1 Нормативно-правові, методологічні та практичні аспекти захисту інформації в інформаційних і телекомунікаційних системах

УДК 681.3.06

СИСТЕМНИЙ АНАЛІЗ ПЕРЕХОДУ ВІД КОНЦЕПЦІЇ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ДО ДОКТРИНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Іван Горбенко, Олександр Потій, Сергій Черних*, Михайло Прокофьєв**

*Харківський Національний університет радіоелектроніки, *Служба безпеки України, **НТУУ «КПІ»*

Анотація: **Розглядаються питання створення Доктрини інформаційної безпеки України. Здійснюється аналіз Концепції національної інформаційної політики України та обґрунтована необхідність розробки Доктрини. Обґрунтовані та сформульовані основоположні принципи формування Доктрини. Надається генезис Доктрини, визначаються основні її елементи та структурні компоненти. Вводиться поняття інформаційно-політичної моделі держави, розкривається системний характер Доктрини. Пропонується загальний підхід до розробки форми та змісту Доктрини інформаційної безпеки держави.**

Summary: **The article considers questions concerning creation of the Doctrine of Ukraine information safety. Analysis of Ukraine national information policy conception is carried out and necessity of Doctrine development is proved. The basic principles of Doctrine forming are proved. Doctrine genesis is shown and its basic elements and structural components are determined. The notion of information-political state model is introduced and systematic character of Doctrine is shown. General approach to form development and Doctrine matter of information state safety is offered.**

Ключові слова: **Національна безпека, доктрина інформаційної безпеки, інформаційно-політична модель держави, система інформаційної безпеки держави.**

Вступ

07. 09. 2002 року опубліковано проект Концепції національної інформаційної політики України (далі Концепція) [1], розроблений Державним комітетом інформаційної політики, телебачення і радіомовлення. Розробка проекту здійснювалася відповідно до Указу Президента України від 06. 12. 2001 року № 1193 “Про рішення Ради національної безпеки і оборони України від 31. 10. 2001 року “Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України”.

Концепція визначає правові, економічні та організаційні основи національної інформаційної політики України і спрямована на досягнення наступних основних цілей:

- створення умов для побудови в Україні розвинутого інформаційного суспільства як органічного сегмента глобального інформаційного співтовариства;
- забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури;
- впровадження новітніх інформаційних технологій;
- захист національних моральних і культурних цінностей;
- забезпечення конституційних прав на свободу слова та вільний доступ до інформації.

У Концепції вказується (ст. 3), що інформаційна політика держави є складовою частиною соціально-економічної політики і спрямована на формування стратегії розвитку і використання національних інформаційних ресурсів.

Таким чином, розробка і прийняття даної Концепції фактично закріплює як державну політику рух України до інформаційного суспільства. На наш погляд, саме прийняття документа такого характеру вже є позитивною тенденцією, оскільки, як вказується в Окінавській хартії глобального інформаційного суспільства «інформаційне суспільство дозволяє людям ширше використовувати свій потенціал і реалізувати свої прагнення» [2]. У Концепції ставиться задача впровадження в Україні новітніх інформаційних технологій (ІТ), що сьогодні «є одним з найбільш важливих факторів, що впливають на формування суспільства XXI століття. ІТ стають життєво важливим стимулом розвитку світової економіки. ІТ повинні служити досягненню взаємодоповнюючих цілей, стійкого економічного росту, підвищенню суспільного добробуту, стимулюванню соціальної згоди і повної реалізації їхнього потенціалу в області зміцнення

демократії, транспарентного і відповідального керування, міжнародного миру і стабільності. Досягнення цих цілей і рішення проблем, що виникають, вимагають розробки ефективних національних і міжнародних стратегій» [2]. Розробка Концепції саме і спрямована на рішення останньої задачі.

У запропонованій роботі розглядаються питання, охоплювані Концепцією, котра може бути охарактеризована як документ, що містить та обґрунтовує першочергові заходи в інформаційній сфері, які необхідно запровадити державі. У роботі здійснено аналіз двох розділів Концепції, що розглядають проблеми впровадження новітніх інформаційних технологій і інформаційної безпеки, аналізується творча можливість даної Концепції в галузі забезпечення інформаційної безпеки. Проте об'єктивні умови не дозволяють Концепції виступити в ролі основного документа формування системи інформаційної безпеки України.

Головною метою даної роботи є розробка методологічних основ формування Доктрини. Для цього вирішуються такі задачі:

- обґрунтування необхідності розробки і прийняття в Україні Доктрини інформаційної безпеки (далі Доктрина);
- визначення з позиції системного підходу її сутності, ролі та місця в нормативно-правовому полі держави;
- формулювання принципів та концептуальних поглядів на формування Доктрини;
- розробка пропозицій щодо цілей, задач і структури Доктрини.

Аналіз Концепції є для нас відправною точкою у вирішенні цих завдань та досягненні головної мети.

І Аналіз положень Концепції Національної інформаційної політики щодо проблем сучасних інформаційних технологій і інформаційної безпеки

Матеріально-технологічною основою ефективного використання інформаційних ресурсів, як нового, могутнього фактора соціально-економічного розвитку держави і суспільства, є інформаційна технологія (ІТ). ***Інформаційна технологія*** *– цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розподілення даних, доступ до джерел інформації незалежно від місця їхнього розміщення* [14]. Задачам з впровадження новітніх інформаційних технологій в Україні присвячено третій розділ Концепції. У ст. 6 формулюються зокрема такі задачі:

– захист національних інтересів України в умовах глобалізації інформаційних процесів, входження у світовий інформаційний простір і глобальні інформаційні мережі;

– інтеграція телерадіоінформаційної структури України в телерадіоінформаційний простір країн - членів ЄС і світовий телерадіоінформаційний простір;

– приєднання національної інфраструктури зв'язку України до Європейської інформаційної інфраструктури і глобальної інформаційної інфраструктури.

Серед основних вимог до національної інформаційної інфраструктури, з погляду нормативно-правового забезпечення, можна виділити наступні вимоги (ст. 9):

– забезпечення відповідності національної інформаційної інфраструктури вимогам міжнародних стандартів ISO/IEC і рекомендаціям ITU з метою забезпечення реальної взаємодії та погодженості технічних засобів, інформаційних пристроїв і послуг з відповідними засобами, пристроями і послугами глобальної інформаційної інфраструктури;

– адаптація державної нормативно-технічної та правової бази до вимог міжнародного законодавства, при цьому пріоритетним є задоволення технічних і технологічних вимог Євросоюзу.

Виконання цих вимог державної політики вимагає перегляду існуючих підходів до розробки національних стандартів у галузі інформаційних технологій взагалі та ІТ-безпеки зокрема.

Іншою важливою складовою державної політики у галузі сучасних ІТ є політика щодо використання комп'ютерних технологій та систем телекомунікації, що спрямована на:

– розвиток науково-технічної, технологічної і виробничої бази вітчизняної інформаційної індустрії;

– прискорення формування комп'ютерної технологічної інфраструктури національних інформаційних ресурсів;

– створення інтегрованого телекомунікаційного середовища держави й організація виробництва вітчизняних засобів системи забезпечення інформаційної безпеки особистості, держави і суспільства;

– забезпечення необхідного рівня фінансування наукових досліджень в області телекомунікаційних технологій.

Даний перелік напрямків можна доповнити ще одним, а саме побудова ефективної системи освіти широких верств населення, підготовки та перепідготовки фахівців у галузі комп'ютерних і телекомунікаційних технологій.

Аналіз сформульованих у Концепції напрямків розвитку і вирішуваних задач дозволяє зробити висновок про визнання в Україні того факту, що інформаційна індустрія перетворилася в один із секторів національної економіки, який розвивається найбільш бурхливо, а інформаційна сфера стає однією з найважливіших складових життєдіяльності нашого суспільства. Разом з тим, необхідно враховувати, що інтенсивний розвиток інформаційних технологій, цілеспрямований рух України до створення національної інформаційної інфраструктури та її інтеграція в європейську і загально світову глобальну інфраструктуру сприяє посиленню небезпеки несанкціонованого втручання у роботу інформаційних і телекомунікаційних систем України.

Проблемі інформаційної безпеки (ІБ) присвячено одинадцятий розділ Концепції. Основи державної політики у галузі державної безпеки визначено у перших двох статтях розділу (ст. ст. 38, 39). Тридцять дев'ята стаття практично формулює суть національних інтересів України в інформаційній сфері. Виділено чотири складові цих інтересів.

