СУЧАСНІ ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В РЕАЛІЯХ ВІЙСЬКОВОЇ АГРЕСІЇ

Слінько Т.М.

кандидатка юридичних наук, професорка,
завідувачка кафедри конституційного права України
Національного юридичного університету імені Ярослава Мудрого

Військові конфлікти, які останнім часом усе частіше спалахують у тому чи іншому куточку світу, для людства завжди мали серйозні наслідки. Сьогодні, у добу стрімкого розвитку інформаційних технологій, цифровізації (digitalization) більшості сфер, ведення воєнних дій супроводжується таким явищем, як кіберагресія. Зауважимо, що через його поширення, розширення способів і засобів вчинення (йдеться передусім про такі складові, як кібератаки, кібершпигунство і кібервійни) людство зазнає непоправних втрат, а саме завдається шкода об’єктам критичної інфраструктури, які виводяться з ладу,

відбуваються збої у роботі державних органів і установ, банків тощо. Звісно, усе це робиться з метою впливу на супротивника, дестабілізації політичної й економічної ситуації, зокрема, задля підвищення незадоволення серед громадян. Зрозуміло, що рф як країна-агресор також вдається до згаданих, так би мовити, брудних засобів. Однак, як свідчать останні події, постійні атаки на сайти військових відомств, різних міністерств, фінансових установ, на енергооб'єкти й інфраструктуру лише викликали лють і ненависть до військовослужбовців і політичного керівництва рф, згуртували, об'єднали наш народ.

Не можна не згадати й про використання країною-агресором таких прийомів кібервійни (кіберагресії), як поширення фейків, дезінформації, проведення інформаційних операцій. Усе це робиться для маніпулювання громадською думкою й впливу на політичні процеси. Наприклад, поширення в росЗМІ фейкових новин про перемоги й успіхи армії рф, створення враження масштабної підтримки агресора не лише всередині країни, а й за її межами спрямовані на маніпулювання фактами, їх викривлення задля поширення серед українців почуття невпевненості, зневіри їх у перемозі і, як наслідок, хаосу в суспільстві.

Вказане набуває особливого значення з огляду на те, що починаючи з анексії Криму і Севастополя, окупації частини Донецької і Луганської областей, а особливо з 24 лютого 2022 року – це повномасштабного вторгнення армії рф на територію нашої країни ми щодня стикаємося зі ризиками і загрозами інформаційній безпеці України, існуванню Української держави, її територіальній цілісності, суверенітету, що, як і в більшості демократичних суспільств, захищається національним законодавством. Усе це підтверджує, що інформаційна безпека у реаліях військової агресії стає критичним фактором забезпечення національної безпеки і збереження суверенітету держави.

Отже, нині саме збройна й інформаційна агресія рф, політична напруженість є тим важелем, який підштовхує Україну до рішучих дій, спрямованих на захист свого суверенітету й незалежності, забезпечення безпеки, збереження

цілісності і єдності держави, тим більше, що теоретичне й законодавче підґрунтя для цього існує.

Зокрема, конституційно-правові засади інформаційної безпеки вказані у ст. 17 Конституції України, якою в пріоритетному порядку встановлюється, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки – це найважливіші функції держави, справа всього Українського народу [1]. Чи означає наведене, що інформаційну безпеку поставлено на один щабель із такими важливими компонентами системи національних інтересів, як суверенітет і територіальна цілісність і цей її статус законодавчо закріплений в Основному Законі України? На нашу думку, відповідь має бути позитивною, особливо беручи до уваги ступінь її важливості.

Крім того, правову базу регулювання державної політики у сфері національної безпеки закладено в Законі України «Про основи державної політики національної безпеки України», де вперше дано офіційну оцінку значущості й системній сутності інформаційної безпеки як невід'ємної складової національної безпеки України. Крім того, сукупність ідей та концепцій, що визначають національні інтереси України в інформаційній сфері, загрози їх задоволення, напрями і пріоритети державної політики в інформаційній сфері й механізми регулювання суспільних відносин відображені в Доктрині інформаційної безпеки України, затвердженій і введеній в дію Указом Президента України від 25 лютого 2017 року [2].

Зауважити, що, попри те, у самій Доктрині не передбачені конкретні правові механізми регулювання суспільних відносин у сфері інформаційної безпеки, вона визнається базовим актом, в якому відображені цілі, вектори діяльності української держави у даній сфері. Так, у тексті Доктрини зазначено, що метою її прийняття є «уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни» [2]. У документі також зафіксовано, що «Російською Федерацією застосовуються проти України найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і

релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України» [2].

