DOI 10.33099/2618-1614-2021-16-3-41-46
УДК 354

Т. М. Дзюба,
кандидат технічних наук, доцент,
доцент кафедри управління інформаційною
та кібернетичною безпекою,
Державний університет телекомунікацій

Обґрунтування концептуальних положень інформаційної безпеки України

В умовах інформаційної війни, яка є невід'ємною складовою російської гібридної агресії проти України, забезпечення інформаційної безпеки держави є одним з найважливіших завдань. Вирішення цього завдання пов'язане з необхідністю інтегрування різнорідних поглядів та підходів у єдиній концепції, яка б комплексно описувала всі напрями забезпечення інформаційної безпеки, встановлювала взаємозв'язки між об'єктами та суб'єктами інформаційної безпеки та визначала відповідні механізми запобігання/нейтралізації загроз інформаційній безпеці. За умови розроблення такої концепції стає можливим систематизація всієї діяльності й розроблення відповідного нормативно-правового забезпечення в зазначеній сфері.

Метою статті є обґрунтування концептуальних положень інформаційної безпеки України, сукупність яких могла би стати основою концепції інформаційної безпеки та всіх пов'язаних з нею нормативно-правових актів.

Подальші дослідження, основою яких є дана стаття, можуть спрямовуватися на конкретизацію суб'єктно-об'єктної взаємодії за типовими загрозами інформаційній безпеці, розроблення деталізованої концептуальної моделі інформаційної безпеки України, а також реальних практичних механізмів запобігання/нейтралізації загроз інформаційній безпеці.

Ключові слова: концепція, інформаційна безпека, загроза, ризик, об'єкти інформаційної безпеки, суб'єкти інформаційної безпеки, методи запобігання/нейтралізації загроз інформаційній безпеці.

В умовах збройної агресії проти України, яка у формі кампаній, операцій та акцій гібридної війни триває вже восьмий рік поспіль, надзвичайно актуальною є роль інформаційної безпеки України.

Використання традиційних підходів, які базуються або на тріаді захисту конфіденційності, цілісності та доступності інформації разом зі спостережністю функціонування інформаційних систем або на захисті власного інформаційного простору, сьогодні є малоефективним.

Сучасна інформаційна безпека – це динамічний процес, у якому заходи захисного характеру мають поєднуватися з активними заходами, спрямованими на формування необхідного стану інформаційного простору, просування власних змістів та ідей, превентивного знешкоджування джерел загроз інформаційній безпеці тощо.

Постановка проблеми. Сьогодні очевидною є неможливість розділення питань реалізації державної інформаційної політики та забезпечення власної інформаційної безпеки. В Україні ситуація ускладняється відсутністю офіційно визначених підходів до формування та реалізації державної інформаційної політики в той час, коли різні органи державної влади, складові сектору безпеки та оборони розробляють відповідні власні документи (стратегії, концепції тощо), виходячи з власного призначення, завдань, функцій та повноважень. Іншими словами, єдина концепція державної інформаційної політики відсутня. За таких умов проблематично узгодити інформаційну діяльність різних органів, що, у свою чергу, ускладнює реалізацію комплексного підходу до забезпечення інформаційної безпеки й такого напряму діяльності держави, як стратегічні комунікації.

Фактично те саме спостерігається у сфері інформаційної безпеки. Ми маємо Доктрину інформаційної безпеки України, яка сьогодні вже не повністю відповідає змісту Стратегії національної безпеки України та цілій низці нормативно-правових документів, що регулюють різні питання забезпечення інформаційної безпеки (захист інформації: технічний, криптографічний, правовий, організаційний; інші складові кібербезпеки, захист інтелектуальної власності та персональних даних тощо).

Аналіз останніх досліджень і публікацій. Чинна Доктрина інформаційної безпека України є другою редакцією цього документа. Перша така Доктрина була прийнята у 2009 р. [1]. В її основу були покладені результати наукових досліджень Інституту проблем національної безпеки Ради національної безпеки і оборони України (на теперішній час скорочений) [2]. Загальний підхід зазначеної редакції Доктрини базувався на єдності загроз інформаційній безпеці змістовного (контентного) і технологічного характеру, а також на конкретизації загроз інформаційній безпеці й відповідних напрямів нейтралізації цих загроз для кожної сфери національної безпеки України.

