РОЗДІЛ 4

# Актуальні проблеми забезпечення інформаційної безпеки України

Одержати сотні перемог у бою – це не межа мистецтва.
Підкорити супротивника без бою – ось це вінець мистецтва.
*Сунь Цзи*

## Вступ

Інформаційна безпека України є органічною складовою національної, відтак її розгляд є необхідним для формування базових знань та уявлень про феномен національної безпеки.

Актуальність розгляду даної теми обумовлена цілою групою чинників:

☐ нині головним стратегічним національним ресурсом, основою економічної та оборонної могутності держави стає інформація та інформаційні технології;

☐ інформація у сучасному світі є таким атрибутом, від якого у визначальному плані залежить ефективність життєдіяльності сучасного суспільства;

☐ інформаційні технології принципово змінили обсяг і важливість інформації, яка обертається в технічних засобах її зберігання, обробки і передачі;

☐ загальна комп'ютеризація основних сфер діяльності призвела до появи широкого спектру внутрішніх та зовнішніх загроз, нетрадиційних каналів втрати інформації і несанкціонованого доступу до неї;

☐ масове оснащення державних установ, підприємств, організацій і приватних осіб засобами обчислювальної техніки і включення їх у світовий інформаційних простір містить у собі реальну загрозу створення розгалужених систем регулярного несанкціонованого контролю за інформаційними процесами і ресурсами, навмисного втручання в них;

☐ реальністю сьогодення стало застосування інформаційної зброї і ведення інформаційних війн;

☐ недосконаліть правового регулювання суспільних відносин у сфері інформаційної безпеки призводить до серйозних негативних наслідків, які знаходять свій вираз в ускладненні підтримання необхідного балансу інтересів особи, суспільства і держави, формування конкурентоспроможних місцевих інформаційних агентств і засобів масової інформації;

☐ недобросовісне використання інформаційного простору зсередини держави призводить до зниження рівня внутрішньої інформаційної безпеки України, прямим наслідком чого є дестабілізація соціально-політичної обстановки, проведення акцій опору прийняттю тих чи інших державних рішень;

☐ конституційні права громадян на недоторканність приватного життя, особистої та сімейної таємниці, таємниці листування не мають достатнього організаційно-правового і технічного забезпечення;

☐ погіршується ситуація із забезпеченням збереження державної таємниці, недостатньо розвинені механізми забезпечення службової та комерційної таємниці;

☐ суттєва шкода завдана кадровому потенціалу колективів тих підприємств, які діють у сфері створення засобів інформатизації;

☐ відставання вітчизняних інформаційних технологій змушує при створенні інформаційних систем закуповувати імпортну техніку і залучати іноземні фірми, через що підвищується імовірність несанкціонованого доступу до інформації, що обробляється, і зростає залежність від іноземних виробників комп'ютерної і телекомунікаційної техніки, а також програмного забезпечення.

Відтак процес інформатизації суспільства розвивається стрімко і почасти непередбачено. Інформатизація призводить до створення єдиного інформаційного простору, в межах якого відбувається накопичення, обробка, зберігання й інформацією між суб'єктами цього простору окремими особами, організаціями, державами.

Нормальна життєдіяльність суспільства визначається рівнем розвитку, якістю функціонування і безпекою інформаційного середовища, а також рівнем і станом нормативно-правового забезпечення даних процесів. Інформаційне законодавство спрямоване на закріплення державної інформаційної політики, яка передбачає забезпечення гарантованого рівня національної безпеки в інформаційній сфері, нормального розвитку інформаційних технологій і засобів захисту інформації, виключення монополізму в даній області, запобігання розробленню інформаційно деструктивних технологій впливу на антропогенну популяцію, захист авторських та суміжних прав тощо.

Виробництво і управління, оборона і зв'язок, транспорт та енергетика, банківська справа, фінанси, наука і освіта, медицина, екологія все більше залежать від інтенсивності інформаційного обміну, повноти, своєчасності й достовірності інформації.

Поява і активізацій загроз в інформаційній сфері, передусім загроз від ведення інформаційних війн, суттєво підвищує роль і значення інформаційної безпеки в системі національної безпеки України і обумовлює розширення її змісту. Втрата контролю над національними інформаційними комунікаціями у XXI ст. може призвести до втрати національної незалежності. Майбутні війни – війни без застосування прямого насильства, засобами якого є непрямі дії, одним з методів яких інформаційні війни.

Особливо слід відмітити важливість широкого застосування загальноосвітніх курсів інформаційної безпеки при підготовці кадрів різної професійної спрямованості з урахуванням перспектив розвитку інформаційної цивілізації.

## 1. Поняття та зміст інформаційної безпеки

Характерною ознакою сучасного етапу економічного і науково-технічного прогресу є стрімкий розвиток інформаційних технологій, їх якнайширше використання як у повсякденному житті, так і в управлінні державою. Інформація і інформаційні технології все більше визначають розвиток суспільства і слугують

новими джерелами національної могутності. Становлення інформаційного суспільства радикально змінює політичну, екологічну і соціальну сфери життєдіяльності людства. У цих умовах формування інформаційного суспільства змінює предмет праці на інформацію і знання. У свою чергу, основою глобалізації стають інтеграція інформаційних систем різних держав до єдиної загальносвітової інформаційної системи, формування єдиного інформаційного простору, створення глобальних інформаційно-телекомунікаційних тенет, інтенсивне впровадження нових інформаційних технологій в усі галузі суспільного життя, включаючи і державне управління.

Глобальний процес інформатизації суспільства охопив практично усі країни світу і є нині стрижнем науково-технічного і соціально-економічного розвитку.

Інформатизація становить собою організаційний соціально-економічний та науково-технічний процес створення оптимальних умов для всебічного задоволення інформаційних потреб і реалізації прав громадян, суспільства, органів державної влади й управління на основі формування і використання інформаційних ресурсів та використання інформаційних систем, тенет, ресурсів і інформаційних технологій із використанням обчислювальної й комунікаційної техніки.

Основними ***завданнями інформатизації*** є:

• всебічне інформаційне забезпечення потреб суб'єктів інформаційних відносин;

• створення єдиного безпечного інформаційного простору;

• створення, впровадження і використання інформаційних систем, інформаційних технологій й інформаційних продуктів загального значення;

• підготовка кадрів, підвищення їх кваліфікації у сфері інформатизації.

Осягнення сутності змісту **поняття "інформаційна безпека"** є важливим завданнями наукового аналізу. Будь-яке вчення лише тоді досягає зрілості і досконалості, коли розкриває сутність досліджуваних явищ, має можливість передбачати майбутні зміни не лише в сфері явищ, а й у сфері сутностей. Пізнання сутності інформаційної безпеки можливо лише на основі абстрактного мислення, створення теорії досліджуваного предмета, усвідомлення внутрішнього змісту, виявлення характерних ознак, розкриття сутнісних характеристик поняття, що вивчається.

В історичному процесі складається структура предмета, тобто єдність внутрішнього змісту і зовнішніх проявів, співпадаючих і неспівпадаючих суперечливих сутностей. *Сутність* – сукупність глибинних зв'язків, відносин і внутрішніх законів, які визначають основні риси і тенденції розвитку системи. Сутність може вважатися пізнаною, коли відомі причини виникнення і джерела розвитку об'єкта, що розглядається, шляхи його формування або технічного репродукування, якщо в теорії або на практиці створена його достовірна модель. Одна й та ж сутність може мати множину різних явищ.

Сутність виражається і осягається в дефініції, яка виражає родове поняття. Таким щодо інформаційної безпеки є поняття безпеки, яке характеризує певний процес управління загрозами та небезпеками. Відповідно видове поняття "інформаційна безпека" означає процес управління загрозами та небезпеками в інформаційній сфері.

Саме тому інформаційна безпека є невід'ємною частиною загальної безпеки, чи то національної, чи то регіональної, чи то міжнародної. Аналіз інформаційної безпеки передбачає розгляд сукупності таких об'єктивних чинників:

потреб громадян, суспільства і держави світового співтовариства; уразливість індивідів, суспільства і держави від шрифтових технологій;

наявність широкого кола загроз і небезпек, якими має управляти система забезпечення інформаційної безпеки.

Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона орієнтована на захист значущих або вже згаданих суб'єктів інформаційних ресурсів, законних інтересів. Зміст поняття "інформаційна безпека" розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах.

