УДК 351.746.1

І. В. Кукін
кандидат наук із державного управління,
перший заступник начальника
Головного центру управління службою
Державної прикордонної служби України

СУЧАСНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНІ

У статті досліджуються окремі питання законодавчого врегулювання у сфері національної безпеки. Так, визначено прогалини у Законі «Про національну безпеку України» щодо забезпечення інформаційної безпеки. З урахуванням законодавства України та рекомендацій стандартів управління якістю діяльності ISO серії 9000 запропоновано та обґрунтовано порядок опрацювання документів стратегічного планування з питань забезпечення інформаційної безпеки.

Ключові слова: *інформаційна безпека, інформаційна війна, стратегія інформаційної безпеки, національна безпека, інформаційна політика, стратегічне планування, об'єкти інформаційної безпеки, суб'єкти інформаційної безпеки.*

Постановка проблеми. Одним з елементів сучасних війн можна вважати намагання агресора чинити постійний деструктивний інформаційний вплив на свідомість людей. Його наслідки можуть призводити до проявів сепаратизму, масових фактів перешкоджання населенням держави діяльності органів державної влади та місцевого самоврядування, що знайшло підтвердження під час окупації Російською Федерацією частини території України.

Негативні чинники інформаційного протиборства продовжують впливати на свідомість громадян. У доктрині інформаційної безпеки України акцентовано увагу на недостатній ефективності державної інформаційної політики, недосконалості законодавства в інформаційній сфері, недостатньому рівні медіакультури українського суспільства.

Аналіз останніх досліджень і публікацій. Проблеми забезпечення інформаційної безпеки в системі національної безпеки України досліджувались У. Липпманом, Г.П. Ситником, О.А. Панченко, Н.В. Банчуком В.М. Петриком, М.М. Присяжнюком, О.А. Семенченко О.А. Чуваковим, А.В. Бедрицьким та іншими дослідниками. Водночас схвалення Верховною Радою України у 2018 році Закону України «Про національну безпеку України» вимагає проведення подальших досліджень стратегічного планування щодо забезпечення інформаційної безпеки.

Метою статті є виявлення прогалин та протиріч у чинному законодавстві України з питань забезпечення інформаційної безпеки як окремої підсистеми національної безпеки України.

Виклад основного матеріалу. У монографії О.А. Панченко та Н.В. Банчука акцентовано увагу на тому, що людина постійно перебуває під впливом інформації, яка розповсюджується як довільно, так і цілеспрямовано. Вплив інформації може бути конструктивним (безпечним) та деструктивним. Він одночасно впливає як на окрему людину, так і на суспільство в цілому [1, с. 139].

Загальні основи та принципи національної безпеки й оборони визначені Законом «Про національну безпеку України». Під національною безпекою розуміється «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [2].

Основними складниками національної безпеки законодавець визначив воєнну, громадську та державну безпеки. Державна політика у зазначених сферах

спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки та кібербезпеки [2]. Синергетичний характер терміна «безпека» полягає в об'єднанні в цілісну систему, зокрема політичної, економічної, соціальної та духовної сфер діяльності [3, с. 16].

Погоджуємось із думкою М.М. Присяжнюка, що інформаційна безпека є невід'ємним складником національної безпеки та визначається як «стан захищеності особи, суспільства і держави, за якого досягається інформаційного розвитку (технічного, інтелектуального, соціально-політичного, морально-етичного), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди». Вона спрямовується на захист особистості, суспільства та держави [4, с. 8]. Окремі науковці до об'єктів інформаційної безпеки також зараховують міжнародну спільноту.

На думку Уолтера Липпмана, проблема невідповідності реальності суспільної думки зумовлюється неправильним описом перебігу подій особами, які безпосередньо брали в них участь. Він підкреслює, що новини не завжди відповідають дійсності. Функція новин – повідомлення про подію. Функція істини – виявлення прихованих фактів, установлення між ними зв'язків, формування необхідного для ухвалення рішень інформаційного поля. Для отримання істини бажано бути свідком подій [5, с. 61].

Погоджуємось із думкою А.В. Бедрицького, що основними мішенями інформаційних операцій можуть бути такі: політичне та військове керівництво держави, промисловість та енергетика, інфраструктура (транспорт та комунікації), населення держави, військові підрозділи [6, с. 56].