У подальшому наукові дослідження та відповідні нормативно-правові акти, що ґрунтувалися на результатах цих досліджень, розвивалися за двома паралельними напрямами: контентним (змістовним, для котрого визначальним є зміст інформації та його вплив на поведінку споживачів інформації), для якого залишилася назва «інформаційна безпека» і технологічним (для якого визначальним є технологічні аспекти створення, передачі, використання, знищення тощо інформації), з назвою «кібербезпека».

Сьогодні ми маємо розвинене законодавство за напрямом кібербезпеки (Закон України «Про основні засади забезпечення кібербезпеки України», Стратегію кібербезпеки України та відповідні підзаконні акти). До того ж Україна імплементує відповідні законодавчі документи міжнародного права в галузі кібербезпеки. Існує також достатня кількість наукових публікацій, серед яких доцільно виокремити монографії «Основи формування державної системи кібернетичної безпеки» В. Л. Бурячка, «Основи кібернетичної безпеки» Р. В. Грищука та Ю. Г. Даника, «Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи» А. В. Тарасюка, «Кіберпростір як новий вимір геополітичного суперництва» Д. В. Дубова, підручники, навчальні посібники та наукові праці В. Б. Толубка, В. А. Савченка, О. Г. Корченка, С. В. Толюпи, Ю. Г. Даника, Р. В. Грищука, В. Л. Бурячка, В. В. Семка, Д. В. Дубова, С. Л. Гнатюка, В. О. Бойка, Ю. І. Хлапоніна.

Уже існує також значна кількість наукових робіт за контентним напрямом інформаційної безпеки, до яких слід віднести насамперед численні монографії Г. Г. Почепцова, наукові праці А. О. Рося, І. В. Замаруєвої, Л. Ф. Компанцевої, А. В. Баровської, О. М. Хайруліна, Я. М. Жаркова, М. Т. Дзюби, чудові дослідження Оксани Мороз «Нація овочів» та «Боротьба за правду». Окремо слід відзначити книгу Д. Ю. Золотухіна «Біла книга спеціальних інформаційних операцій проти України: 2014–2018» [3], у якій на прикладах реальних інформаційних операцій проти України визначені конкретні шляхи забезпечення інформаційної безпеки.

Інтегрований підхід до забезпечення інформаційної безпеки України без її розділення на контентний і технологічний напрями викладений передусім у монографії «Проблеми захисту інформаційного простору України» В. П. Горбуліна та М. М. Биченка [2] і численних працях А. О. Рося. Серед останніх досліджень слід виокремити монографії «Консолідація інформаційного законодавства України» та «Інкорпорація інформаційного законодавства України» В. А. Ліпкана, «Інформаційна безпека держави» В. М. Богуша та О. К. Юдіна, наукові праці В. Ю. Богдановича, Р. Р. Марутян, В. М. Петрика, М. М. Присяжнюка.

У всіх зазначених наукових працях викладені аргументовані авторські погляди на різні аспекти інформаційної безпеки, однак невирішеним залишається завдання інтеграції різних поглядів та підходів у єдину концепцію, яка могла би стати основою для розроблення відповідних нормативно-правових актів, визначення та практичної реалізації комплексних механізмів запобігання та реагування на загрози інформаційній безпеці, активного впливу на світовий інформаційний простір для задоволення національних інтересів України.

Метою статті є обґрунтування концептуальних положень інформаційної безпеки України, сукупність яких могла би стати основою концепції інформаційної безпеки та всіх пов'язаних з нею нормативно-правових актів.

Виклад основного матеріалу дослідження

У роботі [4] Г. П. Ситник запропонував ієрархію керівних документів державної політики такого вигляду (*рис. 1*).

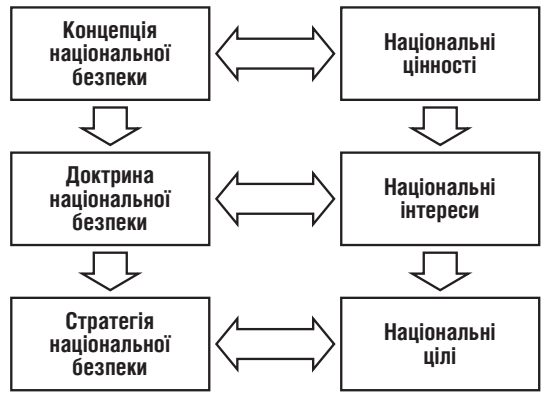

Рис. 1. Ієрархія керівних документів державної політики (за Г. П. Ситником)

Відповідно до зазначеного підходу, концепція є визначальним документом, у якому зазначаються національні цінності держави і викладаються загальні підходи до їх збереження та примноження.