Перша складова національних інтересів (СНІ1). Дотримання конституційних прав і свобод людини та громадянина у галузі одержання інформації та користування нею, забезпечення духовного відновлення України, збереження і зміцнення моральних цінностей суспільства, традицій і гуманізму, культурного і наукового потенціалу держави.

Друга складова національних інтересів (СНІ2). Інформаційне забезпечення державної політики України.

Третя складова національних інтересів (СНІ3). Розвиток сучасних інформаційних технологій, вітчизняної інформаційної індустрії засобів інформатизації, телекомунікації і зв'язку, забезпечення потреб внутрішнього ринку продукцією і вихід цієї продукції на світовий ринок, забезпечення накопичення, збереження та ефективного використання вітчизняних ресурсів.

Четверта складова національних інтересів (СНІ4). Захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки інформаційних і телекомунікаційних систем на території України.

Особлива увага в Концепції приділяється першій складовій. Ст. 38 підсилює важливість проблеми забезпечення конституційних прав людини і громадянина на свободу інформаційної діяльності і державних гарантій на обмеження цієї діяльності з метою захисту прав та свобод інших осіб, а також інтересів держави.

Далі в Концепції сформульовані основні загрози інформаційній безпеці України (ст. 40). Перелік загроз, наведений у цьому документі, а по суті саме так можна охарактеризувати зміст сорокової статті, цілком достатній. Але, якщо аналізувати проблему інформаційної безпеки України окремо, формування простого переліку загроз недостатньо. Необхідно розробити науково-обґрунтовану класифікацію видів і джерел загроз. Така задача може бути вирішена тільки разом з визначенням змісту національних інтересів в інформаційній сфері, а також здійсненні комплексного аналізу стану інформаційної безпеки України на сучасному етапі й оцінці цього стану в найближчій перспективі. Види, зміст і джерела загроз мають формулюватися як мінімум за напрямками національних інтересів.

Інші статті розділу визначають напрямки протидії загрозам в області інформаційної безпеки. До цих напрямків відносяться:

- організаційні заходи (ст. 41);
- заходи щодо захисту прав і свобод людини і громадянина (ст. 42);
- задачі розвитку матеріально-технічної бази системи інформаційної безпеки особистості, держави і суспільства (ст. 43);
- науково-практична робота з забезпечення інформаційної безпеки (ст. 44);
- удосконалення нормативно-правової бази системи інформаційної безпеки (ст. 45).

Вивчення статей 41–44 Концепції, дозволяє зробити загальний висновок про те, що їхній зміст є переліком першочергових заходів і мір, які необхідно реалізувати в Україні вже сьогодні. Але їхня реалізація має здійснюватися планомірно, на єдиній системній основі. На жаль, Концепція не забезпечує такого підходу. Відзначимо, що в концепції навіть не формулюється поняття «система інформаційної безпеки держави», що є основним. Проте, більшість зі сформульованих задач дійсно відбивають сучасний стан проблем інформаційної безпеки України, орієнтованих на використання останніх науково-технічних досягнень у галузі інформаційної безпеки. Реалізації на практиці цих задач буде сприяти впровадження в Україні найсучасніших технологій забезпечення ІБ.

Так, забезпечення можливостей виявлення загроз порушення конфіденційності, цілісності і доступності (ст. 41) припускає створення і широке застосування систем керування ризиками на різних рівнях (держава, відомство, організація, окремі ІТ-системи). Такі задачі, як формування цілісної системи захисту мереж передачі даних, організація захисту інформації в системах електронного документообігу й електронного підпису, створення інформаційно-телекомунікаційної системи органів державної влади, організація

керування засобами криптографічного і технічного захисту (ст. 43) можуть бути вирішені шляхом формування в рамках Національної системи конфіденційного зв'язку Національної інфраструктури відкритих ключів (PKI) із широким застосуванням сучасних технологій відкритої криптографії.

В області науково-практичної діяльності задачі налагодження механізмів постійного моніторингу, прогнозування загроз інформаційній безпеці і вироблення рекомендацій з їхньої нейтралізації на практиці означають застосування технологій ефективного менеджменту безпеки, реалізації процедур аудиту безпеки, вимагають реальної інтеграції України в глобальні системи моніторингу уражень IT-систем (наприклад, програма CERT, участь у підтримці бази даних уражень ICAT).

Особливо варто виділити задачу створення системи української стандартизації в сфері інформаційної безпеки з урахуванням міжнародних стандартів інформаційного обміну і захисту інформації. На жаль, сьогодні ми далекі від реальної гармонізації з міжнародною і європейською системою стандартизації. На наш погляд неприпустимо подальше зволікання з рішенням питань про прийняття як національних таких стандартів як ISO/IEC 15408, ISO/IEC 13335, ISO/IEC 17799, ще недостатньо вивчені архітектурні стандарти безпеки, стандарти механізмів безпеки й інші нормативні документи.

Таким чином, аналіз основних положень Концепції національної інформаційної політики в області інформаційної безпеки дозволяє зробити наступні висновки:

1. Концепція визначає тільки суть національних інтересів України в інформаційній сфері.
2. На державному рівні закріплена необхідність рішення актуальних проблем в області управління (менеджменту) безпеки, управління ризиками, аудита систем безпеки, застосування останніх досягнень відкритої криптографії, гармонізації національної нормативної бази з міжнародною і європейською, а також інших задач на принципово новому рівні.
3. Концепція є переліком першочергових задач в області інформаційної безпеки, які вже сьогодні вимагають свого рішення.

II Методологічні основи формування Доктрини інформаційної безпеки України

2.1. Передумови формування Доктрини інформаційної безпеки

Чим же викликана посилена увага до проблем інформаційної безпеки? Чому після прийняття концептуальних документів в інформаційній сфері, більшість держав відразу ж переходять до розробки політики інформаційної безпеки держави? Можна привести досить багато причин. На наш погляд основними з них є:

– розвиток IT призвів до якісних та кількісних змін у змісті національних інтересів, національної і міжнародної безпеки, у методах її забезпечення; сьогодні важливою складовою національних інтересів України є активне формування «інформаційного суспільства» і входження національної інформаційної інфраструктури в глобальну інформаційну інфраструктуру;

– інформаційна сфера, що представляє собою специфічну сферу діяльності суб'єктів громадського життя, пов'язану зі створенням, збереженням, поширенням, передачею, обробкою і використанням інформації, стала однією з найважливіших складових сучасного суспільства. Інтенсивний розвиток інформаційної інфраструктури, процеси глобалізації, що особливо яскраво виявляються в інформаційній сфері, інформатизація практично всіх сторін громадського життя, діяльності органів державної влади і управління істотно підсилили залежність ефективності функціонування суспільства і держави від стану інформаційної сфери;

– інформаційна інфраструктура й інформаційні ресурси стають ареною міждержавної боротьби за світове лідерство; тому цілеспрямований рух України до створення інформаційної інфраструктури й інтеграції її в європейську і світову інфраструктури приводить до посилення небезпеки несанкціонованого втручання в роботу інформаційних і телекомунікаційних систем держави;

– демонополізація послуг зв'язку, створення ринку послуг і засобів зв'язку привели до появи на території України мереж і систем зв'язку, що належать акціонерним товариствам і приватним особам. Існує деяка економічна залежність операторів зв'язку від іноземних інвесторів. Різноманітність існуючих мереж і служб зв'язку ставить проблему координації зусиль щодо створення і розвитку мереж зв'язку з урахуванням потреби зміцнення обороноздатності держави і забезпечення їхньої інформаційної безпеки;

– індустрія інформатизації, телекомунікації і зв'язку, інформаційних послуг на сучасному етапі соціально-економічного розвитку є однією з сфер економіки, що найбільш динамічно розвивається, здатною конкурувати за прибутковістю з паливно-енергетичним комплексом, автомобіле- і авіабудуванням, іншими галузями виробництва. Більш того, інформаційна індустрія стала визначати наукоємність продукції, її конкурентноздатність на світовому ринку.

Усе це говорить про те, що забезпечення національних інтересів України в інформаційній сфері стає

важливим фактором національної безпеки.