Наведена у Законі «Про національну безпеку України» термінологія дозволяє припустити, що інформаційна безпека є складником державної безпеки, оскільки вона має невоєнний характер та забезпечує «…захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших важливих національних інтересів від реальних і потенційних загроз невоєнного характеру» [2].

Військовим стандартом України визначено, що інформаційна боротьба – це «комплекс скоординованих заходів, які проводяться органами державного і військового управління та визначеними силами і засобами сторін із метою завоювання та утримання інформаційної противаги над противником шляхом впливу на його інформаційну інфраструктуру та інформацію, що в ній циркулює, а також підриву морально-психологічної стійкості особового складу військ і населення противника з одночасним захистом від аналогічного впливу з його боку» [7].

Отже, інформаційну безпеку можна розглядати представником як воєнної, так і громадської безпеки. Частку деструктивної інформації може бути спрямовано агресором на руйнування морально-психологічного потенціалу сил безпеки та оборони (Збройні Сили України, військові формування, правоохоронні, розвідувальні органи тощо), зниження захищеності важливих інтересів, прав і свобод людини і громадянина щодо поширення, збирання, накопичення, перетворення та використання інформації.

Оскільки ухвалення рішень із протидії загрозам національній безпеки потребує використання своєчасної та достовірної інформації, то деструктивний інформаційний вплив здійснюється агресором для унеможливлення ухвалення органами державної влади та місцевого самоврядування своєчасних та адекватних управлінських рішень.

Загрози національної безпеки, цілі, завдання, механізми захисту національних інтересів визначаються Стратегією національної безпеки України, яка є основою планування та реалізації державної політики. На її основі розробляється система документів довгострокового планування та звітності, що показана на рис. 1.

Основними документами стратегічного планування, що розробляються на виконання стратегії національної безпеки України, можна вважати національну розвідувальну програму та стратегії: воєнної безпеки, громадської безпеки та цивільного захисту, розвитку оборонно-промислового комплексу, кібербезпеки. Із метою визначення стану реалізації, уточ-

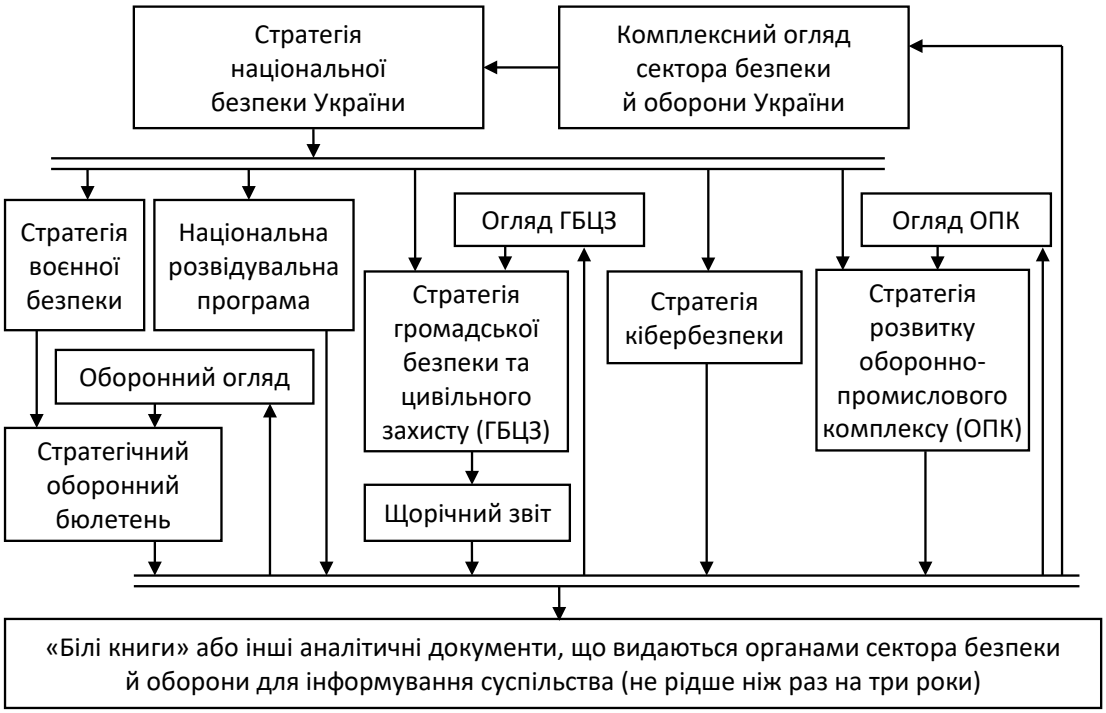

Рис. 1. Система документів планування та звітності у сфері національної безпеки й оборони