Авторка дослідження [5] пропонує мати єдину доктрину інформаційної політики та безпеки, на підставі якої документи нижчих рівнів ієрархії (концепції, стратегії, державні цільові програми, національні проєкти) розробляти окремо за напрямами:

- розвитку національного інформаційного простору;
- розвитку інформаційного суспільства;
- розвитку офіційної комунікації;
- інформаційної безпеки.

План реалізації всіх заходів, визначених державними цільовими програмами різних напрямів, має бути, на думку авторки дослідження, спільним.

Ураховуючи безпосередній зв'язок та ієрархічну підпорядкованість концепції інформаційної безпеки загальній доктрині інформаційної політики та безпеки, а також необхідність визначення в концепції основних положень стратегії інформаційної безпеки, яка перебуває нижче за ієрархією, доцільно визначити такий зміст концептуальних положень інформаційної безпеки:

1) національні цінності, які необхідно захищати від загроз інформаційного характеру;

2) національні інтереси, задоволення яких потребує захисту від загроз інформаційного характеру;

3) місце інформаційної безпеки в системі національної безпеки держави;

4) роль інформаційної безпеки для забезпечення національної безпеки держави;

5) об'єкти інформаційної безпеки (відповідно до національних цінностей та інтересів, а також до змісту загроз інформаційного характеру);

6) загрози інформаційній безпеці України;

7) суб'єкти (сили) забезпечення інформаційної безпеки;

8) методи запобігання/нейтралізації загроз інформаційній безпеці України.

Оскільки існує суттєва різниця між загрозами інформаційній безпеці та відповідними методами їх запобігання/нейтралізації контентного й технологічного характеру, доцільно ці два напрями інформаційної безпеки розглядати окремо, але в єдиній системі та з інтегруванням відповідних їхніх заходів у тих випадках, коли це можливо та/або необхідно.

Національні цінності. У ранніх виданнях радянських енциклопедій було таке визначення нації: «Нація є стійка спільність людей, що історично склалася, виникла на основі спільності мови, території, економічного життя і психічного складу, який проявляється у спільності культури». Це визначення в подальшому піддавалося критиці, змінювалось, удосконалювалось, однак саме в такому визначенні присутні ті національні цінності, які підлягають захисту від загроз будь-якого характеру.

Цими цінностями є територія, історія, мова, культура, економіка. Доцільно до них додати таку цінність, як державний суверенітет, тобто верховенство держави на своїй території та незалежність у міжнародних відносинах [6].

Таким чином, система інформаційної безпеки має захищати від загроз, пов'язаних зі спробами (та вже існуючими фактами) захоплення/зменшення нашої території; переписування та вільного трактування (в інтересах інших держав) нашої історії; знецінення нашої мови та культури, зменшення їхніх ролі й ваги у світі; погіршення нашого економічного стану; впливу на наш державний суверенітет.

Підтвердженням даного припущення є характер та зміст інформаційних операцій, які Російська Федерація проводить проти України, починаючи з отримання Україною незалежності й до сьогодні.

Національні інтереси. Класичним підходом до визначення національних інтересів є їх визначення для трьох об'єктів національної безпеки: громадянина (людини, особи), суспільства (організованої сукупності людей на певному етапі історичного розвитку, об'єднаних характерними для них відносинами) та держави (політичної форми організації правління, що характеризується суверенною владою, політичним та публічним характером, реалізацією своїх повноважень на певній території через систему спеціально створених органів та організацій, за допомогою яких здійснюється політичне, економічне та ідеологічне управління суспільством і керівництво загальносуспільними правами).

Національними інтересами щодо громадянина можуть бути забезпечення його права на вільне створення, поширення, використання, знищення тощо інформації (якщо ця інформація не загрожує національним цінностям та інтересам інших громадян, суспільства та української держави); забезпечення права та можливостей на отримання достовірної та повної інформації, необхідної для життя й розвитку (з обмеженнями на отримання конфіденційної інформації інших громадян і держави); забезпечення стану інформаційного простору, в якому відсутні шкідливі інформаційні впливи на психіку громадян України та відвернені шкідливі впливи технологічного характеру (кібервпливи).