Не можна сказати, що існуюча нормативно-правова база і, зокрема, розглянута вище Концепція не визначають державну політику в ряді напрямків інформаційної безпеки. Політичне керівництво держави, керівники багатьох міністерств і відомств, і в першу чергу Служби безпеки України і Департаменту спеціальних телекомунікаційних систем і захисту інформації, приділяють велику увагу повній реалізації задачі по забезпеченню інформаційної безпеки України. Але така робота сьогодні має проводитися більш цілеспрямовано, заходи повинні бути об'єднані єдиним задумом. Політика інформаційної безпеки України буде більш зваженою і відповідати реальним умовам, якщо основні її напрямки будуть розглянуті й обґрунтовані з єдиних системних позицій. Таким чином, сьогодні склалися об'єктивні передумови розробки нового документа в області інформаційної безпеки – Доктрини інформаційної безпеки України (далі – Доктрина). Цей документ має бути комплексним і основним системоутворюючим фактором у процесах становлення системи інформаційної безпеки України.

2.2. Основоположні принципи формування і розробки Доктрини інформаційної безпеки України

З урахуванням визначень, приведених у [3, 4], визначимо, що *Доктрина інформаційної безпеки – це сукупність основних офіційних поглядів на мету, задачі, принципи й основні напрямки забезпечення інформаційної безпеки держави*. З позицій системного підходу Доктрина має розглядатися як складний об'єкт (система) політичного і нормативно-правового характеру. На наш погляд основними принципами формування Доктрини інформаційної безпеки України можуть бути таки принципи.

Принципи ієрархічної залежності, конституційності, спадковості та несуперечності формування.

Сутність принципу ієрархічної залежності полягає в тому, що Доктрина, як системний об'єкт, знаходиться в загальній ієрархічній структурі нормативного поля нашої держави.

Суть принципу конституційності полягає в тому, що положення Доктрини та її основні елементи формуються на основі Конституції і Концепції національної безпеки України, а також з урахуванням норм діючого законодавства.

Суть принципу спадковості полягає в тому, що реалізація положень Доктрини спрямована на забезпечення послідовного впровадження загальної державної політики зверху вниз без перекручувань.

Суть принципу несуперечності полягає в тому, що формування положень Доктрини має здійснюватися за умови забезпечення несуперечності положень державної політики в області інформаційної безпеки положенням державної політики забезпечення національної безпеки в цілому.

Для ілюстрації генезису Доктрини, розглянемо наступну ієрархічну схему:

конституція → концепція національної безпеки → стратегія національної безпеки → Доктрина інформаційної безпеки → створення системи інформаційної безпеки держави.

Правову основу Доктрини повинні складати Конституція України, Концепція Національної безпеки України [1], а також діюче законодавство, що регулює відносини в області забезпечення безпеки України і захисту інформації. Доктрина є розвитком Концепції національної безпеки України стосовно інформаційної сфери. Як нормативний документ Стратегія національної безпеки в Україні відсутня. Хоча останнім часом фахівці вважають дуже актуальною задачею розробку такого документа. Стратегія національної безпеки є основним програмним документом виконавчої гілки влади держави, що дає орієнтири на визначений відрізок часу, окреслюючи загальні контури програми імплементації пріоритетних національних інтересів держави [4].

Основними складовими елементами Концепції та Стратегії національної безпеки є [1, 4]: ***національна безпека, національні інтереси***, ***національні цілі***, ***пріоритети і принципи задоволення і захисту національних інтересів***, ***загрози національній безпеці і система національної безпеки***.

Наріжними поняттями у наведеному переліку є поняття «національна безпека» і «система національної безпеки». Зараз у Верховній Раді знаходиться на розгляді нова редакція Концепції національної безпеки. Як з'ясувалося, вітчизняні фахівці не дають однозначного тлумачення сутності цих базових елементів в умовах нової соціально-політичної обстановки, яка змінилася не тільки в Україні, а і в усьому світі. Найбільш вдалими, на наш погляд, є визначення, що наводяться в [5].

Система національної безпеки *– це сукупність державних структур і недержавних організацій, що функціонують у сфері захисту прав і свобод людини, базисних цінностей від зовнішніх і внутрішніх загроз, а також відповідна підсистема законодавчих актів держави і нормативних документів недержавних організацій.*

Національна безпека – *це ступінь захищеності життєво важливих інтересів, базових цінностей, прав і свобод особи суспільства і держави від зовнішніх і внутрішніх загроз* (дане визначення трохи переформульоване авторами, але по суті не відрізняється від визначення, даного в [5]).

Головними об'єктами національної безпеки виступають громадянин та його права і свободи, суспільство та його духовні і матеріальні цінності, держава та її конституційний лад, суверенітет, територіальна цілісність і недоторканність кордонів [1].

Відповідно до принципу ієрархічної залежності, спадковості і конституційності розробки Доктрини, основними її елементами можуть бути:

– *поняття і зміст інформаційної безпеки України;*
– *національні інтереси України в інформаційній сфері;*
– *загрози національним інтересам в інформаційній сфері;*
– *загальні принципи забезпечення інформаційної безпеки держави (загальні принципи державної політики в області інформаційної безпеки);*
– *поняття і зміст системи інформаційної безпеки.*

Принцип історичності і змінності Доктрини. Якщо зосередитись на питаннях оцінки стану інформаційної безпеки держави, можливості держави виявляти і протистояти загрозам національним інтересам в інформаційній сфері, то ми маємо погодитися з тим, що Доктрина не може бути документом, не змінним у часі. *Доктрина інформаційної безпеки розробляється у конкретний історичний момент, для конкретних умов, що склалися у даний момент, з урахуванням розвитку обстановки на визначеному відрізку часу*. Даний принцип не суперечить загальному положенню справ у розробці основних і концептуальних державних документів. Так, повертаючись до ієрархічної схеми, Стратегія національної безпеки є більш змінним документом, чим Концепція національної безпеки і тим більше, ніж Конституція. Таким чином, Доктрина інформаційної безпеки, як і Стратегія національної безпеки, виступає в ролі програмного документа і повинна розглядатися як «видатковий матеріал». При зміні ситуації розробляється нова Стратегія національної безпеки і, як наслідок, це приведе до необхідності розробки нової Доктрини інформаційної безпеки.

Принцип комплексності розробки Доктрини. Чи повинна Доктрина інформаційної безпеки, як сукупність поглядів, бути єдиним документом? З погляду застосування і реалізації Доктрини вона повинна мати дві важливі властивості – повноту і гнучкість, що знаходяться у певному протиріччі.

Для того, щоб Доктрина, як система поглядів, була повною, тобто відображала всі істотні сторони і проблеми інформаційної безпеки держави, а також гнучкою, тобто враховувала зміни, що несе час, вона повинна міститися у різних документах. Сам же документ за назвою Доктрина інформаційної безпеки буде виступати в ролі системоутворюючого фактора, а його концептуальні підходи до забезпечення інформаційної безпеки повинні знайти свій розвиток у підпорядкованих нормативних документах. При такому підході до формування державної політики інформаційної безпеки *розробка Доктрини та інших документів має здійснюватися планомірно і системно, на основі єдиної комплексної державної програми нормативно-правового забезпечення системи інформаційної безпеки держави*.

Принцип відкритості розробки Доктрини. Доктрина інформаційної безпеки держави не повинна бути закритою ні для фахівців, ні для широких верств населення. Відкритість розробки Доктрини, впровадження її основних положень в усі сфери громадського життя і державного управління забезпечать її високу соціальну і суспільну значимість, підвищать консолідуючу роль у створенні і побудові *не державної* системи інформаційної безпеки, а ***Національної*** системи інформаційної безпеки України. Даний принцип безпосередньо спрямований на реалізацію основного принципу забезпечення національної безпеки України – принципу балансу інтересів особистості, суспільства і держави. Реалізація принципу відкритості буде сприяти ствердженню в інформаційному суспільстві ***культури безпеки.*** Потрібно вказати, що принцип відкритості відповідає сьогоднішній політиці державної влади на відкритість і прозорість державного управління, а також відповідає вибору демократичного шляху розвитку України.

Принцип реалізованості (практичної значимості) Доктрини. Доктрина інформаційної безпеки за формою і змістом має дійсно стати керівним, програмним документом в галузі інформаційної безпеки. Важливим є те, що реалізація принципу спрямована на узгодження матеріально-технічних, наукових (інтелектуальних) та виробничих можливостей держави з практичними задачами, що виникають при створенні системи інформаційної безпеки держави. Необхідно, щоб положення Доктрини були завжди застосовні до розробки документів нижнього рівня в сфері інформаційної безпеки, а також до організації конкретної практичної діяльності в області інформаційної безпеки. З принципу реалізованості випливає наступний принцип – ***принцип єдності форми і змісту Доктрини***.