Так, визначення інформаційної безпеки було дано у Федеральному Законі Росії "Про участь у міжнародному інформаційному обміні". У даному законі **інформаційна безпека** розглядалася як стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій і держави. Ця трактовка виходить з того, що захист інформації та інформаційної інфраструктури і становить собою зміст інформаційної безпеки. При цьому акцент робиться на технічній стороні даної проблеми.

Дещо інше визначення **інформаційної безпеки** міститься у Доктрині інформаційної безпеки Російської Федерації, де воно визначається як стан захищеності її національних інтересів держави в інформаційній сфері, які визначаються сукупністю збалансованих інтересів особи, суспільства і держави. З цього визначення слідує, що зміст поняття безпеки базується на інтересах суб'єктів суспільних відносин в інформаційній сфері, від збалансованості яких залежить рівень загроз.

Слід зазначити, що у науковій літературі поки відсутній єдиний консолідований погляд на зміст поняття "інформаційна безпека". Для одних воно відображає стан, для інших процес, діяльність, здатність, систему гарантій, властивість, функцію. Відтак постає необхідність в угрупуванні напрямів визначення аналізованого поняття.

Так, наприклад, представник першого напряму за нашою умовною класифікацією, Ю.А.Фісун, співробітник Академії управління МВС РФ, характеризує *інформаційну безпеку* як "стан захищеності інформаційного середовища, який відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз". Такої ж позиції притримуються і розробники концепції інформаційної безпеки центру Разумкова, а також деякі українські дослідники, які вважають за необхідне визначати інформаційну безпеку як стан захищеності. Так, наприклад, В.К. Гаєвський, В.А. Авраменко визначають **інформаційну безпеку** як стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації, у той час як О.Г. Додонов визначає інформаційну безпеку як стан за-

хищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави.

Аналогічного погляду дотримується і інший російський дослідник І. Панарін, роблячи більший акцент на ролі політичної еліти, яка може протистояти інформаційному впливу. На його думку, *інформаційна безпека – це* стан інформаційного середовища суспільства і політичної еліти, який забезпечує її формування й розвиток в інтересах керівництва країни, громадян і суспільства.

Дещо в *іншому ракурсі* трактує інформаційну безпеку А.А.Тер-Акопов, який репрезентує позицію другого напряму. Під *інформаційною безпекою* він розуміє стан захищеності інформації, яка забезпечує життєво важливі інтереси людини. У рамках даного напряму існує визначення інформаційної безпеки як стану, тенденції розвитку, умови життєдіяльності соціуму, його структур, інститутів і установ, при яких забезпечується збереження їх якісної з об'єктивними обумовленими інноваціями в ній, і вільне, відповідне власній природі і її функціонування. Ряд представників цього напряму розглядають інформаційну безпеку як стан, який характеризується відсутністю небезпеки, тобто чинників і умов, які загрожують безпосередньо індивіду, спільноті, державі з боку інформаційно-комунікаційного середовища. Прибічники такого підходу розглядають інформаційну безпеку як стан і процес захищеності особи, суспільства, держави від реальних або потенційних загроз. Водночас, на нашу думку, розглядати безпеку лише в якості стану є не зовсім точним, і це не відображає динамізму як самої безпеки, так і тієї системи, для якої безпека виступає як функція її подальшого розвитку та існування.

Поняття "процес" відрізняється від поняття "стан". Поняття процес означає послідовність станів, пов'язаність стадій їх зміни і розвитку, тобто на відміну від поняття "стан", поняття "процес" акцентує увагу на моменті спрямованості в зміні об'єкта, цілепокладанні, у той час, як "стан" відображає лише один момент, певну мить безпеки, а отже, не вичерпує її повністю.

Представник *третього напряму,* В.І.Ярочкін, визначає безпеку як стан захищеності особи, суспільства і держави від зовнішніх та внутрішніх небезпек та загроз, який базується на діяльності людей, суспільства, держави, світового співтовариства по виявленню (вивченню), попередженню, послабленню, ліквідації і відбиттю небезпек і загроз, здатних знищити їх, позбавити фундаментальних матеріальних і духовних цінностей, завдати неприйнятної шкоди, закрити шлях для прогресивного розвитку". Застосування діяльнісного підходу, на наш погляд, є більш адекватним при описуванні інформаційної безпеки, і ми в певній мірі можемо підтримати дане визначення у загальному плані, у той же час не погодитись із деталізацією напрямів діяльності, які з часом змінюватимуться, а отже, закладатимуть потенціал нестійкості як до самого визначення, так і до функціонування відповідних суб'єктів.

М.П.Хрипков вважає, що діяльність по забезпеченню особи, суспільства і держави виникає в ході вирішення суперечності між такою об'єктивною реальністю, як небезпека, і потребою розумної сутності, соціального індивіда, соціальної групи попередити її можливі шкідливі наслідки. Водночас, за даного випадку, функціонування системи забезпечення інформаційної безпеки зводиться лише до реагування, у той час як превенція залишається поза увагою.

Саме тому, на наше переконання, інформаційна безпека становить собою діяльність органів державного управління. Звідси витікає важливий висновок, що слід діяти активно, здійснюючи вплив на джерела інформаційної небезпеки. При цьому щодо змісту інформаційної безпеки доцільно використовувати не поняття "інтереси", а більш фундаментальне поняття "цінності", через те, що у цінностях знаходять вираз інтереси суб'єктів суспільних відносин, зіткнення яких породжує загрози.

Наступний погляд передбачає, що у самому загальному вигляді під *інформаційною безпекою* можна розуміти здатність суб'єкта зберігати свої системостворюючі властивості, основні характеристики при патогенних дезорганізуючих, деструктивних впливах на кіберпростір, інформаційно-комунікаційні технології.

На думку прибічників даного погляду, безпека і забезпечення безпеки становлять собою різні поняття, через те, що безпека виражає характеристику стану соціальної спільноти, у той час як забезпечення безпеки – діяльнісну характеристику, тобто діяльність органів державної влади і управління по підтриманню безпеки. У цьому плані безпека усвідомлюється як основа цілепокладання політики, а забезпечення безпеки – як діяльність по досягненню безпечного стану суспільства або соціальної групи. Цієї ж думки притримується і автор даного посібника.

Цікавою є думка відомого українського дослідника проблем інформаційної безпеки Р.А.Калюжного, який вважає, що **інформаційна безпека –** вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин, пов'язаних із створенням, розповсюдженням, зберіганням та використанням інформації.

У цілому ж інформаційна безпека покликана забезпечити реалізацію національних інтересів за допомогою усього арсеналу засобів, що маються в її розпорядженні. У цьому сенсі ми вважаємо, що найвищий сенс політики інформаційної безпеки – вільний розвиток і процвітання суспільства.

Отже *інформаційна безпека* являє собою одне з важливіших понять в науці і різних сферах людської діяльності. Сутність і комплексність цього поняття виявляється характером сучасного інформаційного суспільства. Аналіз різних підходів до визначення змісту поняття "інформаційна безпека" дає можливість зауважити про недоцільність суворого обрання тієї чи іншої позиції. Наведені вище погляди, а вірніше, підходи до визначення поняття інформаційної безпеки дають змогу розглядати дану проблему більш комплексно і системно, додати знань про цей багатогранний феномен. Більше того, на наше переконання, найбільш прийнятним є інтегральний підхід, за якого інформаційна безпека визначатиметься за допомогою окреслення найбільш важливих її сутнісних ознак з урахуванням постійної динаміки інформаційних систем.

Такий підхід дав нам можливість дійти висновку, що інформаційна безпека не може розглядатися лише в якості окремого стану. Безперечно, що це є і властивістю, атрибутом інформаційного суспільства, діяльністю і результатом діяльності людини, спрямованими на забезпечення певного рівня безпеки в інформаційній

сфері. Інформаційна безпека має враховувати майбутнє, а отже, вона не є станом, а становить собою процес. Таким чином, ***інформаційну безпеку*** слід розглядати крізь ***органічну єдність ознак, таких як стан, властивість, а також управління загрозами і небезпеками, за якого забезпечується обрання оптимального шляху їх усунення і мінімізації впливу негативних наслідків.***

Також наголосимо на тому, що не підтримуємо позицій тих дослідників, які зводять інформаційну безпеку лише до захисту інформації. Інформаційна безпека за своєї суттю є більш широким поняттям. Отже інформаційна безпека багатогранна область діяльності, в якій успіх може принести лише системно-комплексний підхід.