Національними інтересами щодо суспільства можуть бути забезпечення розвитку суспільства шляхом створення відповідного стану інформаційного простору; запобігання будь-яким інформаційним впливам, спрямованим на порушення єдності суспільства, унеможливлення та ускладнення зв'язків між членами суспільства; унеможливлення зміни історичних та культурних цінностей, сформованих норм і правил поведінки суспільства.

Національними інтересами щодо держави можуть бути зміцнення довіри громадян і суспільства до влади; збільшення рівня міжнародної підтримки та допомоги; посилення ролі України у світі; унеможливлення впливу колабораціоністських та сепаратистських ідей на становище й розвиток України; стійкість до всіх (контентних і технологічних) інформаційних впливів на всі сфери життєдіяльності держави.

Місце та роль інформаційної безпеки. В останній (чинній) редакції Стратегії національної безпеки України [7] відсутній розподіл на окремі сфери національної безпеки. Однак у заключних положеннях цього документа визначені документи стратегічного планування за окремими напрямами діяльності нашої держави. Ці напрями можна розглядати як окремі сфери національної безпеки.

Якщо розглядати сфери інформаційної безпеки та кібербезпеки відірвано від інших сфер національної безпеки, то визначити властиві їм загрози (особливо національного, стратегічного рівня) майже неможливо, оскільки інформація та інформаційні процеси набувають цінності та ваги лише у зв'язку з конкретною діяльністю. Водночас сьогодні прояви загроз інформаційній безпеці, такі як дискредитація керівництва, компрометація діяльності, дезінформація, використання шкідливого програмного забезпечення, блокування доступу до інформаційних ресурсів, викрадення конфіденційної інформації, несанкціонована модифікація інформаційних ресурсів тощо спостерігаються в усіх без винятку сферах життєдіяльності наших суспільства й держави. Тобто

інформаційна безпека (включно з кібербезпекою) займає сьогодні центральне місце серед інших сфер національної безпеки та відіграє в системі національної безпеки держави інтегруючу й системоутворюючу роль, оскільки блокує впливи і загрози для інших сфер національної безпеки.

Визначена інтегруюча та системоутворююча роль інформаційної безпеки зумовлена відповідної роллю інформаційної сфери (сфери діяльності, пов'язаної зі створенням (виробництвом), перетворенням, обробкою, зберіганням, поширенням інформації та знань; сукупністю інформації, інформаційної інфраструктури та системи регулювання суспільних відносин, які виникають під час створення, обробки, поширення й використання інформації).

Об'єкти інформаційної безпеки. Оскільки інформаційна безпека (зокрема кібербезпека) є невід'ємною складовою системи національної безпеки України, її об'єкти не можуть відрізнятися від об'єктів національної безпеки. Тобто об'єктами інформаційної безпеки (зокрема кібербезпеки) є людина і громадянин, суспільство й держава.

Залежно від загроз інформаційній безпеці та напряму діяльності нашої держави загальні об'єкти інформаційної безпеки можуть уточнюватися та конкретизуватися.

Так, якщо розглядати контекстну (змістовну) складову інформаційної безпеки, то доцільніше розглядати як об'єкти ті чи інші цільові аудиторії, які можуть бути як окремими особами (наприклад керівниками органів державної влади, лідерами громадської думки, відомими політиками, громадськими діячами та ін.), так і певними соціальними групами, однорідними за визначальними характеристиками (місцем проживання, ставленням до державної влади, соціально-економічним становищем, зайнятістю, віком, статтю, освітою тощо).

Технологічна складова інформаційної безпеки (кібербезпеки) потребує визначення інформаційних процесів, систем та ресурсів, пов'язаних з діяльністю об'єктів інформаційної безпеки (людини, суспільства й держави) для їх захисту від загроз кібербезпеці та створення в інформаційному просторі умов для задоволення національних інтересів.

Загрози інформаційній безпеці. У статті [8] пропонується в кожній загрозі національній безпеці України окремо виділяти інформаційну частину, оскільки так чи інакше реалізація кожної загрози використовуватиме інформаційний простір. Цей підхід є найбільш логічним і відповідним сутності та змісту загроз інформаційній безпеці.

