРЕНІТЕТУ ДЕРЖАВИ

Питання визначення віртуального суверенітету неможливо без урахування проблем утворення принципово нової влади – влади мережі, або *нетократії,* адже віртуальна складова інформаційного суверенітету безпосередньо пов'язана з *кіберпростором*, його специфічним розташуванням поза фізичним виміром і часом. В попередніх роботах автор наголошував про актуальність дослідження особливостей інформаційної складової суверенітету держави, або інформаційного суверенітету в сучасних умовах інформаційного суспільства, коли суттєво змінюється роль держави, формується новий правовий простір наддержавного характеру, який доповнюється простором мережі, віртуальним, інформаційним, що у свою чергу обумовлює необхідність захисту від негативних зовнішніх впливів, потребу в існуванні механізму правової регуляції за допомогою норм як національного законодавства, так і норм міжнародного права [1], [2], [3].

Реальна спроможність віртуального світу бути сферою застосування *кіберсили*, яка спроможна нести загрозу державному суверенітету будь-якої держави [4; с. 6-7]. Разом з тим, проблема контролю у сфері віртуальної реальності, не означає нездатності утворювати власні ресурсні його складові та захищати свої суверенні права. Протистояння колишніх в інформаційних війнах людства, коли відбувався вплив інформації на свідомість за допомогою методів пропаганди, дезінформації та маніпулювання з метою формування необхідних для супротивника політичних поглядів сьогодні доповнилося *кібервійною*, як сучасною складовою війни інформаційної.

У 2017 році в Україні було прийнято Закон Про основні засади забезпечення *кібербезпеки* України, відповідно до якого визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі [5].

Ще у 2011 році резолюцією Ради Безпеки ООН № 1113 від 05.03.2011. кібервійна була інтерпретована, як використання комп'ютерів або цифрових засобів із боку уряду або з явним знанням чи схваленням цим урядом проти іншої держави або приватної власності в іншій державі, включаючи навмисний доступ, перехоплення даних або пошкодження цифрової та керованої цифровим методом управління інфраструктури. А також виробництво та поширення пристроїв, які можуть бути використані для підриву внутрішньої активності [6]. Безумовно, що в спрощеному розумінні кібервійна буде фактом протистояння у кіберпросторі в мережі Інтернет.

На сьогодні існує певна варіативність стосовно визначення самого поняття «кібервійна», так: більш розширену інтерпретацію кібервійни пропонують Нік Даєра-Візефорда та Світлана Матвієнко. Вони розглядають її через призму геополітичної динаміки та класових конфліктів, що спричиняють протиборство в цифрових мережах [7].

Суттєвою рисою кібервійни є *квазітериторія* її ведення. Кіберпростір відзначається тим, що для нього не існує державних кордонів. Він об'єднує географічні