Дослідження сутності інформаційної безпеки має враховувати той факт, що сутність є внутрішнім змістом предмета, який знаходить вираз у стійкій єдності усіх багатоманітних і суперечливих формах буття.

*Базовою характеристикою* інформаційної безпеки слід вважати імовірність появи загрози підвищеного ризику реалізації загрози або небезпеки для індивіда, суспільства та держави.

*Критерієм ефективності* забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних затрат.

Отже можна говорити про структуру поняття інформаційної безпеки. Основним її елементом є життєво важливі інтереси соціальної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональних або інших національно-державних структур у рамках міжнародного співтовариства. Зсередини національно-державного утворення його життєво важливі інтереси перебувають у взаємодії з інтересами елементів, які складають дане утворення. В якості останніх виступають соціальні групи, еліта, організації, партії, релігійні та етнічні утворення, рухи тощо. Сукупність внутрішніх і зовнішніх інформаційних загроз створює передумови для порушення безпечного функціонування системи державного управління.

Значущість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення інформаційної безпеки як одне з глобальних і пріоритетних завдань політики національної безпеки.

Як нами вже зазначалося, національні інтереси в інформаційній сфері є похідними від національних цінностей. Отже інтереси інформаційної безпеки витікають із таких цінностей, як права людини, свобода, економічне процвітання. Саме тому головним інтересом для України є її виживання як вільної незалежної нації при збереженні її фундаментальних цінностей і інститутів безпеки.

Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх і зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування. Відтак інформаційна безпека може описуватися за допомогою терміна "гомеостазис".

До **характеристик**, за допомогою яких можна описати дану систему, віднесемо такі:

• *доступність* – можливість за прийнятний час отримати шукану інформаційну послугу будь-яким суб'єктом виконавчої влади;

• *цілісність* – актуальність і несуперечливість інформації, її захищеність від руйнування і несанкціонованої зміни;

• *конфіденційність* – захист від несанкціонованого ознайомлення.

Сутність і зміст інформаційної безпеки проявляються по-особливому на кожному з рівнів державного управління, зокрема на:

• *стратегічному* – Кабінет Міністрів України;

• *тактичному* – центральні органи виконавчої влади;

• *оперативному* – місцеві органи виконавчої влади, провідне місце серед яких посідають місцеві державні адміністрації.

Отже можна говорити і про прояви інформаційної безпеки у самому процесі її забезпечення, таким чином можна виділити такі рівні:

• *нормативно-правовий* закони, нормативно-правові акти, тощо;

• *адміністративний* дії загального характеру, які вживаються органами державного управління;

• *процедурний* конкретні процедури забезпечення інформаційної безпеки;

• *програмно-технічний* конкретні технічні заходи забезпечення інформаційної безпеки.

Для розкриття сутності і змісту інформаційної безпеки важливим є зв'язок останньої із політикою держави. Складовою частиною політики держави як регулятора суспільних відносин відповідно до гуманістичних начал є обов'язок забезпечення інформаційної безпеки особи, суспільства і держави.

Інформаційна безпека як одна з характеристик стійкого розвитку виступає в якості базової цінності держави. У той же час ціннісні орієнтації, що ґрунтуються на уявленнях про інформаційну безпеку у різних суспільних груп і окремих осіб, почасти не співпадають. Саме у цьому знаходить свій безпосередній вираз вплив держави, яка за допомогою системи методів виражає загальні цінності в сфері інформаційної безпеки.

### *1.1. Категорійно-понятійна система інформаційної безпеки*

***Інформаційна безпека*** – складова національної безпеки, – свідомий, цілеспрямований вплив на загрози та небезпеки державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України; вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України, неухильне дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

***Інформаційні відносини*** – відносини, які виникають у всіх сферах життя і діяльності людини, суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації.

***Інформаційний суверенітет*** – здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, забезпечення національної безпеки держави.

***Інформаційний простір (національний)***: 1) інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту і поширення інформації, інформаційних продуктів та інформаційних ресурсів, на яке розповсюджується юрисдикція держави; 2) сукупність національних інформаційних ресурсів та інформаційної інфраструктури, які дозволяють на основі єдиних принципів і загальних правил забезпечувати інформаційну взаємодію громадян, суспільства і держави з їх рівним правом доступу до відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб суб'єктів держави на всій її території з додержанням балансу інтересів на входження у світовий інформаційний простір і забезпечення інформаційної безпеки відповідно до Конституції України та міжнародних правових норм.

***Інформаційна інфраструктура*** – сукупність взаємодіючих систем виробництва, накопичення, збереження і розвитку інформаційних продуктів та їх доставки, виробництво інформаційних технологій, сервісне обслуговування інфраструктури і системи підготовки кадрів.

***Інформаційна система*** – організаційно впорядкована сукупність інформаційних ресурсів та інформаційних технологій і засобів забезпечення інформаційних процесів.

***Інформаційні ресурси***: 1) сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо); 2) організована сукупність інформаційних продуктів певного призначення, що необхідні для забезпечення інформаційних потреб громадян, суспільства, держави у певній сфері життя чи діяльності.

***Інформаційні технології***: 1) цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування; 2) цілеспрямовано організована сукупність інформаційних процесів для створення і використання інформаційних продуктів, або надання інформаційних послуг; 3) технологічний процес, предметом перероблення й результатом якого є інформація; 4) процес матеріалізації знань у продукцію і послуги за допомогою комп'ютерно-телекомунікаційних систем; 5) система методів і способів використання комп'ютерної техніки і систем зв'язку для створення, пошуку, одержання, відображення, реєстрації, накопичення, збереження, захисту і поширення інформаційних продуктів.

***Інформаційне середовище*** – усталене поєднання окремих суб'єктів національного інформаційного простору України, інформаційної інфраструктури та інформаційних ресурсів, що взаємодіють в інформаційних процесах.

***Інформаційний ринок*** – це система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг

***Інформаційний продукт (продукція)***: 1) документована інформація, яка підготовлена і призначена для задоволення потреб користувачів; 2) документована інформація, яку підготовлено у відповідності до потреб користувачів і яка призначена чи застосовується для задоволення потреб користувачів; 3) створена виробником сукупність документованої інформації, відомостей, даних і знань, яка призначена для забезпечення інформаційних потреб користувача.

***Інформаційне забезпечення*** – підтримка засобами систем баз даних і баз знань процесів виробництва, торгівлі, керування, навчання, наукових досліджень, та будь-якої іншої діяльності у всіх сферах життя суспільства, які спрямовані на створення умов для задоволення інформаційних потреб людини, суспільства та держави.

***Інформаційне поле***: 1) сукупність енергетичних субстанцій окремих об'єктів, які є елементами інформаційного поля Землі та Всесвіту; 2) просторово-часові вібрації (інформаційно-розпорядницькі структури), що містять відомості про минуле, сьогодення і майбутнє Всесвіту.

***Інформаційне суспільство***: 1) суспільство, в якому більшість працюючих займаються створенням, збиранням, відображенням, реєстрацією, накопиченням, зберіганням і поширенням інформації, особливо її вищої форми – знань; 2) суспільство, в якому діяльність людей ґрунтується на використанні послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку.

***Інформатизація***: 1) сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, які спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки; 2) діяльність, спрямована на створення та широкомасштабне використання в усіх сферах життя суспільства інформаційних технологій.

***Інформатика*** – наукова діяльність, що вивчає інформаційні структури і процеси збирання (набуття, придбання), відображення, реєстрації, накопичення, зберігання і поширення (розповсюдження, реалізація) інформації за допомогою ЕОМ.

***Інформаціологія*** новітня загальна фундаментальна наука про інформаційні природні процеси матеріалізації та дематеріалізації в мікро- й макроструктурах Всесвіту, що самоорганізуються.

***Інформація***: 1) документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі; 2) відомості про осіб, предмети, технології, засоби, ресурси, події та явища, що відбуваються в усіх сферах діяльності держави, життя суспільства, і навколишньому природному середовищі, незалежно від форми їх подання; 3) будь-які знання про предмети, факти, поняття і т. ін. проблемної сфери, якими обмінюються користувачі системи оброблення даних.

