УДК 355.40: 356.35

Сніцаренко П. М., д.т.н., с.н.с.;
Саричев Ю. О., к.т.н., с.н.с.;
Семененко В. М., к.т.н., с.н.с.;
Ткаченко В. А., к.військ.н.

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Удосконалення чинного інформаційного законодавства України як необхідна умова адекватності заходів щодо забезпечення інформаційної безпеки держави

Резюме. Обґрунтовано пропозиції щодо удосконалення чинного законодавства України з питань інформаційної безпеки держави.

Ключові слова: інформаційне законодавство України, інформаційна безпека держави, термінологія.

Постановка проблеми. Як визначено у попередній статті за участю авторів [1], виходячи з вимог статті 17 Конституції України, головною сутністю інформаційної політики держави має бути забезпечення її інформаційної безпеки відповідно до визначення, яке наведене в Законі України [2]. Водночас, як свідчить проведений аналіз, інформаційним законодавством України така спадковість не визначається. Це призвело до довільного розуміння як державної інформаційної політики, так і сутності інформаційної безпеки держави, що засвідчують, зокрема, численні наступні законодавчі акти України. Зазначене шкодить становленню та розвитку теоретичних основ щодо забезпечення інформаційної безпеки держави, а також адекватності реалізації відповідних практичних заходів. Тому удосконалення чинного інформаційного законодавства України є актуальним проблемним питанням як для теорії, так і для практики, що потребує вирішення.

Аналіз останніх досліджень і публікацій. Аналіз публікацій у фаховому середовищі щодо інформаційної безпеки України був проведений у роботі [1], в якій зазначено, що головною причиною "розмитості" державної інформаційної політики України та, від того, недосконалості національних механізмів забезпечення інформаційної безпеки, слід вважати неоднозначний та подекуди неадекватний понятійно-категорійний апарат цієї важливої галузі державної діяльності, який закладено чинним законодавством. Численні приклади цього знаходяться, зокрема, у таких важливих для інформаційної сфери документах як Закони України: "Про інформацію" [3], "Про телекомунікації" [4], "Про основні засади забезпечення кібербезпеки України" [5], Стратегія національної безпеки України [6], Стратегія кібербезпеки України [7], Доктрина інформаційної безпеки України [8], Воєнна доктрина України [9], Стратегічний оборонний бюлетень України [10]. Наслідком цього як теоретична, так і практична діяльність дезорієнтуються, що призводить до довільного розуміння та використання термінів, їх ситуативної модифікації, ігнорування у випадках, коли таке недоцільне.

Іншою причиною непевного стану щодо забезпечення інформаційної безпеки України стало те, що до сьогодні, незважаючи на конституційну норму, ще не прийнято рамкового закону, яким би стверджувалися основні поняття і положення щодо інформаційної безпеки держави. Це загалом гальмує об'єднавчі процеси та забезпечення їх адекватності як в теоретичному руслі, так і в напрямах практики.

Зважаючи на наведене, першочергово потребує уточнення чинна законодавча база, що регулює інформаційну сферу України, а особливо її понятійно-категорійний апарат. Саме тому **метою статті** є надання пропозицій щодо удосконалення чинного інформаційного законодавства України, переважно стосовно базових термінологічних положень як загальнотеоретичної передумови однозначного розгляду та розуміння питань забезпечення інформаційної безпеки держави.

Виклад основного матеріалу. Усунення існуючих нормативно-правових недоліків стане можливим, а національна практика забезпечення

інформаційної безпеки держави буде адекватнішою за умови внесення суттєвих змін до чинного інформаційного законодавства України, зокрема, через удосконалення термінології цієї предметної сфери.