нення дійсних та визначення нових загроз і ризиків суб'єктами національної безпеки України опрацьовуються стратегічний оборонний бюлетень, огляди та звіти. На підставі комплексного огляду сектора безпеки й оборони України розробляється нова редакція стратегії національної безпеки України. Обов'язковість розроблення стратегії інформаційної безпеки у Законі «Про національну безпеку України» не визначено.

Сектор безпеки й оборони утворюють: «система органів державної влади, Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних та розвідувальних органів, державних органів спеціального призначення з правоохоронними функціями, сил цивільного захисту, оборонно-промислового комплексу України, діяльність яких спрямована на захист національних інтересів України від загроз, а також громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки України» [2].

До його складу входять: «Міністерство оборони України, Збройні Сили України, Державна спеціальна служба транспорту, Міністерство внутрішніх справ України, Національна гвардія України, Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба України з надзвичайних ситуацій, Служба безпеки України, Управління державної охорони України, Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки й оборони України, розвідувальні органи України, центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику. Інші державні органи та органи місцевого самоврядування здійснюють свої функції із забезпечення національної безпеки у взаємодії з органами, які входять до складу сектора безпеки й оборони». Координацію діяльності здійснює Рада національної безпеки й оборони України [2].

На думку О.А. Чувакова, питання забезпечення безпеки стосується всіх сфер життєдіяльності людини. Інформаційна безпека може вважатися самостійною сферою забезпечення національної безпеки [8, с. 8].

Указом Президента України у 2017 році схвалено Доктрину інформаційної безпеки

України. У цьому документі визначено національні інтереси, загрози, напрями, пріоритети та механізми реалізації державної політики в інформаційній сфері. Завдання координації діяльності центральних та місцевих органів виконавчої влади у сфері забезпечення інформаційного суверенітету покладено на Міністерство інформаційної політики України [9].

Основними пріоритетами державної політики Україні в інформаційній сфері визначено створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них, урегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору шкідливої інформації, створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, побудову дієвої та ефективної системи стратегічних комунікацій, розвиток механізмів взаємодії держави та інститутів громадянського суспільства, боротьбу з дезінформацією та деструктивною пропагандою, посилення можливостей сектора безпеки й оборони щодо протидії спеціальним інформаційним операціям із боку країни-агресора, недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні, забезпечення захисту і розвитку інформаційного простору України, комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації, підвищення медіаграмотності суспільства, пропагування в Україні державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту від зовнішніх і внутрішніх загроз [9].

Відповідно до Положення про Міністерство інформаційної політики України, його основними повноваженнями у сфері забезпечення інформаційної безпеки можна вважати нормативно-правове регулювання та розроблення програмних документів у сфері захисту інформаційного простору України від зовнішнього інформаційного впливу, поширення суспільно важливої інформації, забезпечення функціонування державних інформаційних ресурсів, участь у формуванні державної інформаційної політики, вжиття заходів щодо захисту прав громадян на вільне збирання, зберігання, використання і поширення інформації, координацію діяльності органів виконавчої влади та взаємодію з органами місцевого самоврядування, організацію досліджень впливу засобів масової інформації на суспільну свідомість, участь в організації навчання фахівців у сфері інформаційної політики, моніторинг матеріалів у засобах масової інформації, участь в опрацюванні планів заходів та програм щодо позитивного позиціонування України у світі [10].

На нашу думку, визначений у Законі «Про національну безпеку України» перелік документів стратегічного планування (див. рис. 1) може також уміщувати стратегію інформаційної безпеки, огляд виконання стратегії інформаційної безпеки. Підґрунтям для опрацювання стратегії інформаційної безпеки має слугувати стратегія національної безпеки України, яка розробляється з урахуванням комплексного огляду сектора безпеки й оборони України. Основні процеси стратегічного планування щодо забезпечення інформаційної безпеки наведено на рис. 2.