***Інформаційна війна*** – процес боротьби між суб'єктами із застосуванням інформаційної зброї.

***Інформаційна зброя*** – засоби, які дозволяють вчинювати задумані дії із повідомленнями, що передаються, обробляються, створюються, знищуються і сприймаються.

***Інформаційна загроза*** – вхідні дані, початково призначені для активізації в інформаційній системі алгоритмів, що відповідають за звичайний режим функціонування.

***Сугестія*** – прихований інформаційний вплив на інформаційну систему, що самонавчається.

***Сугестивний вплив*** – вплив по формуванню у інформаційної системи, що самонавчається, прихованих від неї самої цілей.

Зважаючи на той факт, що будова системи забезпечення внутрішньої інформаційної безпеки неможлива поза контекстом загроз та небезпек, наступним елементом для розгляду і будуть загрози інформаційній безпеці, що в сукупності і дозволить окреслити напрями функціонування системи забезпечення інформаційної безпеки.

## 2. Характеристика загроз інформаційній безпеці системи державного управління

Загрози інформаційній безпеці, з одного боку, є організаційним компонентом системи управління національною безпекою, а з іншого слугують індикатором ефективності її функціонування. Адже реалізація загроз і переростання їх у небезпеки свідчить про неефективність функціонування даної системи, і навпаки. На сьогодні розглядати будь-які загрози в інформаційній сфері необхідно з урахуванням того контексту, в якому вони виникають і знаходять свій вияв. Найбільшою небезпекою на даному етапі розвитку українського суспільства є ***інформаційні війни***.

### *2.1. Поняття інформаційної війни*

Намагання у повній мірі усвідомити усі грані поняття інформаційної війни нагадують здебільшого намагання сліпих, які прагнуть зрозуміти природу слона: той, хто дотикається до ноги, називає її деревом; хто дотикається до хвоста називає його канатом. Відверто скажемо, що питання формування понятійного апарату в сфері інформаційних відносин ще остаточно не вирішені. І передусім це пов'язано із несформованістю загальної теорії національної безпеки та її понятійного апарату.

Передусім хотіли б наголосити на тій обставині, що чисельність трактувань даного поняття, має більш глибинні коріння, ніж це може здатися на перший погляд. Йдеться про несформованість загальної теорії національної безпеки, а отже, і базового висхідного алгоритму будови понятійного апарату. Ми лише акцентуємо увагу на тій обставині, що формування понятійного апарату інформаційної безпеки неможливе без формування даного апарату в рамках загальної теорії національ-

ної безпеки – "націобезпекознавства", основи якої ми розглядали у першому розділі.

Більше того, його формування має бути обумовлено і корелювати із останнім. Не можна, наприклад, визначати інформаційну безпеку, використовуючи формулу: захищеність від..., у той час як поняття національної безпеки (тобто родового поняття) визначається через формулу: управління загрозами та небезпеками. Певна річ, що понятійний апарат відповідних теорій, які слугують інструментом пізнання тих чи інших явищ у конкретних сферах життєдіяльності, не може розвиватися синхронно. Втім фундаментальні принципи його формування мають бути дотримані. За інших умов говорити про формування загальної теорії національної безпеки, а в її межах приватних теорій національної безпеки, зокрема теорії інформаційної безпеки, а отже і науково обґрунтованої цілісної концепції забезпечення національної безпеки, стає неможливим.

На сьогодні саме інформаційні війни становлять собою найбільшу небезпеку нормальному функціонуванню системи органів державного управління. Це і обумовлює детальний розгляд нами питань щодо визначення поняття та встановлення сутнісних ознак інформаційної війни.

Вперше термін "інформаційна війна" з'явився наприкінці 80-х рр. XX ст. Він став результатом плідної праці теоретиків Збройних Сил США і став уживаним після вдало проведеної роботи по знищенню СРСР. Активного застосування даний термін набув під час проведення воєнної кампанії США в Іраку у 1991 р., де уперше були не лише застосовані інформаційні технології, а вперше було відкрито наголошено на цьому, що спричинило ще більший резонанс.

Передусім, коли йдеться про будь-яку війну, включаючи інформаційну, то слід говорити про певний стан взаємовідносин між противниками. Здебільшого це не є присутнім, тому застосування даного терміна, на нашу думку, носить псевдонауковий характер. Інформаційна війна виникає з нових підходів до застосування інформації, визначення її ролі та місця. Можна виділити два трактування поняття інформаційної війни: гуманітарне і технічне.

Наприклад, М. Павлютенкова зазначає, що у гуманітарному сенсі інформаційна війна становить собою активні методи трансформації інформаційного простору, що знаходить свій вираз у системі нав'язування моделей світу, які покликані забезпечити бажані типи поведінки, атаках на структури породження інформації, процеси міркувань. У той же час технічне трактування даного поняття полягає у тому, що за допомогою спеціальних програм руйнується обладнання, програмне забезпечення тощо.

Отже аналіз даного бачення певних процесів в інформаційній сфері дозволяє з високою часткою очевидності говорити про підміну понять, тому що війна за своїм значенням означає стан, у якому держави застосовують одна проти одної усі форми тиску з дотриманням дії законів та звичаїв ведення війни (jus in bello). Втім, наведений вище приклад бачення поняття інформаційної війни дає усі підстави стверджувати, що описані вище ознаки не складають даного поняття.

Безперечним є той факт, що формування інформаційного суспільства стає не просто фактом, а все більше починає впливати на формування державної політики

інформаційної безпеки. Досягнення тих чи інших цілей виявилося можливим із застосуванням лише інформаційних технологій, які б чинили вплив на суспільну свідомість. Одним з проявів застосування даного методу є жорсткий часовий пресинг на суб'єктів управління національною безпекою, який не залишає їм часу на прийняття виваженого, такого, що відповідає українським національним інтересам, рішення. Відтак, досягнення певних геополітичних та інших важливих цілей уможливлюється за допомогою невоєнних методів.

Сумний досвід не приділення необхідної уваги даним питанням спричинив розпад СРСР, могутньої держави, яка до 1991 р. була єдиним реальним конкурентом США у володарюванні світом. Саме це дає можливість стверджувати про необхідність розроблення ***концепції інформаційного стримування***. Події із касетним скандалом у 2001 р., витівки офіцера безпеки українського посольства в Німеччині В.Кравченка у лютому 2004 р., нічим не підтверджені заяви про викрадення дітей у Харкові, широкий розголос хабарництва у 3 окремому батальйоні в Лівані у серпні 2005 р. та ряд інших прикладів дають усі підстави стверджувати, що в Україні поки відсутня розроблена на концептуальному рівні концепція (система теоретико-методологічних засад, положень) забезпечення інформаційної безпеки. Більше того, аналіз сучасної геополітичної обстановки дає нам усі підстави зробити висновок, що проти України здійснюються широкомасштабні інформаційні акції, спрямовані на дискредитацію, дезорганізацію, підрив іміджу і дестабілізацію нашої держави. І передусім цей вплив чиниться на систему управління національною безпекою.

Не можна оминути і того питання, що так звана четверта влада – ЗМІ – відіграла не останню роль в закріпленні у свідомості пересічного громадянина терміну "інформаційна війна". Причому під останнім ЗМІ здебільшого розуміють злив компромату через засоби масової інформації, здебільшого електронні. Ідеальним засобом для цього є Інтернет, який дає можливість розповсюджувати будь-яку інформацію без будь-яких обмежень. Характерним є те, що по Україні процент використання Інтернету не перевищує 10, у той час як у Європі він дорівнює близько 75 відсоткам. Таким чином, відбувається парадоксальна ситуація, коли імідж України руйнується ззовні, причому "зсередини" більшість населення навіть не має про це і гадки.

Що стосується іншого розуміння поняття інформаційної війни, себто технічного, то тут обов'язковою умовою є та, що ведення інформаційної війни є результатом узгодженої діяльності по використанню інформації як зброї ведення бойових дій у будь-якій сфері життєдіяльності. При цьому інформаційна війна включає такі дії:

• здійснення впливу на інфраструктуру систем життєзабезпечення телекомунікації, транспортні мережі, електростанції тощо;

• промисловий шпіонаж порушення прав інтелектуальної власності, розкрадання патентованої інформації, викривлення або знищення важливих даних, проведення конкурентної розвідки;

• хакінг – злам і використання особистих даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо.