Принцип цілеспрямованості. Головною метою Доктрини інформаційної безпеки є формування принципів і підходів до захисту національних інтересів України в інформаційній сфері. На практиці дана мета може бути досягнута за умови створення єдиної цілеспрямованої системи інформаційної безпеки держави. Доктрина є основою створення такої системи і має забезпечити можливість визначення функцій і основних елементів цієї системи, організаційних основ і оцінки ефективності функціонування системи.

Принцип моделюємості процесів забезпечення інформаційної безпеки держави. Розробка такого документа як Доктрина інформаційної безпеки має спиратися на комплексну оцінку стану інформаційної безпеки держави. Така оцінка здійснюється на основі визначення і кількісного аналізу найбільш важливих інтересів України в інформаційній сфері та загроз цим інтересам. Це, в свою чергу, дасть можливість розробити і реалізувати першочергові заходи щодо нейтралізації найбільш небезпечних загроз з урахуванням можливостей держави. Визначення пріоритетних інтересів України в інформаційній сфері є важливою і відповідальною самостійною задачею. Виконання комплексної оцінки інформаційної безпеки держави вимагає спеціального інструментарію, а адекватність і вірогідність отриманих результатів можуть бути доведені в рамках визначеної моделі.

Як основний інструментарій здійснення комплексної оцінки інформаційної безпеки держави автори пропонують використовувати *інформаційно-політичну модель (ІПМ) держави.* За аналогією з військово-політичної моделлю держави [6], уведемо поняття ІПМ: *під ІПМ держави будемо розуміти формалізований чи напівформалізований опис (відображення, представлення) процесу здійснення цілеспрямованої державної політики щодо забезпечення інформаційної безпеки держави.*

Розробка і використання ІПМ держави дозволить вирішити такі задачі, як:

– вивчення й оцінка захищеності життєво важливих інтересів особистості, суспільства і держави в інформаційній сфері в загальній системі національної безпеки;

– синтез раціональної структури, критеріїв і показників оцінки ефективності системи інформаційної безпеки держави;

– обґрунтування комплексу заходів для підвищення ефективності системи забезпечення інформаційної безпеки;

– обґрунтування необхідного рівня інформаційної безпеки держави, адекватного рівню існуючих і нових загроз безпеки;

– обґрунтування вимог, з урахуванням матеріально-технічних, інтелектуальних та виробничих можливостей, до елементів системи інформаційної безпеки держави в цілому, державних і недержавних структур, що функціонують в інтересах забезпечення інформаційної безпеки України, кількісних і якісних показників і характеристик системи інформаційної безпеки.

У цілому розробка і застосування ІПМ держави забезпечить комплексний підхід до проведення досліджень системи інформаційної безпеки держави в інтересах підвищення її ефективності. При цьому відкриваються більш широкі можливості щодо вивчення динаміки взаємодії політичних, економічних, інформаційних і інших факторів і процесів при вирішенні проблем інформаційної безпеки.

Принцип паралельної розробки Доктрини. Розробка Доктрини, як випливає з розглянутої ієрархічної схеми генезису Доктрини, пов'язана та спирається на раніше розроблену сукупність державних документів. Однак зараз Концепція національної безпеки тільки переглядається, Стратегія національної безпеки, як документ, взагалі відсутня, а на думку деяких фахівців [5], в Україні як така відсутня і система національної безпеки. Виходить, що сьогодні не можна приступити до розробки Доктрини інформаційної безпеки. Отже, не можна і приступити до створення системи інформаційної безпеки держави. Таким чином, у нинішніх умовах неможливо здійснити роботу відповідно до вище визначеної послідовної схеми, а чекати на це Україна не має часу. З іншої сторони потреба у такому документі як Доктрина сьогодні надзвичайно актуальна і елементи системи інформаційної безпеки вже створюються. Але, відкидаючи послідовність роботи в часі, ні в якому разі не можна відкидати послідовну (ієрархічну) залежність документів і заходів, що визначена ієрархічною схемою. Виходом з такої ситуації є використання при розробці державних нормативних документів причинно-наслідкового підходу. Це дасть можливість використовувати принцип паралельної розробки найважливіших державних документів при одночасній економії часу. Відповідно до цього принципу удосконалення Концепції національної безпеки, розробка Стратегії національної безпеки та Доктрини інформаційної безпеки, створення системи інформаційної безпеки можна і потрібно, з метою економії часу, здійснювати паралельно.

2.3. Місце Доктрини в національному, регіональному і міжнародному правовому полі

Розробка Доктрини має здійснюватися з урахуванням норм вітчизняного законодавства в інформаційній сфері, а також враховувати раціональні положення відповідних документів інших держав і міжнародних організацій. При цьому необхідно враховувати зовнішньо- і внутрішньополітичні фактори формування Доктрини інформаційної безпеки. На рис. 1 представлена узагальнена схема, що характеризує місце Доктрини в ієрархії національних, регіональних і міжнародних нормативно-правових документів у сфері інформаційної безпеки.

З огляду на те, що основний вектор сьогоднішньої зовнішньої політики України спрямований на інтеграцію в ЄС і вступ у Всесвітню організацію торгівлі [7, 8], при розробці Доктрини необхідно врахувати

положення і вимоги документів Євросоюзу в даній області. Певну роль у формуванні державної політики України можуть відігравати і такі міжнародні документи як Окінавська хартія глобального інформаційного суспільства, документи Організації економічного співробітництва і розвитку [8, 9] (Керівні принципи безпеки інформаційних систем, Принципи державної політики в області криптографії, Принципи регулювання і захисту приватності і передачі персональна даних, Декларація захисту персональних даних у глобальних мережах) і документи інших громадських організацій. Сьогодні для України актуальною стає задача гармонізації національної нормативної бази з нормативною базою Євросоюзу.

Нормативні документи, що визначають політику держави в області інформаційної безпеки, існують в багатьох розвинутих країнах. При розробці Доктрини має бути враховано досвід інших країн, у першу чергу Російської Федерації, США і країн-членів ЄС. Така спрямованість обумовлена тим, що в зовнішній політиці ці держави розглядаються як стратегічні партнери України.

Таким чином, розглядаючи зовнішньополітичні фактори формування Доктрини інформаційної безпеки, слід наголосити на тому, що вона має розроблятися в тісному узгодженні з міжнародними документами і нормативною базою Євросоюзу, а також з урахуванням досвіду розробки подібного роду документів інших країн, зокрема США і Росії.

З іншого боку на мету, задачі, форму і зміст Доктрини буде впливати вітчизняна нормативна база і в першу чергу чинне законодавство України в інформаційній сфері. Це Закони України «Про державну таємницю», «Про захист інформації в АС», «Про інформацію», «Про зв'язок», «Про Національну систему конфіденційного зв'язку». Також необхідно врахувати і тенденції розвитку національній нормативної бази в даній сфері, а саме розгляд законодавчою владою таких нових законів України як закони «Про електронний цифровий підпис», «Про електронний документообіг», «Про електронну комерцію» і ін.

Доктрина є концептуальним документом, тому вона не може не враховувати положень концепцій і національних програм розвитку галузей національної економіки, сучасний стан економіки держави. У першу чергу тут необхідно звернути увагу на положення Концепції і програми інформатизації України, Концепції розвитку зв'язку, Концепції освіти, Концепції національної інформаційної політики, а також Національних програм «Електронна Україна» і «Електронний уряд».

Аналіз і врахування положень розглянутих документів дозволить максимально точно визначити напрямки й особливості забезпечення інформаційної безпеки в різних сферах життєдіяльності держави, уточнити зміст національних інтересів України в інформаційній сфері.

Взаємодія Доктрини й інших документів носить багатозначний і двосторонній характер. Якщо Конституція і Концепція національної безпеки України практично впливають на форму і зміст Доктрини, то щодо інших документів взаємодія полягає або в необхідності гармонізації положень, наприклад, з нормативними актами Євросоюзу, міжнародними документами, або в необхідності врахування положень і досвіду розробки аналогічних документів інших країн. Так, на наш погляд, Доктрина інформаційної безпеки Російської Федерації [3, 11, 12, 13] може бути використана українськими розробниками, як приклад єдності форми і змісту, приклад реалізації системного підходу під час розробки нормативного документа.