Так, до **Закону України "Про інформацію"** пропонуються такі зміни:

пункт 1 статті 1 викласти в редакції:

"*інформація* – значення (сутність, змістовність) даних (відомостей), знання або висновки, отримані на їх основі";

у статті 1 необхідно ввести також низку нових понять у редакції:

"*факт* – реальна (дійсна) подія, явище, випадок";

"*відомості* – зафіксовані у будь-якій формі подання певні факти про будь-кого, будь-що";

"*дані* – будь-які відомості, факти або показники, що подаються в умовній формі, зручній для інтерпретації, обробки, пересилання людиною чи технічними засобами, як основа для певних уявлень, висновків, рішень";

"*інформаційна сфера* – середовище та умови діяльності, пов'язані зі створенням, обробкою, використанням (поширенням) і захистом інформації (інформаційних ресурсів)";

"*інформаційний ресурс* – сукупність інформаційних продуктів, доступних користувачу (споживачу) для безпосереднього використання у разі потреби";

"*інформаційний продукт* – інформація або дані (відомості), які підготовлені у формі, зручній для користувача (споживача), і призначені для задоволення його потреб";

"*інформаційна продукція* – документовані інформаційні продукти".

У статтю 3 додати визначення:

"*державна інформаційна політика України* – складова державної політики як сукупність політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових та організаційних завдань і заходів, спрямованих на забезпечення інформаційної безпеки України".

У статтю 10 за змістом внести вид інформації "*інформація воєнна*", а через це внести до Закону нову статтю 20 в редакції:

"Стаття 20. *Інформація воєнна.*

1. *Інформація воєнна* – зміст, значення (сутність) даних воєнного характеру, незалежно від форми подання, що використовуються у практичній роботі органами військового управління, при управлінні військами та зброєю, а також органами воєнно-політичного керівництва держави при вирішенні питань оборони.

2. Джерелами інформації воєнної можуть бути органи військового управління, сили та засоби усіх видів розвідки, органи управління взаємодіючих військ (сил), перебіжчики, полонені, захоплені у противника бойові документи і зразки озброєння та військової техніки, місцеві жителі, а також спеціальна література, різні довідники, описи, топокарти тощо.

3. Правовий режим інформації воєнної визначається законодавством України, а також міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України".

До **Закону України "Про основні засади забезпечення кібербезпеки України"** пропонується внесення таких змін:

пункт 5 статті 1викласти в редакції:

"*кібербезпека* – складова інформаційної безпеки як стан захищеності життєво важливих інтересів людини, суспільства і держави у кіберпросторі, при якому запобігається нанесення шкоди через:

неповноту, невчасність та невірогідність інформації, що використовується, а також відсутність інформації за її потреби;

негативний інформаційний вплив;

нерегульоване або злочинне застосування інформаційних технологій;

несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, а також інших електронних інформаційних ресурсів;

політику держави, зокрема з питань спілкування в соціальних мережах;

недостатній рівень медіакультури суспільства, зокрема з питань використання електронних засобів масової інформації".

Пункт 6 статті 1:

"*кіберзагроза* – наміри, дії (бездіяльність) або явища чи процеси, матеріалізація яких може призвести до таких негативних наслідків для людини, суспільства, держави за необхідності використання можливостей кіберпростору:

неповноти, невчасності та невірогідності інформації, що використовується, а також відсутності інформації за її потреби;

негативного інформаційного впливу;

нерегульованого або злочинного застосування інформаційних технологій;

несанкціонованого розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, а

також інших електронних інформаційних ресурсів;

відсутності цілісної комунікативної політики держави, зокрема з питань спілкування в соціальних мережах;

низького рівня медіакультури суспільства, зокрема з питань використання електронних засобів масової інформації".

Пункт 9 статті 1:

"*комп'ютерна (кібер-) злочинність* – вчинення правопорушень, пов'язаних з комп'ютерними системами і даними (інформацією), які визначені статтями 2 – 12 Конвенції про кіберзлочинність".

Пункт 10 статті 1:

"*кібероборона* – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів держави, які спрямовані на підготовку і застосування інформаційної інфраструктури сил оборони, а також інших сил та засобів, для відбиття воєнної агресії у кіберпросторі".