Безперечно, що якщо ми говоримо про інформаційну війну, то вочевидь зрозумілим є факт, що даний термін є найбільш спорідненим із воєнними. Тому, коли

йдеться про інформаційну війну, то слід говорити про існування рішучої і небезпечної діяльності, пов'язаної із реальними бойовими діями. Більше того, за даного випадку постає необхідність у виокремленні декількох підвидів інформаційних війн: кібернетична війна, електронна війна, психотронна війна, психотропна війна, штабна війна, психологічна, енергоінформаційна війна.

Таке розуміння інформаційної війни дає можливість погодитись із визначенням поняття інформаційної війни, яке мається у Збройних Силах США. Отже **інформаційна війна** – це дії, що вчинюються для досягнення інформаційної переваги у підтримці національної воєнної стратегії через вплив на інформацію та інформаційні системи противника при одночасному забезпеченні безпеки власної інформації і інформаційних систем. Одним з прикладів є існування спеціальної програми запису усіх телефонних дзвінків, що виходять за кордон США, на спеціальну апаратуру. За допомогою даної програми усі телефонні дзвінки, що виходять за межі країни, записуються, а потім пропускаються через спеціальний пристрій, який за допомогою пошукових систем за ключовими словами здійснює виявлення та ідентифікацію важливої інформації.

Відтак, існування розвинутої системи інформаційної безпеки закладе фундамент для стійкого функціонування системи державного управління. На думку деяких дослідників, стрімкий розвиток інформаційних технологій спричинить у майбутньому появу нових за змістом видів війн, які відбуватимуться без жодного пострілу. Особливо наголосимо, що сучасні інформаційні війни спрямовані здебільшого на економічну інфраструктуру.

Цілі інформаційної війни є дещо іншими, аніж війни у звичному розумінні: не фізичне знищення противника і ліквідація його збройних сил, а широкомасштабне порушення роботи фінансових, транспортних і комунікаційних мереж і систем, руйнування економічної інфраструктури і підкорення населення країни, що зазнала атаки, волі країни-переможця.

Є й інші думки з цього приводу. За даними російського дослідника А.А.Кокошина вперше термін "інформаційна війна" було введено у 1985 р. у Китаї. В основі теоретичних підходів китайських спеціалістів в області інформаційного протиборства лежать погляди давньокитайського воєнного діяча Сунь-цзи. Він перший узагальнив досвід інформаційного впливу на супротивника. У своєму трактаті "Мистецтво війни" Сунь-цзи писав: "у будь-якій війні, як правило, найкраща політика зводиться до захоплення держави в цілому... Одержати сотні перемог у бою це не межа мистецтва. Підкорити супротивника без бою – ось це вінець мистецтва".

На початку 90-х рр. термін "інформаційна війна" з'явився у США та активно увійшов в загальносвітову практику. На сьогодні даний термін використовується в двох площинах:

- у широкому розумінні – для визначення протиборства в інформаційній сфері в засобах масової інформації для досягнення різних політичних цілей;
- у вузькому розумінні – для визначення воєнного протиборства, у військовій інформаційній сфері для досягнення односторонніх переваг в отриманні, зборі, обробці та використанні інформації на полі бою (в операції, битві).

У вітчизняній практиці в широкому розумінні найчастіше використовують термін "інформаційне протиборство"; у вузькому розумінні "інформаційні воєнні дії".

Автор даного навчального посібника дотримується позиції, відповідно до якої **інформаційне протиборство** – це форма боротьби сторін в інформаційному просторі з використанням політичних, економічних, дипломатичних, військових та інших методів, способів та засобів, для впливу на інформаційне поле супротивника та захисту власного інформаційного поля в інтересах досягнення поставлених цілей.

Ураховуючи таке визначення можна зазначити, що інформаційне протиборство включає в себе три незмінні складові: 1) вплив; 2) аналіз; 3) протиборство.

Причому основним елементом, від якого залежить ефективність кампанії, є аналіз, мета якого полягає в оцінці, стратегічному прогнозуванні та плануванні в аспектах внутріполітичного та зовнішньополітичного становища. Що ж стосується "інформаційної війни", то як всеохоплююча, цілісна стратегія, вона обумовлена всезростаючою значущістю та цінністю інформації у питаннях командування, управління та політики. Також можна послуговуватись визначенням "*інформаційної війни*" як "комунікативної технології по впливу на масову свідомість з короткочасними та довгочасними цілями".

На заході *інформаційну війну* визначають як "нефізичну атаку на інформацію, інформаційні процеси та інформаційну інфраструктуру", причому "ціллю інформаційної війни є вплив на систему знань та уявлень зовнішнього супротивника". Під знанням тут розуміється об'єктивна інформація, загальна для усіх, а під уявленнями інформація, яка носить суб'єктивний характер.

Основним інструментом ведення інформаційної війни є *інформаційна зброя*. До "інформаційної зброї" ми будемо відносити, по-перше, засоби інформаційно-технічного характеру, які знищують, перекручують або викрадають інформацію, не зважаючи на систему захисту, обмеження доступу до цієї інформації законних користувачів. По-друге, це, безперечно, інформаційно-психологічні засоби, які дезорганізують інформаційні системи шляхом дезінформації, формування помилкових логічних інформаційних концепцій, інтерпретацій та ін., впливаючи, таким чином, на суспільну думку, на життя суспільства, держави або групи держав в цілому.

Таким чином, **інформаційна зброя** – це "пристрої та засоби, які призначені для нанесення протидіючій стороні максимальної шкоди в ході інформаційної боротьби (шляхом небезпечних інформаційних впливів).

Об'єктами впливу можуть бути: інформаційно-технічні системи, інформаційно-аналітичні системи, інформаційно-технічні системи, які включають людину, інформаційно-аналітичні системи, які включають людину, інформаційні ресурси, системи формування суспільної свідомості та думки, яка базується на засобах масової інформації та пропаганди, а також психіки людини.

Необхідно підкреслити, що інформаційна зброя є інструментом встановлення контролю над інформаційними ресурсами потенційного супротивника, тому інформаційна зброя втручається в роботу систем управління та інформаційних систем, систем зв'язку тощо, в цілях порушення їх працездатності, аж до повного виведен-

ня їх з ладу, вилучення, перекручення даних, які в них містяться, або цілеспрямованого уведення спеціальної інформації. Почасти інформаційна зброя виступає в ролі розповсюджуваної дезінформації в системі формування суспільної свідомості й прийняття рішень. Особливу небезпеку у даному випадку становлять дані, які надходять для органів державної влади, тому що від їх достовірності залежить поінформованість і здатність даних органів приймати правильні рішення і вживати своєчасні заходи по управлінню державою.

До інформаційної зброї також відносять й сукупність спеціальних способів та засобів впливу на психіку суспільства та держави в цілому.

Для проведення будь-якої інформаційної кампанії, як у міжнародних відносинах, так і у внутрішньому інформаційному полі, необхідно враховувати особливості конкретного інформаційного простору. Напочатку необхідно розшукати уразливі точки в інформаційному просторі і тільки потім переходити до рішучих дій.

Інформаційна зброя повинна враховувати варіанти протидії, і чим більше варіантів протидії враховано, тим більше вірогідності успіху в тій чи іншій інформаційній агресії. Також необхідно підкреслити, що специфікою інформаційної війни (інформаційного протиборства) є те, що вона ведеться, на відміну від збройної боротьби, як у мирний, так і у воєнний час. Вона націлена на всі можливості і фактори ураженості, які неминуче виникають при зростанні залежності від інформації, а також на використання інформації у найрізноманітніших конфліктах. Об'єктом уваги стають інформаційні системи (включаючи відповідні лінії передач, центри обробки та людський фактор цих систем), а також інформаційні технології, які використовуються в системах озброєння. Таким чином, можна виділити такі *сфери інформаційного протиборства*: світоглядна, політична, дипломатична, воєнна, науково-технологічна, соціальна та гуманітарна, ідеологічна, екологічна.

Інформаційна війна має наступальні та оборонні складові, але, починаючи з цільового проектування та розробки своєї архітектури командування, управління, комунікації, комп'ютерів та розвідки, вона забезпечує особам, які приймають рішення, відчутну інформаційну перевагу у різноманітних конфліктах. Інформаційна війна може бути спрямована проти *трьох елементів*: комп'ютер; програмне забезпечення; людина.