Можна спостерігати сильний взаємний вплив Доктрини і нормативно-правових актів України на вітчизняну нормативну базу. З одного боку при розробці Доктрини чинне законодавство буде впливати на форму і зміст документу. З іншого боку, реалізація положень Доктрини приведе не тільки до змін у діючих нормативно-правових актах, але і до розробки нових документів. У цьому виявляється принцип еволюційного розвитку законодавчої бази України.

Системний характер Доктрини виявляється не тільки в тому, що Доктрина є продовженням державної політики національної безпеки. По суті система інформаційної безпеки є підсистемою системи національної безпеки. Системність виявляється також і в тому, що сама Доктрина є основним чинником подальшого розвитку нормативно-правової, наукової і матеріально-технічної бази системи інформаційної безпеки.

Якщо зосередитися на творчому аспекті Доктрини, практичній реалізації її положень, то вона повинна слугувати основою розробки і реалізації як мінімум наступних концепцій і програм.

1. *Концепція і програма нормативно-правового забезпечення системи інформаційної безпеки України.* Ці документи мають закласти основи довгострокової системної, цілеспрямованої і планомірної роботи з реформування й удосконалення національного законодавства у галузі інформаційної безпеки, розробки і впровадження механізмів реалізації правових норм, що регулюють відносини в інформаційній сфері, удосконалення системи ліцензування діяльності у галузі захисту інформації.

2. *Концепція і програма стандартизації у галузі інформаційної безпеки*, спрямовані на удосконалення процесів стандартизації, створення умов для розробки національних стандартів в галузі інформаційних

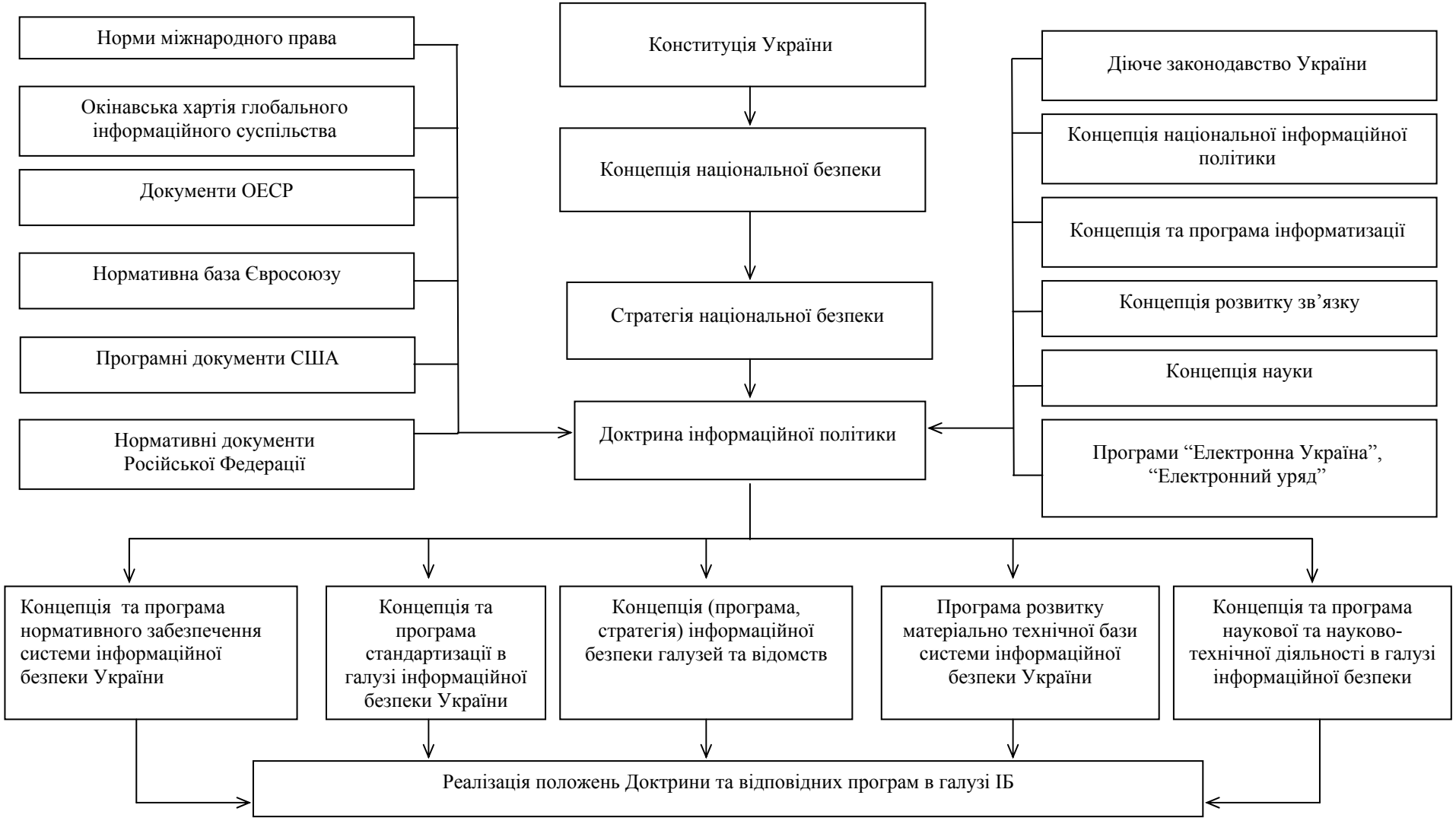
Норми міжнародного права
Окінавська хартія глобального інформаційного суспільства
Документи ОЕСР
Нормативна база Євросоюзу
Програмні документи США
Нормативні документи Російської Федерації
Конституція України
Концепція національної безпеки
Стратегія національної безпеки
Доктрина інформаційної політики
Діюче законодавство України
Концепція національної інформаційної політики
Концепція та програма інформатизації
Концепція розвитку зв'язку
Концепція науки
Програми "Електронна Україна", "Електронний уряд"
Концепція та програма нормативного забезпечення системи інформаційної безпеки України
Концепція та програма стандартизації в галузі інформаційної безпеки України
Концепція (програма, стратегія) інформаційної безпеки галузей та відомств
Програма розвитку матеріально технічної бази системи інформаційної безпеки України
Концепція та програма наукової та науково-технічної діяльності в галузі інформаційної безпеки
Реалізація положень Доктрини та відповідних програм в галузі ІБ

Рисунок 1

технологій і захисту інформації в АСУ, в інформаційно-телекомунікаційних системах загального і спеціального призначення, забезпечення реальної гармонізації національних стандартів з Європейськими та міжнародними стандартами, становлення та удосконалення нормативно-методичної і матеріально-технічної бази системи сертифікації засобів захисту інформації та атестації ІТ-систем різного призначення.

3. *Програма розвитку матеріально-технічної бази системи інформаційної безпеки України, систем криптографічного і технічного захисту інформації*. Основою метою даної програми є стимулювання вітчизняного виробництва засобів захисту інформації різного призначення, визначення державної політики впровадження якісних засобів захисту інформації в ІТ-системи, приналежних як державному, так і недержавному секторам економіки.

4. *Концепція і програма розвитку наукової і науково-технічної діяльності в області інформаційної безпеки, програма освіти у галузі ІБ*. Ці програми спрямовані на підтримку пріоритетних фундаментальних і прикладних наукових досліджень у галузі інформаційної безпеки, криптографічного, технічного і голографічного захисту інформації, підвищення соціального статусу і захищеності науковців, збереження і збільшення наукового потенціалу держави в даній області, підготовку висококваліфікованих кадрів.

Доктрина інформаційної безпеки держави має стати основою для розробки концепцій, програм, стратегій, політик і інших нормативних документів забезпечення інформаційної безпеки міністерств і відомств, Отже, можна з повною впевненістю сказати, що Доктрина інформаційної безпеки має бути і буде по своїй суті системним документом. Вона виступає основним системоутворюючим фактором для створення системи інформаційної безпеки України і є органічним продовженням і розвитком Концепції національної безпеки. Доктрина є основою для формування зваженої і цілеспрямованої державної політики у галузі забезпечення інформаційної безпеки, підготовки пропозицій з удосконалювання правового, методичного, науково-технічного й організаційного забезпечення системи інформаційної безпеки України, розробки концепцій, стратегій і цільових програм забезпечення інформаційної безпеки.