Будь-яку загрозу інформаційній безпеці (контентній складовій) можна представити таким чином. Існує джерело загрози (людина, організація, природне явище, збіг різних обставин тощо), яке створює (використовує вже створену, отримує доступ, зокрема несанкціонований, до інформації, котра є важливою, значущою та може бути використана) якусь інформацію. Через інформаційний простір інформація від джерела надсилається (поширюється) до об'єкта впливу. Результатом має стати зміна поведінки об'єкта впливу так, як це потрібно джерелу загрози (активні дії об'єкта впливу; підтримка/засудження об'єктом впливу тих чи інших ідей, процесів, персон; прийняття рішення об'єктом впливу щодо власного поширення інформації, отриманої від джерела загрози тощо).

Найтиповішими загрозами для контентної складової інформаційної безпеки є поширення конфіденційної (для об'єкта впливу) інформації (leaks); дискредитація та компрометація ідей, процесів, персон, організацій; дезінформація (поширення фейків, неповної та упередженої інформації); перевантаження нерелевантною інформацію (забовтування, розкручування неважливої другорядної тематики тощо); використання технологій зомбування (під час створення та поширення інформації); тиск та залякування.

Відповідно, кожну загрозу кібербезпеці (технологічній складовій інформаційної безпеки) можна представити таким чином. Для задоволення національних інтересів об'єкти національної безпеки використовують інформаційні ресурси та системи, організуючи при цьому відповідні інформаційні процеси. Порушення порядку та правил доступу до інформаційних ресурсів, необхідних для задоволення національних інтересів, їхня несанкціонована модифікація та/або знищення, порушення нормального перебігу інформаційних процесів та нормального режиму функціонування інформаційних систем, порушення порядку доступу та використання інформаційних систем перешкоджають або ускладнюють задоволення національних інтересів. Для таких загроз також визначається джерело (антропогенне, техногенне, стихійне) та особливості реалізації загрози в інформаційному просторі.

Найтиповішими загрозами для кібербезпеки (технологічної складової) інформаційної безпеки є: несанкціоноване збирання інформації (перехоплення, прослуховування, використання шпигунського апаратного та програмного забезпечення тощо); несанкціонований доступ до інформаційних ресурсів, систем та процесів; викрадення та/або модифікація чи знищення інформаційних ресурсів; виведення з ладу, перевантаження, знищення апаратного та програмного забезпечення інформаційних систем; несанкціоноване внесення змін у структуру та спрямованість інформаційних процесів.

І контентні, і технологічні загрози інформаційній безпеці проявляються практично в усіх сферах національної безпеки. Відповідно, від прогнозованих наслідків реалізації загрози інформаційній безпеці для кожної сфери національної безпеки (оцінених ризиків) доцільно визначити основні, пов'язані та другорядні об'єкти. Наприклад, хакерське угрупування, пов'язане з Російською Федерацією, планує виведення з ладу автоматизованої системи управління технологічним процесом енергорозподільчої енергетичної компанії в одній з областей України. Очевидно, що головним об'єктом такої загрози є сфера енергетичної безпеки України (відповідні центральні

та регіональні органи виконавчої влади). Пов'язаними є сфери: воєнної безпеки, соціальна, економічна, охорони громадського порядку; інші можуть вважатися другорядними. Запропонований підхід до встановлення відповідності між загрозою інформаційній безпеці та конкретним об'єктом дає змогу класифікувати загрози інформаційній безпеці за всіма сферами національної безпеки України, значно спрощує визначення суб'єктів та методів нейтралізації загроз.

Суб'єкти інформаційної безпеки. Визначення суб'єктів інформаційної безпеки потребує усвідомлення процесу забезпечення інформаційної безпеки та чіткого уявлення про всі можливі методи запобігання/реагування на відповідні загрози.