Крім того, неможливо заперечувати й того факту, що однією з головних цілей та завдань інформаційної війни є подавлення в людині морального творчого початку, зміна її світогляду.

На міжнародній арені інформаційні війни ведуться: між державами та блоками держав; між міжнародними корпораціями, транснаціональними корпораціями і міжнародними фінансовими групами; між міжнародними корпораціями, ТНК і міжнародними фінансовими групами з державами; між терористичними організаціями та державами; між міжнародними корпораціями, ТНК і міжнародними фінансовими групами; між злочинними організаціями; між злочинними організаціями та державами.

Взагалі ж технології інформаційного віку певним чином зрівняли індустріальні, постіндустріальні і доіндустріальні країни: всі вони мають доступ до інструментарію, необхідного для ведення інформаційної війни, а отже, і виступають як

суб'єктами так і об'єктами інформаційної війни, а отже і забезпечення внутрішньої інформаційної безпеки.

### *2.2. Поняття та види загроз національним інтересам та національній безпеці в інформаційній сфері*

Як інформаційна війна, так і інформаційне протиборство й інформаційна боротьба є проявами одного, більш широкого, поняття **загрози національним інтересам та національній безпеці в інформаційній сфері**. Для більш комфортного розуміння як синонім до вищенаведеного поняття будемо вважати вираз "інформаційна безпека".

Слід зазначити, що аналізові змісту поняття "інформаційна безпека" зазвичай дослідниками приділяється значна увага, у той час як такі поняття, як "небезпека" і "загроза" розглядаються дещо спрощено і здебільшого у звуженому плані, відірваному від контексту поняття "інформаційна безпека" та майже не пов'язаному із контекстом родового поняття "загроза" в рамках націобезпекознавства.

Необхідність у розробленні поняття **"загроза інформаційній безпеці"** визначається: 1) відсутністю єдиного підходу до дослідження основних понять інформаційної безпеки; 2) недостатньою розробленістю родового поняття "загроза" і питань його відмежування від інших споріднених понять, таких, як "небезпека", "виклик", "ризик", і відповідно видового "інформаційна загроза" та його відмежування від таких понять, як "інформаційна війна", "інформаційне протиборство", "інформаційний тероризм"; 3) наявністю невирішеної проблеми формування категорійно-понятійного апарату теорії інформаційної безпеки; 4) можливістю на підставі теоретичних розробок даного апарату формувати адекватну систему моніторингу та управління загрозами й небезпеками в інформаційній сфері.

Найбільш широко ***загрози інформаційним ресурсам*** можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, яка зберігається в ній. Виникнення загрози, тобто віднаходження джерела актуалізації певних подій у загрози, характеризується таким елементом, як *уразливість*. Саме за наявності вразливості як певної характеристики системи і відбувається активізація загроз. Безперечно, що самі загрози за своєю суттю відповідно до теорії множин є невичерпними, а отже і не можуть бути піддані повному описові у будь-якому дослідженні.

Відповідно до Закону України "Про основи національної безпеки України" до загроз національним інтересам і національній безпеці в інформаційній сфері відносять такі:

- ☐ прояви обмеження свободи слова та доступу громадян до інформації;
- ☐ поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- ☐ комп'ютерна злочинність та комп'ютерний тероризм;
- ☐ розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави

або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

□ намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації.

До ***загроз інформаційній безпеці системі управління національною безпекою*** належать: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання.

## 3. Теоретичні аспекти формування та функціонування системи забезпечення інформаційної безпеки України

Як нами вже наголошувалося проблема забезпечення національних інтересів і національної безпеки в інформаційній сфері поки перебуває на стадії розроблення. Хоча не можна не відмітити і того факту, що саме проблеми інформаційної безпеки, як свідчить проведений нами контент-аналіз наукових досліджень, висвітлюються найбільше.

Втім питанням формування системи забезпечення інформаційної безпеки, адекватної загрозам, уваги приділялося недостатньо.

Відтак постає необхідність у визначення поняття "система забезпечення національної безпеки в інформаційній сфері".

Інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері, системою заходів економічного, політичного і організаційного характеру, адекватних загрозам та небезпекам національним інтересам особи, суспільства та держави в інформаційній сфері.

Основними *суб'єктами* забезпечення інформаційної безпеки є держава і особа.

Для створення і підтримання належного рівня національної безпеки в інформаційній сфері розробляється система правових норм, що регулюють відносини в інформаційній сфері, визначаються основні напрями діяльності органів державного управління, формуються або перетворюються органи та сили забезпечення інформаційної безпеки і механізм контролю та нагляду за їх діяльністю.

### *3.1. Поняття системи забезпечення інформаційної безпеки*

У даному навчальному посібнику автор ґрунтується на вже розробленій ним концепції розрізнення системи безпеки та системи забезпечення безпеки. Сказане зумовлює необхідність визначити мету функціонування даної системи.

Відсутність системи забезпечення інформаційної безпеки унеможливлює надійне забезпечення не лише інформаційної, а й національної безпеки. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже, основною функцією даної системи є забезпечення збалансованого існування інтересів особи, суспільства і держави в інформаційній сфері.

Система забезпечення інформаційної безпеки України (СЗІБ) створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері. Основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які вживають систему адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління.

Формування СЗІБ має відбуватись за усвідомлення необхідності функціонування механізму балансу інтересів усієї системи державного управління в інформаційній сфері.

Зазначимо, що за роки незалежності в Україні лише закладено основи для формування системи забезпечення інформаційної безпеки. Так, певним чином можна говорити про напрацювання великого масиву нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері[1]. Президентом України вживаються активні заходи щодо вдосконалення системи управління інформаційною сферою. Важливе політико-правове значення мають чинні Укази Президента України "Про деякі заходи щодо захисту держави в інформаційній сфері" (22.04.98); "Про вдосконалення державного управління інформаційною сферою" (16.09.98); "Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади" (14.07.2000); "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі" (31.07.2000); "Про додаткові заходи щодо безперешкодної діяльності засобів масової інформації, дальшого утвердження свободи слова в Україні" (09.12.2000); "Про рішення Ради національної безпеки і оборони України від 19 липня 2001 р. "Про заходи щодо захисту національних інтересів у галузі зв'язку та телекомунікацій" (23.08.2001) та ін.

Водночас функціонування даної системи не обмежується лише великим масивом нормативно-правових актів. Відтак не можна констатувати про остаточне створення основних елементів системи забезпечення інформаційної безпеки. І причин тому є багато. Це і не сформованість системи забезпечення національної безпеки, і невизначеність політики національної, а отже, й інформаційної безпеки, і відсутність, врешті-решт, доктрини інформаційної безпеки, яка має розвивати положення Концепції національної безпеки, котра в Україні взагалі відсутня. Згодом недосконалість нормативно-правового регулювання даних процесів негативно впливає і на державне управління у даній сфері.

Нормативно-правові засади побудови, поточної діяльності та розвитку системи забезпечення інформаційної безпеки України на сьогодні складають: Консти-

[1] Закон України "Про інформацію" // Відомості Верховної Ради України.– 1992.– № 48.– Ст. 650.; Закон України "Про електронні документи та електронний документообіг" // Відомості Верховної Ради України.– 2003.– № 36.– Ст. 275.; Указ Президента України від 06.12.2001 № 1193/2001 "Про рішення Ради національної безпеки і оборони України" від 31 жовтня 2001 р. з питання "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки".; Закон України "Про електронний цифровий підпис" // Відомості Верховної Ради України.– 2003.– № 36.– Ст. 276.

туція України, Закон України "Про основи національної безпеки України", інші законодавчі та нормативно-правові акти, що регулюють суспільні відносини в інформаційній сфері. Нормативно-правове підґрунтя має досить розвинений характер, тому що більшість норм відповідають міжнародним стандартам, принципам і нормам забезпечення прав і свобод людини та громадянина, зокрема права на свободу слова, отримання та поширення інформації. Водночас системні проблеми даються взнаки і при вирішенні галузевих проблем, тому не сформованість нормативно-правової бази щодо регулювання суспільних відносин у сфері національної безпеки відповідним чином негативно впливає на можливість формування достатньої і ефективно діючої нормативно-правової бази з питань забезпечення національної безпеки в інформаційній сфері.