III Загальний підхід до розробки форми і змісту Доктрини інформаційної безпеки

З урахуванням наведеного вище здійснимо аналіз взаємодії основних елементів та розробимо загальний підхід до визначення форми і змісту Доктрини інформаційної безпеки України. До основних елементів Доктрини, як уже визначено вище, відносяться *поняття і зміст інформаційної безпеки України, національні інтереси України в інформаційній сфері, загрози національним інтересам в інформаційній сфері, загальні принципи забезпечення інформаційної безпеки держави (загальні принципи державної політики в області інформаційної безпеки), поняття і зміст системи інформаційної безпеки.*

При визначенні загального підходу до розробки Доктрини, як системи поглядів, будемо виходити із сутності взаємодії таких фундаментальних категорій теорії систем і системного аналізу як *ціль*, *функція* і *структура*. При такому підході загальний процес розробки Доктрини буде полягати у формуванні ***цілей і задач інформаційної безпеки держави***, визначенні основних ***функцій держави із забезпечення інформаційної безпеки*** та обґрунтуванні ***структури і організаційних основ системи інформаційної безпеки держави.***

На рис. 2 представлена схема, що ілюструє взаємодію основних елементів Доктрини та можливий порядок її розробки. Вихідними передумовами є принципова частина, зміст національних інтересів в інформаційній сфері, види і джерела загроз інформаційної безпеки, особливості забезпечення інформаційної безпеки в різних сферах життєдіяльності держави і громадського життя. На базі аналізу цих даних, із застосуванням ІПМ держави здійснюється комплексна оцінка стану інформаційної безпеки держави, робляться висновки про ступінь (рівень) захищеності національних інтересів у конкретний момент часу, виробляється перспективна (прогнозна) оцінка інформаційної безпеки держави. Це дозволить сформулювати і визначити суть інформаційної безпеки України в конкретний історичний момент розвитку країни.

Комплексна оцінка дозволить сформулювати або уточнити основні цілі і розкрити загальні задачі забезпечення інформаційної безпеки держави. Детальний аналіз цілей, їхня декомпозиція дозволить визначити основні положення державної політики в інформаційній сфері, функції держави із забезпечення інформаційної безпеки, а потім і функції системи інформаційної безпеки держави. На наш погляд, державна політика в інформаційній сфері взагалі та в галузі ІБ зокрема, має бути спрямована на рішення таких задач, як:

– пом'якшення протиріч між потребами суспільства в розширенні вільного обміну інформацією і необхідністю збереження окремих регламентованих обмежень на її поширення;

– підтримка необхідного балансу інтересів особистості, суспільства і держави в інформаційній сфері, формування на території України конкурентноздатних українських інформаційних агентств і ЗМІ;

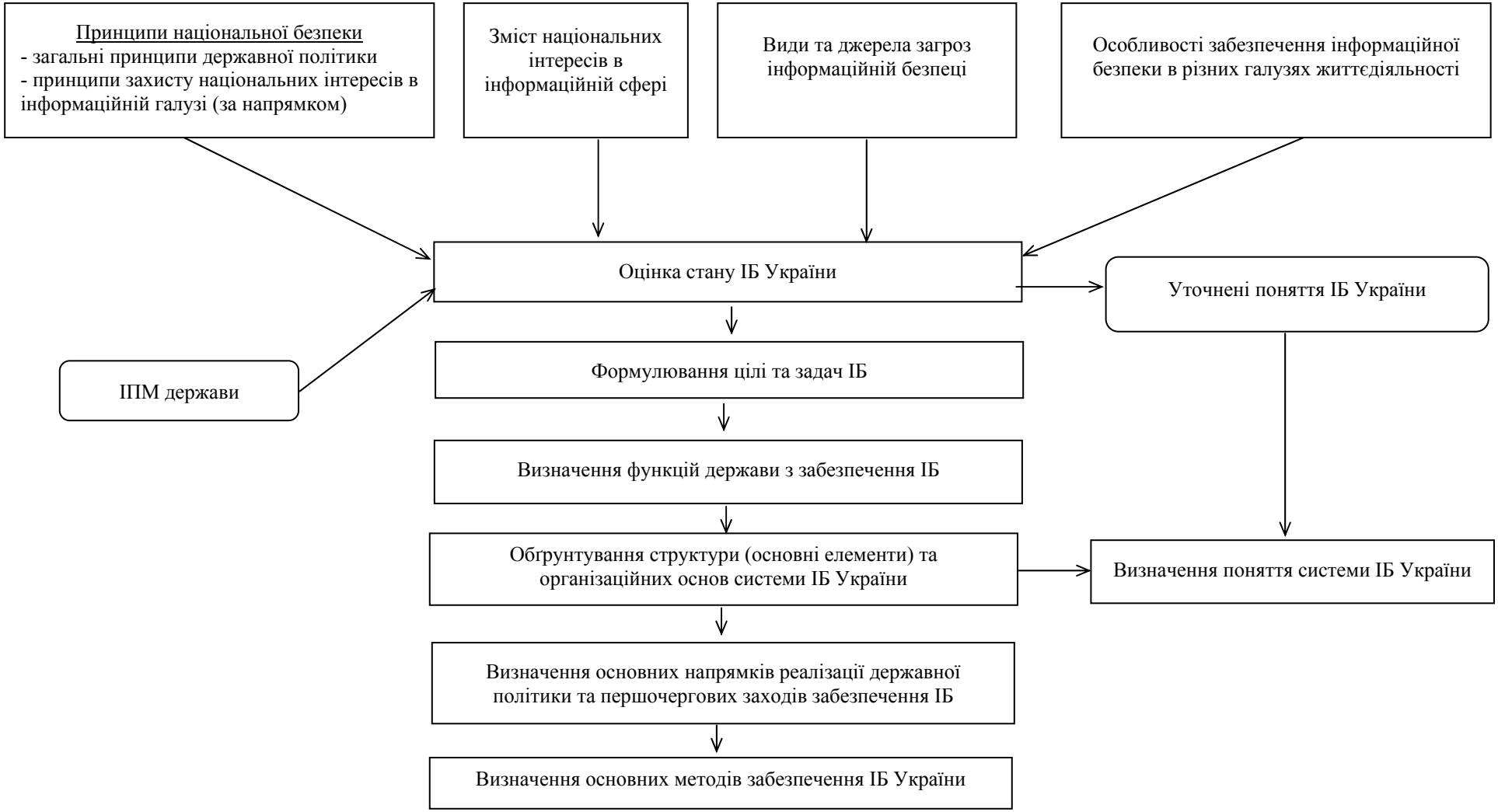
Принципи національної безпеки
- загальні принципи державної політики
- принципи захисту національних інтересів в інформаційній галузі (за напрямком)
Зміст національних інтересів в інформаційній сфері
Види та джерела загроз інформаційній безпеці
Особливості забезпечення інформаційної безпеки в різних галузях життєдіяльності
Оцінка стану ІБ України
Уточнені поняття ІБ України
ІПМ держави
Формулювання цілі та задач ІБ
Визначення функцій держави з забезпечення ІБ
Обґрунтування структури (основні елементи) та організаційних основ системи ІБ України
Визначення поняття системи ІБ України
Визначення основних напрямків реалізації державної політики та першочергових заходів забезпечення ІБ
Визначення основних методів забезпечення ІБ України

Рисунок 2

– зменшення факторів дестабілізації соціально-економічної обстановки в суспільстві шляхом поліпшення забезпеченості прав громадян на доступ до інформації і недопущення маніпулювання інформацією;

– забезпечення реального захисту даних про фізичних осіб (персональних даних), прав громадян на недоторканність приватного життя, особистої та сімейної таємниці;

– виключення витиснення українських інформагентств і ЗМІ з внутрішнього ринку шляхом чіткого проведення державної політики в області формування національного інформаційного простору;

– удосконалювання системи забезпечення охорони державної таємниці;

– створення вітчизняного кадрового потенціалу наукових і виробничих колективів, що працюють у галузі створення засобів інформатизації, телекомунікацій, зв'язку і захисту інформації;

– зниження імовірності несанкціонованого доступу до національних інформаційних ресурсів та залежності України від іноземних виробників обчислювальної і телекомунікаційної техніки, а також програмного забезпечення і ін.

Основними функціями держави є формування організаційної структури системи інформаційної безпеки, державних органів забезпечення національних інтересів в інформаційній сфері, обґрунтування функцій цих організацій і вимог до ефективності їхньої діяльності. Значну роль у забезпеченні інформаційної безпеки держави мають відігравати аналітичні, прогностичні і контролюючі функції держави.