Під час опрацювання огляду виконання стратегії інформаційної безпеки доцільно врахувати оцінку реалізації цієї стратегії суб'єктами національної безпеки, оцінку її реалізації незалежними експертами, пропозиції від громадян та результати незалежного опитування громадської думки. Нові здобутки у сфері інформаційної безпеки також можуть оприлюднюватись Міністерством інформаційної політики України у відповідному розділі «Білої книги». Зазначені звітні документи є необхідними для опрацювання комплексного огляду сектора безпеки й оборони України, на підставі якого розробляється нова редакція стратегії національної безпеки України.

Підґрунтям цього є стаття 17 Конституції України, яка визначає, що «забезпечення ... економічної та інформаційної безпеки є найважливішими функціями держави…» [11]. Також запровадження системи управління якістю діяльності в органах державної влади та місцевого самоврядування потребує врахування всіх можливих джерел розбіжностей реальних

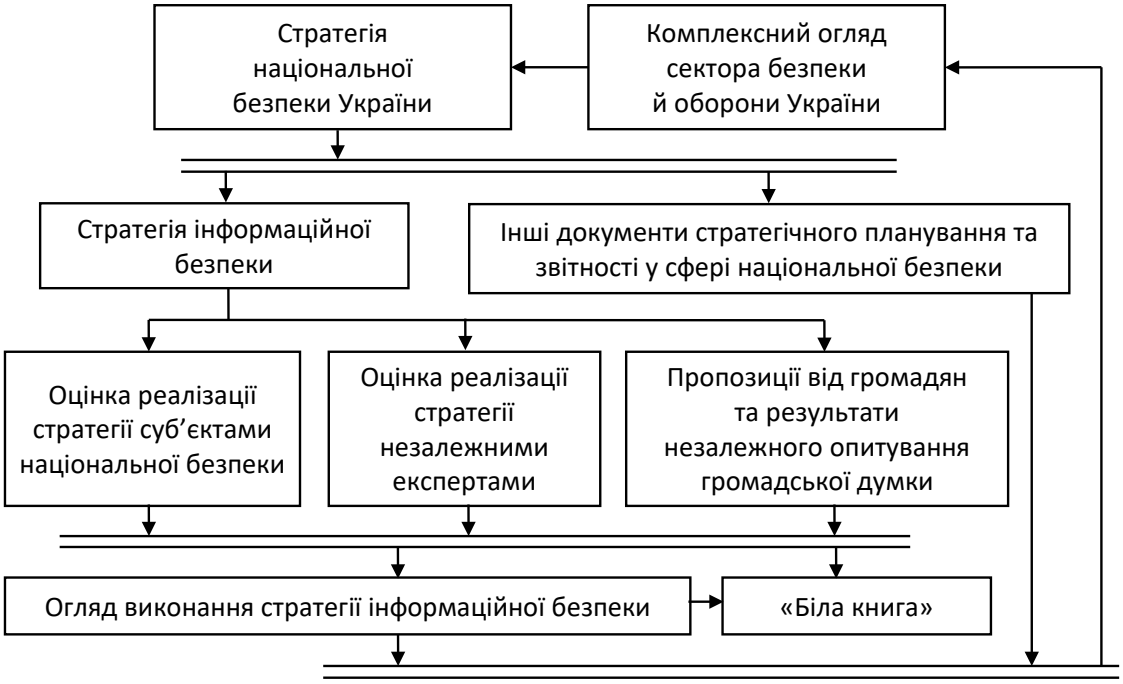

Рис. 2. Основні процеси стратегічного планування щодо забезпечення інформаційної безпеки

та очікуваних усіма категоріями споживачів (окрема особа, суспільство, держава) властивостей державних послуг [12, с. 7]. Застосування рекомендацій стандартів ДСТУ ISO серії 9000 не суперечить визначеним Законом «Про національну безпеку України» засадам демократичного цивільного контролю над сектором безпеки й оборони [2].