У Законі України "Про основи національної безпеки України" визначено дев'ять основних напрямів державної політики національної безпеки в різних сферах життєдіяльності. До однієї з них належить інформаційна, що дає усі підстави стверджувати, що інформаційна безпека є вагомою складовою національної.

У найбільш загальному плані під ***системою забезпечення інформаційної безпеки*** слід розуміти систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення.

**Основами формування** і функціонування системи забезпечення інформаційної безпеки є:

☐ комплексне визначення поняття інформаційної безпеки та її складових елементів, світоглядне і концептуальне закріплення у концепції, доктрині, програмах, планах та інших документах;

☐ формування і діяльність оптимальної структури системи інформаційної безпеки, аналіз функціонування її окремих елементів, організація функціонування даної системи в цілому;

☐ формування єдиного методологічного підходу, а також вироблення і прийняття єдиного цілісного і узгодженого законодавства з питань інформаційної безпеки;

☐ створення чіткого механізму, метою якого було б координування діяльності елементів системи забезпечення інформаційної безпеки на усіх рівнях державного управління;

☐ підготовка і забезпечення найкращими професійними кадрами всіх складових елементів підсистеми інформаційної безпеки.

Відповідно до основ формування можна виокремити основні ***функції системи забезпечення інформаційної безпеки України***.

**1.** Створення та забезпечення діяльності державних і недержавних органів та організацій елементів системи забезпечення інформаційної безпеки, що включає:

• розроблення адміністративно-правових засад для побудови та функціонування системи інформаційної безпеки (доктрини інформаційної безпеки, організаційної та функціональної структури системи);

• системне забезпечення діяльності елементів системи: інформаційне, аналітичне, адміністративно-правове, матеріально-технічне, кадрове, ресурсне забезпечення усієї системи управління національною безпекою.

**2.** Управління системою інформаційної безпеки, здійснення свідомого цілеспрямованого впливу суб'єктом управління на загрози та небезпеки, внутрішні та зовнішні чинники, що впливають на інформаційну безпеку:

• розроблення на підставі доктрини інформаційної безпеки конкретних планів та технологій забезпечення інформаційної безпеки відповідно до потреб кожного рівня соціального управління;

• здійснення прогнозування, планування, організації, регулювання та контролю усією системою інформаційної безпеки та окремими її елементами;

• оцінка результативності дій, витрат на проведення заходів щодо забезпечення інформаційної безпеки.

**3.** Здійснення планової та оперативної діяльності щодо забезпечення інформаційної безпеки:

• визначення інтересів особи, суспільства і держави в інформаційній сфері та їх пріоритетності відповідно до державної інформаційної політики;

• діагностування загроз та небезпек, виявлення джерел їх виникнення, а також прогнозування можливих наслідків у разі настання із відпрацюванням відповідних превентивних заходів.

**4.** Міжнародне співробітництво у сфері інформаційної безпеки:

• розроблення нормативно-правової бази, що регулює інформаційні відносини між державами та їх взаємодію в галузі інформаційної безпеки;

• входження в існуючі та утворення нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на розв'язання проблем інформаційної безпеки з урахуванням національних інтересів України;

• участь у роботі керівних, виконавчих та забезпечуючих підрозділів цих структур (організацій), спільне проведення планових та оперативних заходів.

Необхідним в контексті проблем, що розглядаються, є проведення аналізу змісту та призначення системи забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки досягається у процесі свідомої цілеспрямованої діяльності суб'єктів управління НБ по запобіганню можливого порушення їх нормального функціонування в результаті дії загроз та небезпек.

***Метою забезпечення інформаційної безпеки*** є створення нормальних умов функціонування конкретної системи управління НБ, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки.

Вживаючи термін "система", ми робимо логічний наголос на утворенні нової якості, яку складають загрози та небезпеки, суб'єкти забезпечення інформаційної безпеки. Адже структурна зв'язаність елементів системи забезпечення інформаційної безпеки є істотною її якісною характеристикою, і розрив зв'язків між цими елементами може призвести до зникнення самої системи. Відтак, актуалізується питання забезпечення структурної єдності даної системи.

Так, наприклад, захищеність Кабінету Міністрів України і Міністерства внутрішніх справ України в сукупності не утворять стан захищеності усієї системи інформаційної безпеки системи управління НБ.

***Об'єктами*** системи забезпечення інформаційної безпеки України є:

• інтереси системи управління НБ в інформаційній сфері;

• система управління НБ, а також її структурні компоненти і відносини між ними (суспільні відносини в інформаційній сфері);

• власне система забезпечення інформаційної безпеки України.

### *3.2. Мета функціонування, завдання системи забезпечення інформаційної безпеки*

Визначальним елементом створення будь-якої системи є її мета. Отже очевидним є розгляд даного компоненту і при створенні системи забезпечення інформаційної безпеки України.

***Мета функціонування системи забезпечення інформаційної безпеки*** полягає:

1) в організації управління системою інформаційної безпеки через ефективне функціонування самої системи її забезпечення;

2) у створенні необхідних економічних і соціокультурних умов та правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах життя і діяльності громадянина, суспільства й держави.

Ефективність системи управління національними інформаційними ресурсами та їхнім захистом значною мірою визначає загальний рівень національної безпеки, а будь-які недоліки в структурі й функціонуванні системи управління цими процесами призводять до непоправних збитків суспільству й державі. Наприклад, відомо, що втрати економіки Німеччини від індустріального шпигунства перевищують 20 млрд. євро на рік, втрата торгових і технічних секретів США (за неофіційними даними) обійшлась американським компаніям у 1992 р. в 100 млрд доларів.

Для досягнення поставленої мети на систему забезпечення інформаційної безпеки покладаються певні завдання.

***Головним завданням системи забезпечення інформаційної безпеки України*** є створення умов для організації управління системою інформаційної безпеки.

До основних **завдань** системи забезпечення інформаційної безпеки відносять:

☐ забезпечення інформаційної безпеки усіх складових елементів системи управління НБ;

☐ забезпечення інформаційно-аналітичного потенціалу країни;

☐ реалізація державної політики інформаційної безпеки в рамках реалізації політики національної безпеки;

☐ ведення активної розвідувальної, контррозвідувальної і оперативно-розшукової діяльності з метою забезпечення інформаційної безпеки через здобуття необхідної розвідувальної, контррозвідувальної і оперативно-розшукової інформації для відпрацювання стратегічних, тактичних і оперативних рішень у сфері управління інформаційною безпекою та вироблення механізмів їх реалізації;

☐ виявлення, попередження і припинення розвідувальної та іншої, спрямованої на нанесення шкоди інформаційній безпеці України, діяльності спеціальних служб, а також окремих осіб чи організацій;

☐ виявлення, попередження і припинення інформаційного тероризму та іншої діяльності, спрямованої на підрив функціонування системи управління НБ;

☐ моніторинг (спостереження, оцінка і прогноз) стану інформаційної безпеки у зв'язку із впливом загроз та небезпек як зсередини, так і ззовні системи управління НБ;

☐ протидія технічному проникненню до інформаційних систем об'єктів інформаційної безпеки з метою вчинення злочинів, проведення диверсійно-терористичної та розвідувальної діяльності;

☐ запобігання можливій протиправній та іншій негативній діяльності суб'єктів системи забезпечення національної безпеки зсередини системи їй на шкоду;

☐ забезпечення збереження державної таємниці;

☐ організація демократичного цивільного контролю за функціонуванням системи управління НБ тощо.

Відповідно до окресленої мети і завдань доцільно визначити функції системи забезпечення інформаційної безпеки України.

Під **функціями системи забезпечення інформаційної безпеки** розуміється здійснення суб'єктами системи забезпечення інформаційної безпеки України діяльності зі створення умов для оптимального управління системою інформаційної безпеки.

Зазначимо, що погляди щодо функцій даної системи різняться. Так, на думку *Є.Кравця*, серед основних функцій системи забезпечення інформаційної безпеки в умовах надзвичайної ситуації слід виділити: виявлення і прогнозування загроз життєво важливим інтересам об'єктів інформаційної безпеки, здійснення комплексу оперативних і довгострокових заходів для попередження та нейтралізації загроз; створення та підтримання напоготові сил і засобів забезпечення інформаційної безпеки; управління силами і засобами забезпечення інформаційної безпеки в умовах надзвичайної ситуації; здійснення системи заходів з відновлення нормального функціонування об'єктів інформаційної безпеки у регіонах, які потерпіли внаслідок виникнення надзвичайної ситуації; участь в заходах, покликаних забезпечувати інформаційну безпеку за межами України відповідно до міжнародних договорів та угод, укладених або визнаних українською державою. Аналогічними за своїм змістом є пропоновані функції *В.Ю.Богдановичем*.