Основними функціями системи інформаційної безпеки, наприклад, можуть бути:

– прогнозування, виявлення та оцінка рівня потенційних загроз інформаційної безпеки, оцінка наслідків їхньої реалізації;

– аналіз дестабілізуючих факторів в інформаційній сфері, причин їхньої появи і загострення;

– запобігання і ліквідація наслідків реалізації виявлених загроз і дестабілізуючих факторів, зменшення їхнього впливу на процеси забезпечення національних інтересів в інформаційній сфері;

– забезпечення реального балансу інтересів і потреб особистості, суспільства і держави в обміні інформацією і необхідними обмеженнями на поширення інформації та інші функції.

Формулювання повної і несуперечливої множини (дерева) функцій дозволить обґрунтовано підійти до визначення сутності системи інформаційної безпеки і визначити структуру (основні елементи) і організаційні основи системи інформаційної безпеки, визначити базові характеристики і показники інформаційної безпеки держави. До таких характеристик пропонується віднести:

– ступінь інформатизації державного управління та галузей народного господарства;

– якість нормативно-правової бази, на основі якої приймаються рішення щодо забезпечення інформаційної безпеки;

– кількість державних, недержавних і суспільних структур та рівнів ієрархії системи ІБ;

– види і якість нормативних документів, що розробляються на різних рівнях ієрархії системи ІБ, ступінь (рівень, якість) реалізації положень цих документів;

– сукупність показників оцінки ефективності функціонування системи забезпечення ІБ держави.

Усе це дозволить визначити основні напрямки і першочергові заходи щодо реалізації державної політики в області інформаційної безпеки. Як першочергові заходи можуть розглядатися задачі, сформульовані в Концепції національної інформаційної політики. Крім того, отримані результати дозволять визначити й основні методи забезпечення ІБ держави.

На рис. 3 представлено порядок формування цілей і задач з забезпечення ІБ з розкриттям механізму формування національних інтересів в інформаційній сфері, а також обґрунтування класифікації видів і джерел загроз безпеки.

Сутність національних інтересів в інформаційній сфері визначається з урахуванням інтересів головних об'єктів національної безпеки (громадянина, суспільства і держави) і на основі національних інтересів України, що визначені в Конституції України і Концепції національної безпеки України. У запропонованому підході будемо спиратися на чотири складові національних інтересів, що визначені в Концепції національної інформаційної політики.

Для кожної з чотирьох складових, з використанням методів системного аналізу (наприклад, методів експертного опитування, методів багатомірного порівняльного аналізу складних систем і т. п.), формується перелік найбільш небезпечних загроз безпеки. Особливістю даного етапу є те, що аналіз загроз має здійснюватися для кожної складової окремо, оскільки, як видно із сутності цих складових, у загальному випадку загрози будуть мати різний фізичний зміст, відрізнятися за характером впливу на об'єкти безпеки і результатом реалізації. Системний аналіз загроз безпеки дозволить розробити науково обґрунтовану класифікацію видів і джерел загроз.

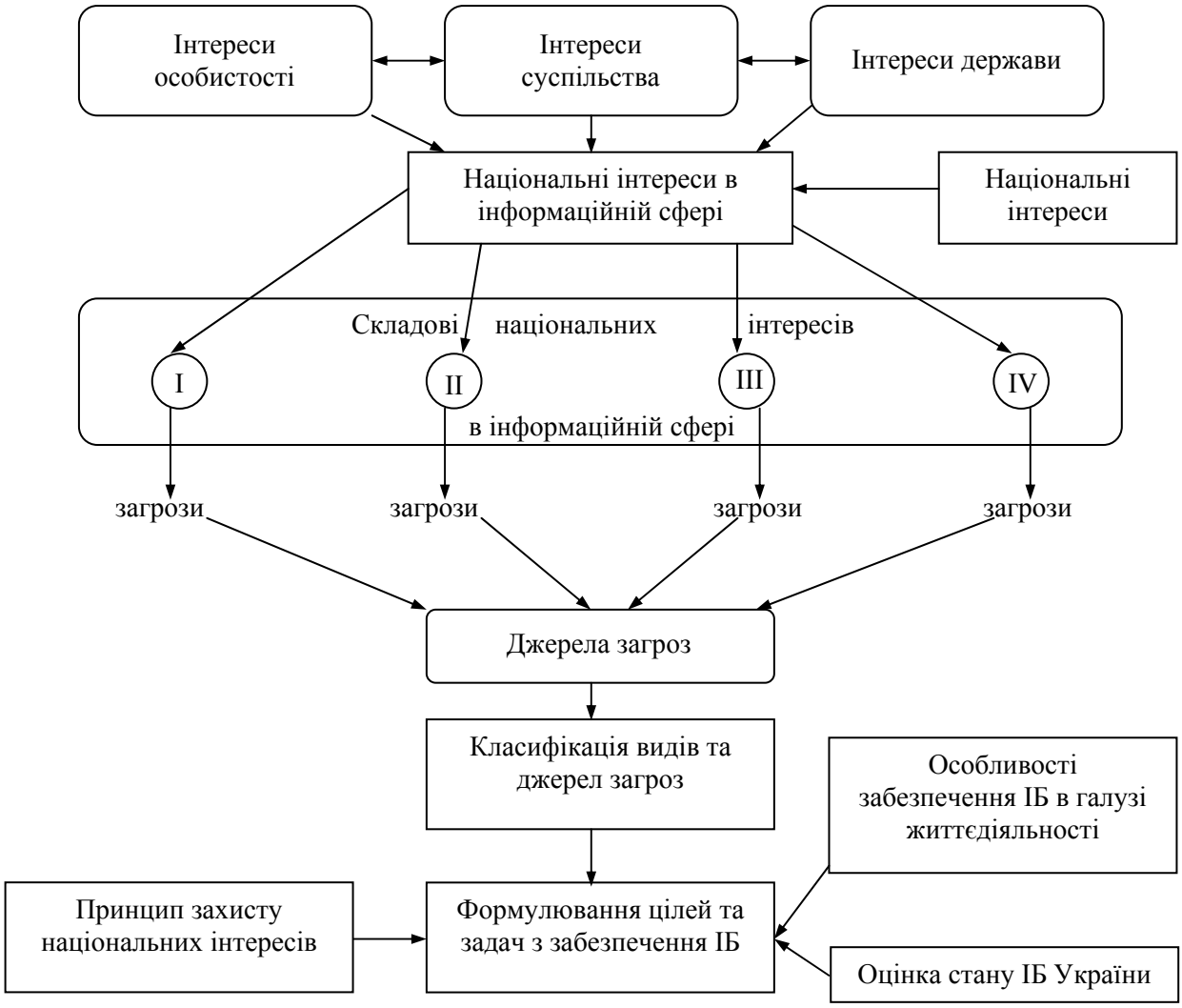

Рисунок 3

Відповідно до Концепції національної безпеки України основними сферами життєдіяльності держави, в яких можуть бути реалізовані загрози, є: політична (внутрішня і зовнішня політика держави), економічна, соціальна, військова, екологічна, науково-технічна та інформаційна.

Крім того, аналіз документів [1, 3, 7], дозволяє зробити висновок про доцільність розгляду особливостей забезпечення ІБ у сфері духовного життя суспільства, у правоохоронній і судовій сферах, у загальнодержавних інформаційних і телекомунікаційних системах, а також в умовах надзвичайних ситуацій.

Класифікація видів і джерел загроз, а також принципи захисту національних інтересів, особливості забезпечення ІБ в різних сферах життєдіяльності держави і громадського життя, результати комплексної оцінки стану інформаційної безпеки держави створять основу наукового обґрунтування і формулювання цілей і задач з забезпечення ІБ держави.

Таким чином, реалізація запропонованого підходу дозволить на єдиній системній основі визначити основні цілі, задачі, принципи і напрямки забезпечення ІБ України, сформувати загальні принципи державної політики забезпечення ІБ, обґрунтувати функції і структуру системи ІБ держави, забезпечити єдність форми і змісту Доктрини ІБ.

Висновки

У даній статті здійснено аналіз проекту Концепції національної інформаційної політики України, зокрема її розділів щодо впровадження новітніх інформаційних технологій та інформаційної безпеки. Основним висновком є те, що в Концепції вперше визначена сутність національних інтересів України в інформаційній

сфері. Однак Концепція не може виступати як системний документ у галузі ІБ і як основа побудови ефективної системи інформаційної безпеки держави.