Передусім загроза інформаційній безпеці має бути виявлена та оцінена (розраховані ризики для всіх об'єктів та сфер національної безпеки). Традиційно завдання виявлення та оцінювання загроз покладається на розвідувальні органи (можливе додаткове залучення аналітичних структур, якщо власні можливості розвідувальних органів недостатні для якісного оцінювання загрози інформаційній безпеці). Однак, ураховуючи постійну високу динаміку інформаційних процесів у сучасному інформаційному просторі, доцільніше включити до суб'єктів забезпечення інформаційної безпеки не розвідувальні органи, а спеціалізовані ситуаційні центри, які в онлайн режимі здійснюють моніторинг інформаційного простору, отримують розвідувальну інформацію від розвідувальних органів, узагальнюють усю отриману інформацію та здійснюють загальне оцінювання і прогнозування розвитку ситуації. Такі ситуаційні центри, об'єднані в єдину систему електронних комунікацій, доцільно створити в кожній сфері національної безпеки.

Звіт про результати виявлення та оцінювання загрози інформаційній безпеці з прогнозованими значеннями ризиків її реалізації в усіх можливих сферах національної безпеки надходить до органу, уповноваженого приймати рішення щодо обробки ризиків та задіяння до запобігання/нейтралізації загрози відповідних виконавчих органів.

Ураховуючи особливості організації державного управління, в Україні такими суб'єктами можуть бути Президент України, Кабінет Міністрів України, Верховна Рада України, сили безпеки та оборони України й суди.

Крім того, враховуючи системоутворюючу та всеосяжну роль інформаційної сфери, як суб'єкти інформаційної безпеки мають розглядатись усі громадяни України та їх відповідні об'єднання (політичні партії, громадські організації тощо).

Серед усієї сукупності суб'єктів інформаційної безпеки України доцільно окремо розглядати ті, які відповідають за формування державної політики (за тим чи іншим напрямом забезпечення інформаційної безпеки), і ті, котрі мають у своєму складі органи, спроможні проводити заходи забезпечення інформаційної безпеки.

Так, сьогодні захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного та оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, забезпечення охорони державної таємниці, боротьба з тероризмом (зокрема з інформаційним тероризмом) покладені на Службу безпеки України; кіберзахист державних інформаційних ресурсів, технічний та криптографічний захист – на Державну службу спеціального зв'язку та захисту інформації України; захист персональних даних – на Уповноваженого Верховної Ради України з прав людини (Департамент у сфері захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини); захист інтелектуальної власності – на Міністерство економіки України; формування та реалізація державної політики у сферах культури, державної мовної політики, популяризації України у світі, державного іномовлення, інформаційного суверенітету України та інформаційної безпеки – на Міністерство культури та інформаційної політики України; забезпечення захисту національних інтересів України у сфері міжнародних відносин, реалізація зовнішньополітичного курсу України, спрямованого на розвиток політичних, економічних, культурних, гуманітарних, наукових та інших зв'язків з іноземними державами, міжнародними організаціями, сприяння утвердженню міжнародного авторитету України, піднесенню у світі її іміджу як надійного та передбачуваного партнера – на Міністерство закордонних справ України; формування й реалізація державної політики у сфері цифровізації, відкритих даних, національних електронних інформаційних ресурсів, інтероперабельності – на Міністерство цифрової трансформації України; боротьба з кіберзлочинністю – на Міністерство внутрішніх справ та Національну поліцію України; проведення інформаційних та психологічних операцій – на Збройні Сили України.

Особливість зазначених суб'єктів інформаційної безпеки полягає в тому, що вони, крім безпосереднього виконання своїх функцій, визначають, формують та організовують реалізацію відповідної державної політики за зазначеними напрямами інформаційної безпеки (тобто можуть установлювати обмеження та визначати відповідні правові механізми).

Невирішеним проблемним питанням залишається координація діяльності різних суб'єктів інформаційної безпеки, оскільки це завдання не покладене на жодного з них. Логічним є створення координуючого органу, підпорядкованого Президенту України, оскільки саме Президент, відповідно до Конституції України, забезпечує державну незалежність, національну безпеку і правонаступництво держави.