Пункт 11 статті 1:

"*кіберпростір* – складова інформаційного простору, середовище електронних інформаційних ресурсів, утворене в результаті функціонування на основі єдиних принципів та загальних правил інформаційних і телекомунікаційних систем" або "*кіберпростір* – інформаційне середовище, в якому відбуваються процеси та відносини щодо добування, обробки та поширення інформації (інформаційних ресурсів) в електронному вигляді".

Пункт 15 статті 1 щодо критичної інформаційної інфраструктури вилучити із Закону через некоректність.

Пункт 19 статті 1:

"*критичний об'єкт інформаційної інфраструктури* – структурний елемент у складі інформаційної системи, інформаційних ресурсів, засобів комунікацій і управління інформаційними потоками або організаційно-технічних структур та механізмів, що забезпечують їх функціонування, виведення з ладу чи порушення функціонування якого може завдати значної шкоди процесу управління в одній або кількох сферах національної безпеки держави".

Крім зазначеного, в статтю 1 додати визначення:

"*кіберудар* – результативність, наслідок кібератаки (одночасно кількох кібератак) на один або кілька об'єктів інформаційної інфраструктури";

"*кіберінцидент* – непередбачувана або небажана подія, в результаті якої може бути завдано чи вже завдано шкоди наявним електронним інформаційним ресурсам та/або об'єктам інформаційної інфраструктури, які забезпечують створення, обробку, використання чи захист таких ресурсів".

Особливо слід наголосити, що на виконання статті 17 Конституції України в інформаційному законодавстві держави має бути рамковий закон щодо забезпечення інформаційної безпеки, який би став єдиним загальним регуляторним актом стосовно інформаційних процесів як в електронному середовищі (кіберпросторі), так і поза ним (друкування, вербальні процеси, організаційно-технічні заходи захисту інформаційних ресурсів тощо). Цей Закон України доцільно назвати **"Про інформаційну безпеку України"**, до змісту якого необхідно включити такі базові визначення:

"*інформаційна безпека України* – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

неповноту, невчасність та невірогідність інформації, що використовується, а також відсутність інформації за її потреби;

негативний інформаційний вплив;

нерегульоване або злочинне застосування інформаційних технологій;

несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, а також інших інформаційних ресурсів;

відсутність цілісної комунікативної політики держави;

недостатній рівень медіакультури суспільства";

"*повнота інформації* – критерій якості інформації, що характеризує мінімальний за змістом її склад, достатній для прийняття рішення користувачем (споживачем)";

"*вчасність інформації* – критерій якості інформації, що характеризує час її надходження не пізніше заздалегідь визначеного користувачем (споживачем) моменту часу";

"*вірогідність (достовірність) інформації* – критерій якості інформації, що характеризує її правдивість, тобто рівень відповідності відображення її змістом реально існуючої дійсності (процесів, об'єктів, явищ)";

"*цілісність інформації* – критерій якості інформації, що характеризує її змістовну нерозривність (збереження встановленої повноти) в умовах реєстрації (документування),

зберігання, перетворення, передачі та подання користувачу (споживачу)";

"*конфіденційність інформації* – критерій якості інформації, що характеризує її як об'єкт, який не підлягає розголосові та не може бути доступним для неавторизованого користувача (споживача) і/ або процесу";

"*доступність інформації* – критерій якості інформації, що характеризує можливість її використання користувачем (споживачем), коли в цьому є необхідність, шляхом виконання відповідних процедур (правил) одержання, перетворення та подання";

"*інформаційний вплив* – організоване цілеспрямоване втручання у свідомість (підсвідомість) чи фізичний стан цільової аудиторії та/або у процес функціонування технічних об'єктів інформаційної інфраструктури шляхом застосування інформаційних засобів і технологій";

"*негативний інформаційний вплив* – інформаційний вплив, що завдає шкоди морально-психологічному та/або фізичному стану певної цільової аудиторії або знижує якість функціонування технічних об'єктів інформаційної інфраструктури";

"*цільова аудиторія* – група осіб (в окремих випадках – одна особа), на яку спрямовується інформаційний вплив";