У роботі проаналізовані причини підвищення уваги до забезпечення інформаційної безпеки в сучасному інформаційному суспільстві взагалі та в Україні зокрема, визначена й обґрунтована необхідність розробки нового національного нормативного документа системного характеру – Доктрини інформаційної безпеки.

Обґрунтовано та сформульовано основоположні принципи формування Доктрини ІБ України як сукупності основних офіційних поглядів на мету, задачі, принципи й основні напрямки забезпечення ІБ держави. Обґрунтовані таки принципи:

- ієрархічної залежності, спадковості, несуперечності та конституційності формування Доктрини ІБ**;**
- історичності та змінності Доктрини;
- комплексності розробки Доктрини;
- відкритості розробки Доктрини;
- реалізації (практичної значимості) Доктрини;
- єдності форми і змісту Доктрини;
- цілеспрямованості;
- моделюємості процесів забезпечення ІБ держави;
- паралельності розробки Доктрини.

В статті також розкрито генезис Доктрини ІБ, її зв'язок зі змістом і залежність від змісту основних державних документів – Конституції та Концепції національної безпеки України, визначено основні елементи Доктрини, до яких відносяться:

- поняття і зміст ІБ України;
- національні інтереси України в інформаційній сфері;
- загрози національним інтересам в інформаційній сфері;
- загальні принципи забезпечення ІБ держави (загальні принципи державної політики в області інформаційної безпеки);
- поняття і зміст системи ІБ.

Визначено такі властивості Доктрини як повнота і гнучкість та їхнє значення в забезпеченні комплексності формування Доктрини ІБ.

Введено поняття інформаційно-політичної моделі держави – формалізований чи напівформалізований опис (відображення, представлення) процесу здійснення цілеспрямованої державної політики щодо забезпечення ІБ держави. Розкрито ключову роль даної моделі в здійсненні комплексної оцінки стану ІБ держави, створення системи ІБ та основ оцінки ефективності функціонування цієї системи.

На основі аналізу місця Доктрини в національному та регіональному правовому полі розкрита сутність взаємного впливу і взаємодії Доктрини як нормативного документа з іншими документами у галузі ІБ. Показано, що взаємодія носить неоднозначний характер. Останнє визначається внутрішньо- і зовнішньополітичними факторами формування Доктрини ІБ.

Розкрито системний характер Доктрини. Вона є основою створення системи ІБ держави, яка, з одного боку, може бути охарактеризована як підсистема, що функціонує в інтересах і для досягнення цілей більш загальної системи національної безпеки. З іншого боку, система ІБ є сукупністю взаємозалежних і взаємодіючих елементів, що функціонують на досягнення власних цілей, а саме для забезпечення ІБ держави. З цього погляду Доктрина виступає основою розробки концепцій і національних програм, спрямованих на рішення проблем забезпечення ІБ в окремих сферах життєдіяльності держави. Крім того, Доктрина ІБ має:

- визначити зміст національних інтересів в інформаційній сфері, закріпити задачі щодо досягнення і захисту цих інтересів, створити умови забезпечення їхньої безпеки від зовнішніх і внутрішніх загроз;
- стати основою для формування державної політики в області забезпечення ІБ та пропозицій щодо удосконалення правового, методичного, науково-технічного й організаційного забезпечення ІБ України;
- стати основою для формування регіональних, галузевих та відомчих програм і політик ІБ;
- стати нормативно-правовою базою створення єдиного безпечного інформаційно-телекомунікаційного простору держави.

Нарешті, запропоновано загальний підхід до розробки форми і змісту Доктрини ІБ. Він ґрунтується на загальних методологічних принципах системного аналізу та на генезисі відносин таких фундаментальних категорій як «ціль», «функція» і «структура». Запропонований підхід дозволяє на основі єдиних системних позицій уточнити наріжні поняття Доктрини – інформаційна безпека та система інформаційної безпеки, визначити мету, задачі, принципи і напрямки забезпечення ІБ, функції держави з забезпечення ІБ, обґрунтувати функції і структуру, основні характеристики, властивості та функціональні можливості системи ІБ при забезпеченні єдності форми і змісту Доктрини.

Література: 1. Концепція (основи державної політики) національної безпеки України. Постанова ВР України від 16 січня 1997 року, № 3/97-ВР. 2. Окинавская хартия глобального информационного общества. 3. Доктрина информационной безопасности Российской Федерации. Независимая газета – № 146, 2002. 4. Гончаренко О. М., Лисицин Е. М. Стратегія національної безпеки України та військова реформа // Наука і оборона. – № 1, 2000. – с. 35–38. 5. Гончаренко А., Джангужин Р., Лисицин Э. Гражданский контроль и система национальной безопасности Украины // Зеркало недели. – № 34, 2002. 6. Богданович В. Ю. Роль та місце воєнно-політичної моделі держави у розробленні та здійсненні політики забезпечення її воєнної безпеки // Наука і оборона. – № 1, 1999, – с. 34–37. 7. Кучма Л. Д. Європейський вибір. Концептуальні засади стратегії економічного та соціального розвитку України на 2002–2010 роки. – Київ, 2002. 8. Програма дяльності кабінету Міністрів України на 2002–2004 роки. 9. OECD Guidelines for Security of Information Systems and Networks. – OECD, 2002. 10. OECD Guidelines for Cryptography Policy. – OECD, 1997. 11. Емельянов Г. В.,Сстрельцов А. А. О Доктрине информационной безопасности Российской Федерации // Информационное общество, вып 3, 2000. – С. 22–24. 12. Емельянов Г. В. Основы государственной политики Российской Федерации в обеспечении информационной безопасности и безопасности компьютеризованных систем // Информационное общество, вып. 6, 2000. – С. 16–19. 13. Каландин А. П. Роль Гостехкомиссии России в обеспечении информационной безопасности и защиты информации в Российской Федерации // Труды II Всероссийской конференции «Информационная безопасность России в условиях глобального информационного общества». – Москва, 2001. 14. Закон Украины «О Национальной программе информатизации» № 74/98-ВР – Ведомости Верховного совета – 1998 – № 27–28.

УДК 681.3:34

КОНЦЕПЦІЯ РОЗВИТКУ НОРМАТИВНОЇ БАЗИ ЩОДО СТВОРЕННЯ КОМПЛЕКСІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

Марк Семенко

Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

Анотація: **Наведено аналіз стану та можливі шляхи розвитку нормативної бази системи технічного захисту інформації щодо створення комплексів захисту інформації від витоку технічними каналами.**

Summary: **The concept contains analyses of condition and possible development ways of standard base system of technical protection of information about creation of complex protect system against technical channel information leakage.**

Ключові слова: **Інформація, технічний захист інформації, нормативна база, витік інформації технічними каналами, комплекс технічного захисту інформації.**

Відповідно до Концепції технічного захисту інформації в Україні систему технічного захисту інформації в державі складають три головні компоненти: нормативна база, організаційні структури та матеріальна база. Безперечним є те, що головною складовою системи, яка впливає на дві інші, є нормативна база.

Нормативна база – це нормативно-правові акти організаційно-розпорядчого характеру та нормативні документи технічного характеру. Не применшуючи значення нормативно-правових актів, слід зазначити, що нормативні документи технічного характеру великою мірою визначають стан технічного захисту інформації в Україні.

Становлення технічного захисту інформації в Україні в значній мірі здійснювалося, виходячи з концепцій і підходів, що застосовувалися в системі протидії технічним розвідкам колишнього СРСР. І на цей час основу бази нормативних документів технічного характеру, за напрямом найбільш традиційним – напрямом визначення вимог і рекомендацій щодо забезпечення технічного захисту інформації від витоку технічними каналами, складають нормативно-методичні документи вищезгаданої системи СРСР.

Досвід розвитку технічного захисту інформації в Україні показує, що заміна директивних організаційних методів в сфері ТЗІ на підходи, засновані на використанні принципів системності і стандартизації, а також комплексності є нагальною потребою. До цього спонукає також велике урізноманітнення сучасних технічних засобів оброблення інформації, використання їх у різних сполученнях та умовах, що у загальному випадку виключає можливість надання конкретних однозначних рекомендацій, схем та засобів для забезпечення захисту інформації від витоку, подібних тим, які наводяться в нормативно-методичних документах системи