Методи запобігання/нейтралізації загроз інформаційній безпеці України. Усі методи запобігання/нейтралізації загроз інформаційній безпеці України можна розділити на:

• адміністративно-правові, які передбачають визначення та використання правових механізмів щодо різних дій з інформацією, інформаційних процесів та систем, інформаційного простору;

• активного впливу, які передбачають запобігання виникненню загроз інформаційній безпеці; виявлення, блокування або знешкодження джерел загроз інформаційній безпеці; реагування на ті загрози інформаційній безпеці, яким не вдалося запобігти; формування необхідного (для забезпечення національної безпеки України) стану інформаційного простору;

• програмно-технічні, які передбачають розроблення та використання апаратних та програмних систем захисту інформаційного простору, інформаційних процесів та ресурсів, важливих для національної безпеки України;

• освітні, спрямовані на формування у громадян України навичок медіаграмотності, кібергігієни та цифрових компетентностей, необхідних для забезпечення стійкості, тобто здатності до функціонування в умовах постійного впливу загроз інформаційній безпеці (в умовах інформаційної війни);

• відновлювальні, спрямовані на відновлення попереднього стану національної безпеки в разі реалізації загроз інформаційній безпеці.

Використання тих чи інших методів залежить від результатів оцінювання ризиків та прийнятого рішення, яким (за класичними підходами з теорії ризиків) можуть бути:

• уникнення ризику (запобігання загрозі інформаційній безпеці або коригування власних дій, яке унеможливлює появу відповідної загрози);

• протидія ризику (нейтралізація загрози інформаційній безпеці, зменшення наслідків її реалізації);

• перенесення ризику (залучення додаткової зовнішньої допомоги для нейтралізації загрози інформаційній безпеці);

• прийняття ризику (свідоме прийняття факту реалізації загрози інформаційній безпеці та її наслідків). Прийняття ризику можливе за умови сформованої стійкості громадян, суспільства та держави.

Висновки і перспективи подальших досліджень

Наведені у статті концептуальні положення інформаційної безпеки дають можливість чітко встановити зв'язки й відношення між різними елементами концепції, що дає змогу побудувати концептуальну модель і системно підійти до розроблення необхідних нормативно-правових актів у сфері інформаційної безпеки; визначити невирішені та проблемні питання, запропонувати механізми їх вирішення.

Подальші дослідження доцільно спрямувати на конкретизацію суб'єктно-об'єктної взаємодії за типовими загрозами інформаційній безпеці, розроблення деталізованої концептуальної моделі інформаційної безпеки України, а також реальних практичних механізмів запобігання/нейтралізації загроз інформаційній безпеці.

Перелік літератури

1. Доктрина інформаційної безпеки України [Електронний ресурс] : затверджена Указом Президента України № 514/2009 від 8 липня 2009 р.: (Указ втратив чинність на підставі Указу Президента № 504/2014 від 06.06.2014) // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/514/2009#Text.

2. *Горбулін В. П.* Проблеми захисту інформаційного простору України : монографія / В. П. Горбулін, М. М. Биченок ; Ін-т проблем національної безпеки ; Рада нац. безпеки і оборони України. – К. : Інтертехнологія, 2009. – 135 с.

3. Біла книга спеціальних інформаційних операцій проти України 2014–2018 [Електронний ресурс] / [під заг. ред.] Д. Ю. Золотухіна. – К. : Мега-прес груп, 2018. – 382, [2 с]. – Режим доступу : https://mip.gov.ua/files/pdf/white_book_2018_mip.pdf.

4. *Ситник Г. П.* Державне управління національною безпекою України : монографія / Г. П. Ситник. – К. : НАДУ, 2004. – 408 с.

5. *Баровська А. В.* Оптимізація структури керівних документів державної політики (на прикладі інформаційної сфери) [Електронний ресурс] : аналітична доповідь / А. В. Баровська ; Національний інститут стратегічних досліджень. – К. : НІСД, 2011. – 88 с. – Режим доступу : https://niss.gov.ua/sites/default/files/2012-03/Barovska_dop-e16cb.pdf.

6. Державний суверенітет в умовах європейської інтеграції : монографія / за ред. Ю. П. Битяка, І. В. Яковюка ; Нац. акад. прав. наук України, НДІ держ. буд-ва та місц. самоврядування. – К. : Право України, 2012. – 336 с.

7. Стратегія національної безпеки України [Електронний ресурс] : затверджена Указом Президента України № 392/2020 від 14 вересня 2020 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/392/2020#Text.

8. *Дзюба Т. М.* Розроблення паспорту загрози для системи раннього виявлення загроз національній безпеці України [Електронний ресурс] / Т. М. Дзюба, М. І. Опанасенко // Кібербезпека: освіта, наука, техніка. – 2020. – № 4 (12). – С. 61–68. – Режим доступу : https://doi.org/10.28925/2663-4023.2021.12.6168.