Не можна оминути й того факту, що Указом Президента України від 28 грудня 2021 року № 685/2021 затверджена Стратегія інформаційної безпеки (далі – Стратегія), яка визначає актуальні виклики й загрози національній безпеці України в інформаційній сфері, стратегічні цілі й завдання, які стоять перед державою у справі як протидії таким загрозам, так і також захисту права осіб на інформацію, персональних даних. Стратегією визначено, що інформаційна безпека України – складова національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави. У ній серед глобальних викликів інформаційній безпеці зазначено: збільшення кількості глобальних дезінформаційних кампаній; наявність великої кількості соціальних мереж як суб'єктів впливу в інформаційному просторі; недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій; інформаційний вплив Російської Федерації як держави-агресора на населення України; інформаційне домінування РФ як держави-агресора на тимчасово окупованих територіях України; несформованість системи стратегічних комунікацій; недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів; застосування різних способів маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції нашої країни; недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам [3].

Вказане зайвий раз підтверджує тезу про те, що вітчизняний інформаційний простір протягом всього існування незалежної України був і залишається об’єктом постійних зовнішніх атак, особливо впродовж останніх 9 років. Крім того, як зазначають експерти в «Аналізі державної політики у сфері національної безпеки і оборони України»: «Дії суб’єктів забезпечення національної безпеки України на початку загострення воєнно-політичної ситуації були не ефективними.

Оперативність прийняття управлінських рішень у сфері національної безпеки була низькою, що не забезпечувало своєчасного реагування на нові загрози. Відсутність постійно діючого механізму моделювання і прогнозування як основи для прийняття рішень не дозволяло діяти на упередження» [4]. Що, звісно, неприпустимо в такий складний для держави час.

Вивчивши думки експертів, можемо сміливо стверджувати, що основними викликами для інформаційної безпеки в Україні в контексті військової агресії виступають: 1) поширення дезінформації (як відомо, російська агресія супроводжується активною дезінформаційною кампанією, яка має на меті маніпулювання громадською думкою, створення хаосу й дестабілізацію українського суспільства; 2) кібератаки на державні об’єкти й критичної інфраструктури (зокрема, кіберзлочинці й державні хакерські групи можуть спрямовувати кібератаки на державні інституції, енергетичні системи, медичні установки та інші критично важливі об'єкти; 3) шпигунство й витік інформації (ворожі агенти у змозі проникати у військові системи й отримувати конфіденційну інформацію, що загрожує оперативній ефективності й безпеці військових дій); 4) дезорганізація комунікацій із фронту (так, забезпечення ефективної комунікації та зв'язку з військовими одиницями на передовій стає важливим завданням, оскільки ворожа агресія може перешкоджати та перехоплювати зв'язок); 5) кібершпигунство та підрив кібербезпеки, зокрема, кібершпигунство може бути використане для отримання розвідувальної інформації про військові плани й техніку; 6) зростання застосування штучного інтелекту і складних алгоритмів у кібератаках; 7) існування ризиків і можливостей для зловживання у сфері захисту персональних даних і збереження конфіденційної інформації передусім стосовно військовослужбовців і ветеранів (до речі, це стає важливим завданням держави, як і докладання зусиль запобігання цьому); 7) розвиток кібервійськових здібностей (саме це має підштовхнути українські військові структури до активного розвитку кібервійськових здатностей для виявлення, відповіді й запобігання кібератакам, а також для підтримки військових операцій).

Усе викладене вище дає підстави стверджувати, що інформаційні загрози нашій державі потребують ретельного аналізу, а технології їх нівелювання і протистояння їм – осучаснення, оскільки, сподіваємося, нами доведено, що інформаційна безпека – один із фундаментальних чинників існування й розвитку будь-якої держави у XXI столітті.

Крім того, враховуючи зростаючу складність кіберзагроз та їх потенційно негативний вплив на національну безпеку, Україна має вдосконалювати свої стратегії кібербезпеки, розвивати міжнародну співпрацю з іншими країнами й міжнародними організаціями, а також активно впроваджувати сучасні технології та методи захисту інформації.

Список використаних джерел:

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

2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.17 р. № 47/2017. Дата оновлення: 25.02.2017 р. URL: https://zakon.rada. gov.ua/ laws/show/47/2017#Text (дата звернення : 28.07. 2023).

3. Стратегія інформаційної безпеки : затв. Указом Президента України від 28 грудня 2021 року № 685/2021. URL : https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення : 03.08. 2023).

4. Аналіз державної політики у сфері національної безпеки і оборони України. 2015 рік. URL: https://rpr.org.ua/wp-content/uploads/2018/02/Analiz-polityky-NB-pravl-final.pdf (дата звернення : 29. 07.2023).