"*інформаційна технологія* – організована сукупність знань, матеріалізованих методами і прийомами визначених елементів інформаційної інфраструктури в цілеспрямованому процесі створення та/або обробки інформації (інформаційних ресурсів) технічними засобами";

"*створення інформації (інформаційних ресурсів)* – процес формування інформаційного продукту шляхом добування, обробки та узагальнення фактів, відомостей або даних, який за рівнем достовірності, оперативності (вчасності) та формою подання відповідає вимогам користувача (споживача)";

"*обробка інформації (інформаційних ресурсів) технічна* – здійснення за допомогою технічних засобів однієї або кількох операцій з інформацією (інформаційними ресурсами), зокрема: введення, збирання (пошук), записування, передавання, приймання (отримання), копіювання, перетворення, реєстрація (документування), розмноження, дублювання, сканування (зчитування), друкування, зберігання, відображення (візуалізація, показ), відтворення, знищення";

"*обробка інформації (інформаційних ресурсів) когнітивна* – здійснення операцій з інформацією (інформаційними ресурсами) людиною шляхом мислення з відтворенням проміжних та кінцевого результатів у вербальний (природномовний) або інший спосіб";

"*інформаційна інфраструктура держави* – сукупність різноманітних інформаційних систем, інформаційних ресурсів, засобів комунікацій і управління інформаційними потоками, які створюють національний інформаційний простір, а також організаційно-технічних структур та механізмів, що забезпечують їх функціонування відповідно до національного законодавства";

"*інформаційна система* – організаційно-технічна система, у якій реалізується інформаційна технологія або їх взаємоузгоджена сукупність";

"*інформаційний простір* – штучно створене середовище, в якому відбуваються процеси та відносини щодо обробки та поширення інформації (інформаційних ресурсів)";

"*критичний об'єкт інформаційної інфраструктури* – структурний елемент у складі інформаційної системи, інформаційних ресурсів, засобів комунікацій і управління інформаційними потоками або організаційно-технічних структур та механізмів, що забезпечують їх функціонування, виведення з ладу чи порушення функціонування якого може завдати значної шкоди процесу управління в одній або кількох сферах національної безпеки держави";

"*загроза інформаційній безпеці* – наміри, дії (бездіяльність) або явища чи процеси, матеріалізація яких може призвести до таких негативних наслідків для людини, суспільства, держави:

неповноти, невчасності та невірогідності інформації, що використовується, а також відсутності інформації за її потреби;

негативного інформаційного впливу;

нерегульованого або злочинного застосування інформаційних технологій;

несанкціонованого розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, а також інших інформаційних ресурсів;

відсутності цілісної комунікативної політики держави;

низького рівня медіакультури суспільства";

"*реалізація загрози інформаційній безпеці* – матеріалізація намірів, дій

(бездіяльності) або явищ чи процесів, які призвели до будь-якого з негативних наслідків для людини, суспільства, держави у сфері інформаційної безпеки";

"*комунікативна політика держави* – сукупність офіційних поглядів, позицій та принципів, а також спрямованість діяльності органів державної влади та державного управління з питань спілкування із соціальним середовищем держави та міжнародною спільнотою для досягнення стратегічної взаємодії";

"*державні комунікації* – спілкування з будь-якою цільовою аудиторією від імені держави";

"*стратегічні комунікації* – скоординоване і належне використання національних комунікативних можливостей, спрямованих на просування цілей держави: публічної дипломатії, зв'язків із громадськістю, військових зв'язків, спілкування з цільовими аудиторіями у ході інформаційних операцій";

"*урядові комунікації* – комплекс заходів, що передбачають діалог уповноважених представників Уряду країни з цільовою аудиторією для роз'яснення урядової позиції та/або політики з певних проблемних питань";

"*кризові комунікації* – комплекс заходів, що реалізуються державними органами країни у кризовій ситуації і передбачають їх діалог із цільовою аудиторією з питань, що стосуються кризової ситуації";