На нашу думку, одна з основних проблем нормативної регламентації забезпечення інформаційної безпеки особистості полягає в тому, що об'єкти інформаційної безпеки розподілено за такими чотирма категоріями, як окрема особа, військовослужбовці та працівники сектора безпеки й оборони, суспільство, міжнародна спільнота. Одна конкретна особа може одночасно перебувати в різних категоріях. Це вимагає визначення завдань забезпечення інформаційної безпеки всім органам державної влади та місцевого самоврядування, а також іншим державним установам.

Висновки і пропозиції. Отже, підсистема інформаційної безпеки є одним із важливих складників національної безпеки України. Недостатній стан її дослідження зумовлює низьку прогалин у нормативно-правовому забезпеченні органів державної влади та місцевого самоврядування. Одним із напрямів підвищення рівня інформаційної безпеки українського суспільства може бути внесення змін до Закону «Про національну безпеку України» щодо деталізації документів стратегічного планування з питань забезпечення інформаційної безпеки.

Напрямом подальших досліджень може бути визначення та регламентація порядку розроблення стратегії інформаційної безпеки, порядку незалежного оцінювання результатів її виконання та опрацювання відповідного огляду.

Список використаної літератури:

1. Панченко О.А., Банчук Н.В. Информационная безопасность личности. Киев. КИТ. 2011. 672 с.
2. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: http://zakon0.rada.gov.ua/laws/show/2469-19
3. Государственное управление в сфере национальной безопасности: словарь-справочник / состав.: Г.П. Сытник, В.И. Абрамов, В.Ф. Смолянюк и др.; Под общ. ред. Г.П. Сытника. Киев. НАДУ. 2012. 496 с.
4. Забезпечення інформаційної безпеки держави [підручник] / Петрик В.М., При-

сяжнюк М.М., Мельник Д.С. та ін.; За заг. ред. О.А. Семенченка та В.М. Петрика. Київ. ДНУ «Книжкова палата України». 2015. 672 с.
5. Липпман Уолтер Общественное мнение; Пер. с англ. Т.В. Барчуновой. Москва. Ин-т фонда «Общественное мнение». 2004. 384 с.
6. Бедрицкий А.В. Информационная война: концепции и их реализация в США; Под ред. Е.М. Кожокина. Москва. РИСИ. 2008. 187 с.
7. Воєнна політика, безпека та стратегічне планування, інформаційна безпека держави у воєнній сфері. Терміни та визначення: Військовий стандарт України ВСТ 01.004.004. Київ. НУОУ. 2015. 24 с.
8. Чуваков О.А. Злочини проти основ національної безпеки України: проблеми кримінально – правової теорії і практики [монографія]; відп. ред. О.М. Костенко. Одеса. Фенікс. 2017. 362 с.
9. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017
10. Питання діяльності Міністерства інформаційної політики України: Постанова Кабінету Міністрів України від 14.01.2015 № 2. URL: https://zakon.rada.gov.ua/laws/show/2-2015-%D0%BF
11. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР зі змінами. URL: http://zakon2.rada.gov.ua/laws/show/254к/96-вр
12. Системи управління якістю. Основні положення та словник термінів: ДСТУ ISO 9000:2015 (ISO 9000:2015, IDT). Київ. ДП «УкрНДЦ». 2016. 45 с.

Кукин И. В. Современные проблемы обеспечения информационной безопасности в системе национальной безопасности Украины

В статье исследуются отдельные вопросы законодательного урегулирования в сфере национальной безопасности, в частности отмечено недостатки в Законе «О национальной безопасности Украины», касающиеся обеспечения информационной безопасности. С учетом законодательства Украины и рекомендаций стандартов управления качеством деятельности ISO серии 9000 предложено и обосновано порядок разработки документов стратегического планирования по вопросам обеспечения информационной безопасности.

Ключевые слова: *информационная безопасность, информационная война, стратегия информационной безопасности, национальная безопасность, информационная политика, стратегическое планирование, объекты информационной безопасности, субъекты информационной безопасности.*

Kukin I. Current problems of providing information security in the national security system of Ukraine

The article deals with separate issues of legislative regulation in the field of national security. In particular, it noted deficiency in the Law «On National Security of Ukraine» regarding the provision of information security. Taking into account the legislation of Ukraine and the recommendations of ISO 900000 quality management standards, the procedure for elaboration of strategic planning documents on information security issues is proposed and substantiated.

Key words: *information security, information warfare, information security strategy, national security, information policy, strategic planning, information security objects, subjects of information security.*