"*медіакультура суспільства* – здатність соціальних груп країни сприймати, аналізувати, оцінювати медіатекст (повідомлення у формі газетної статті, телепередачі, відеокліпу, фільму тощо), а також займатися медіатворчістю та добувати нові знання у цій галузі";

"*захист інформаційних ресурсів* – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформаційних ресурсів та належний порядок доступу до них";

"*комп'ютерна (кібер-) злочинність* – вчинення правопорушень, пов'язаних з комп'ютерними системами і даними (інформацією), які визначені статтями 2-12 Конвенції про кіберзлочинність";

"*комп'ютерна система* – будь-який пристрій або група взаємно поєднаних або пов'язаних пристроїв (мережа), один чи більше з яких виконує автоматичну обробку даних (інформації) відповідно до певної програми";

"*комп'ютерні дані (інформація)* – будь-які дані (інформація) у формі, яка є придатною для обробки в комп'ютерній системі, включаючи програму, яка необхідна для виконання певної функції комп'ютерною системою";

"*протидія комп'ютерній (кібер-) злочинності* – комплекс правових, адміністративних, організаційних, інженерно-технічних заходів, спрямованих на запобігання правопорушень, пов'язаних з комп'ютерними системами і даними (інформацією), а також встановлення кримінальної відповідальності за вчинення таких правопорушень";

"*захист персональних даних* – захист основоположних прав і свобод людини і громадянина на невтручання в його особисте життя у зв'язку з обробкою його персональних даних";

"*правоохоронна діяльність в інформаційній сфері* – діяльність спеціально уповноважених органів держави шляхом застосування юридичних заходів впливу із суворим дотриманням встановленого законом порядку для охорони прав громадян, суспільних установ та організацій, а також держави провадити необмежену національним законодавством чи міжнародним правом діяльність в інформаційній сфері";

"*інформаційна дія* – окрема (поодинока) та однорідна цілеспрямована діяльність (робота, процес, зусилля тощо) в інформаційному просторі для отримання необхідної інформації (інформаційних ресурсів), або інформаційно-психологічного впливу на цільову аудиторію, або інформаційно-технічного впливу на інформаційну систему, або захисту від негативного інформаційного впливу";

"*інформаційний захід* – спланована інформаційна дія або їх взаємозв'язана сукупність для отримання переваги (виграшу, здобутку, досягнення) в інформаційному просторі.

Примітка. Типовими інформаційними заходами є інформаційна атака, інформаційна акція, інформаційна операція, інформаційна кампанія, а також впровадження нових інформаційних систем і технологій";

"*інформаційна атака* – короткочасна цілеспрямована інформаційна дія або сукупність кількох короткочасних узгоджених за метою, завданнями, об'єктами і часом однорідних інформаційних дій для оперативного несанкціонованого втручання у процес функціонування визначених об'єктів інформаційної інфраструктури або здійснення швидкого деструктивного впливу на певні цільові аудиторії";

"і*нформаційна акція* - сукупність

узгоджених та взаємозв'язаних за метою, завданнями, об'єктами і часом інформаційних дій та/або атак, зосереджених на відносно короткий період, які спрямовані на досягнення стійкого ефекту від втручання у процес функціонування інформаційних систем та/або інформаційно-психологічного впливу на визначені цільові аудиторії";

"*інформаційний удар* – результативність, наслідок інформаційної атаки (одночасно кількох атак) на один або кілька об'єктів інформаційної інфраструктури";

"*інформаційна операція* – сукупність узгоджених і взаємозв'язаних за метою, завданнями, об'єктами, місцем та часом одночасних і послідовних інформаційних акцій, атак, а також інших заходів, що проводяться за єдиним замислом та планом для сприяння вирішенню завдань реалізації національної політики в обраній сфері життєдіяльності держави в умовах виникнення міждержавного протистояння (конкуренції).

Примітка. Складовою інформаційної операції, як правило, є інформаційно-психологічна операція, що може проводитися також як самостійна";

"*інформаційно-психологічна операція* – сукупність узгоджених і взаємозв'язаних за метою, завданнями, об'єктами, місцем та часом одночасних і послідовних інформаційних акцій, атак, а також інших заходів, що проводяться за єдиним замислом та планом для вирішення завдань інформаційно-психологічного впливу на цільову аудиторію противника (конкурента) в умовах виникнення міждержавного протистояння";

"*інформаційна кампанія* - сукупність узгоджених і взаємозв'язаних за стратегічною метою, завданнями, об'єктами, місцем та часом одночасних і послідовних інформаційних операцій, акцій, атак, а також інших заходів, що проводяться за єдиним замислом та планом для сприяння вирішенню завдань реалізації національної політики в кількох сферах життєдіяльності держави.

Примітка. Елементами інформаційної кампанії, а також інформаційної (інформаційно-психологічної) операції можуть бути заходи стратегічних, урядових або кризових комунікацій держави".

Висновок. Запропоновані зміни до чинного інформаційного законодавства України, переважно термінологічні, за сутністю є похідними від фундаментального поняття "інформація", не суперечать йому та один одному, мають системний взаємозв'язок. На їх основі може бути удосконалено інші положення названих вище Законів України, а також інші нормативно-правові акти держави, що регулюють інформаційну сферу, чим буде досягнута їх відповідність вимозі Конституції України щодо забезпечення інформаційної безпеки держави та, відповідно, адекватність усіх наступних дій у цій галузі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Саричев Ю. О. Загальнотеоретичні передумови необхідності удосконалення чинного законодавства України з питань інформаційної безпеки держави / Ю. О. Саричев, П. М. Сніцаренко, В. А. Ткаченко // Збірник наукових праць ЦВСД НУОУ ім. І. Черняховського. – 2018. – № 1 (62). – С.62–67.
2. Закон України "Про інформацію" в редакції від 13.01.2011 № 2938-VI // Законодавство України [Електронний ресурс]. – Режим доступу : http: // zakon3.rada.gov.ua.
3. Закон України "Про телекомунікації" від 18.11.2003 № 1280-IV // Законодавство України [Електронний ресурс]. – Режим доступу : http: // zakon2.rada.gov.ua.
4. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII //Законодавство України [Електронний ресурс] – Режим доступу : http: // zakon2.rada.gov.ua.
5. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. – Режим доступу : http: // zakon5.rada.gov.ua.
6. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96/2016 [Електронний ресурс]. – Режим доступу : http: // president.gov.ua.
7. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25.02.2017 № 47/2017 [Електронний ресурс]. – Режим доступу : http: // president.gov.ua.
8. Воєнна доктрина України, затверджена Указом Президента України від 24.09.2015 № 555/2015 [Електронний ресурс]. – Режим доступу : http: // president.gov.ua.
9. Стратегічний оборонний бюлетень України, затверджений Указом Президента України від 20.05.2016 № 240/2016 [Електронний ресурс] – Режим доступу : http: // president.gov.ua.

Стаття надійшла до редакції 11.07.2018

Сницаренко П. Н., д.т.н., с.н.с.;
Саричев Ю. А., к.т.н., с.н.с.;
Семененко В. М., к.т.н., с.н.с.;
Ткаченко В. А., к.воен.н.
Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

Совершенствование действующего информационного законодательства Украины как необходимое условие адекватности мер по обеспечению информационной безопасности государства

Резюме. Обоснованы предложения по усовершенствованию действующего законодательства Украины по вопросам информационной безопасности государства.

Ключевые слова: информационное законодательство Украины, информационная безопасность государства, терминология.

P. Snicharenko, DsT, senior researcher;
Y. Sarichev, PhD (Technical), senior researcher;
V. Semenenko, PhD (Technical), senior researcher;
V. Tkachenko, PhD (Military)
Center for Military and Strategic Studies of the National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv

Improvement of the current information legislation of Ukraine as a necessary condition for the adequacy of measures to ensure the information security of the state

Resume. The preposition for improvement of current legislation of Ukraine in questions state information defense is grounded.

Keywords: information legislation of Ukraine, information defense of the state, terminology.