Отже, до **основних функцій СЗІБ** можна віднести:

• розробка й прийняття політичних рішень, законодавчих і нормативно-правових актів щодо забезпечення системи управління національними інформаційними ресурсами та удосконалення механізмів реалізації правових норм чинного законодавства;

• визначення і здійснення повноважень системою управління НБ щодо оперативного управління (володіння, розпорядження, користування) державними інформаційними ресурсами;

• розробка і реалізація організаційних заходів і нормативно-методичного забезпечення відомчих і регіональних структур у сфері формування та використання інформаційних ресурсів за умови координації діяльності згаданих структур;

• розробка і реалізація фінансово-економічних засад регулювання процесів формування та використання інформаційних ресурсів;

• здійснення державної реєстрації інформаційних ресурсів, забезпечення повноти створення первинних і похідних інформаційних ресурсів на засадах використання інформації, що виникає (створюється) у процесі діяльності об'єктів інформаційної безпеки;

• введення технологічно та методологічно єдиних засад формування інформаційних ресурсів за результатами діяльності структурних компонентів системи управління НБ (крім інформаційних ресурсів, що мають відомості, віднесені до державної таємниці та до іншої інформації з обмеженим доступом);

• забезпечення ефективного використання інформаційних ресурсів у діяльності об'єктів інформаційної безпеки;

• оптимізація державної політики інформатизації щодо забезпечення науково-технічних, виробничо-технологічних і організаційно-економічних умов створення та застосування інформаційних технологій, інших елементів інформаційної інфраструктури для формування, розвитку і ефективного використання інформаційних ресурсів та сприяння доступу об'єктам інформаційної безпеки до світових інформаційних ресурсів, глобальних інформаційних систем;

• забезпечення функціонування ефективно діючої комплексної системи захисту інформаційних ресурсів системи управління НБ;

• забезпечення захисту системи управління НБ від хибної, спотвореної та недостовірної інформації;

• забезпечення розробки та застосування правових, організаційних і економічних механізмів стосовно форм та засобів обігу інформаційних ресурсів України (ринку інформації, інформаційних технологій, засобів обробки інформації та інформаційних послуг);

• регулювання інформаційного співробітництва, спрямованого на забезпечення рівноправного і взаємовигідного використання національних інформаційних ресурсів у процесі міжнародного обміну, здійснення єдиної державної політики наукової підтримки системи управління формуванням, розвитком і використанням національних інформаційних ресурсів;

• кадрове забезпечення функціонування системи управління НБ національними інформаційними ресурсами;

• організаційно-управлінське та адміністративно-правове забезпечення функціонування системи управління НБ;

• інформаційно-аналітичне забезпечення прийняття управлінських рішень у сфері управління інформаційними ресурсами;

• контроль за встановленим порядком і правилами формування, розвитку і використання інформаційних ресурсів;

• нагляд за додержанням законодавства в сфері формування, розвитку, використання інформаційних ресурсів та здійснення правосуддя у сфері суспільних інформаційних відносин.

У межах окреслених мети, завдань та функцій постає необхідність в окресленні методів і структури системи забезпечення інформаційної безпеки України.

### *3.3. Методи забезпечення інформаційної безпеки*

Діяльність по забезпеченню інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у своїй органічній сукупності і складають **методи**. Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування.

Важливими методами аналізу стану забезпечення інформаційної безпеки є *методи опису і класифікації*. Для здійснення ефективного захисту системи управління НБ слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

В якості розповсюджених методів аналізу рівня забезпечення інформаційної безпеки використовуються *методи дослідження причинних зв'язків*. За допомогою даних методів виявляються причинні зв'язки між загрозами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати такі: метод схожості, метод різності, метод сполучення схожості і різності, метод змін, що супроводжують, метод залишків.

Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то у ній зазвичай виділяють такі рівні:

1) фізичний;
2) програмно-технічний;
3) управлінський;
4) технологічний;
5) рівень користувача;
6) сітьовий;
7) процедурний.

На *фізичному рівні* здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, і управлінських технологій.

На *програмно-технічному* рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні *управління* здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки.

На *технологічному рівні* здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На рівні *користувача* реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища.

На *сітьовому* рівні дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою.

На *процедурному* рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити такі групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Виділяють декілька **типів методів забезпечення інформаційної безпеки**:

• *однорівневі методи* будуються на підставі одного принципу управління інформаційною безпекою;

• *багаторівневі методи* будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує для вирішення власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;

• *комплексні методи* – це багаторівневі технології, які об'єднані до єдиної системи координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;

• *інтегровані високоінтелектуальні методи* – багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів з організаційним управлінням.

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління загрозами. До таких стадій належать такі: прийняття рішення по визначенню області і контексту інформаційної загрози й складу учасників процесу протидії; ухвалення загальної стратегії і схеми дій в політичній, економічній, соціальній та інших сферах життєдіяльності; забезпечення адекватного сприйняття загрози та небезпеки у більш низьких організаційних ланках системи управління НБ; виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів системи управління: трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.

Специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також цілей, що переслідуються. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю по забезпеченню інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів по нейтралізації інформаційних загроз. Саме суспільство почасти використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози.

Причому, на жаль, слід констатувати, що в нашій країні не на достатньому рівні усвідомлюють небезпеку саме в інформаційній сфері, немає штатних одиниць в органах державного управління інформаційною безпекою, не на достатньому рівні ведеться підготовка відповідних фахівців для системи управління НБ.

Вельми важливим є застосування *аналітичних методів* пізнання і дослідження стану суспільної свідомості в сфері інформаційної безпеки. Наприклад, усвідомлення важливості забезпечення інформаційної безпеки на рівні індивіда, суспільства і організації заважає розповсюджений міф про те, що захист інформації і криптографія – одне й те ж саме. Водночас таке розуміння є наслідком використання застарілих підходів до інформаційної безпеки, коли інформаційна безпеки лише ототожнюються із захистом інформації шляхом її шифрування.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від різних загроз. Отже система має відповідно реагувати і гарантувати ефективну діяльність у цьому напрямі.

Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином конфіденційність інформації, яка забезпечується за допомогою криптографічних методів, не є головною вимогою при проектуванні систем захисту інформації. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них через те, що користувач буде позбавлений можливості своєчасного і швидкого доступу до цих даних та інформації через функціонування механізму захисту. Саме тому забезпечення конфіденційності інформації має відповідати можливості доступу до неї. Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати *доступність і цілісність* інформації, а її конфіденційність – у випадку необхідності.

Втім не слід плекати надію на створення абсолютної системи інформаційної безпеки, тому що, як зазначалося нами вище, ми стоїмо на тій позиції, що загроза та небезпека є атрибутивними компонентами системи інформаційної безпеки, отже їх існування та реалізація, а також негативні наслідки є природним компонентом системи інформаційної безпеки. Саме вони дають змогу побачити недоліки в системі управління інформаційною безпекою і водночас слугують імпульсом до вдосконалення, тобто до розвитку. Отже важливим методом забезпечення інформаційної безпеки *є метод розвитку*.

Захист інформації не обмежується технічними методами. Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. Їх варіативність занадто лабільна і залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторах загроз, алгоритму вирахування коефіцієнта імовірності настання та розміру негативних наслідків. Наявність конкретних даних з цього питання дозволяє достатньо точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек.

Основним методом аналізу інформаційних ризиків *є кількісний ті якісний аналіз, факторний аналіз* та інші. Мета якісної оцінки ризиків – ранжувати інформаційні загрози та небезпеки за різними критеріями, система яких дозволить сформувати ефективну систему впливу на них.

Важливим методом забезпечення інформаційної безпеки є також *метод критичних сценаріїв*. У зазначених сценаріях аналізуються ситуації, коли уявний противник паралізує систему державного управління і відповідно знижує здатність підтримувати державне управління в межах оптимальних параметрів. Причому аналіз подій у світі дає усі підстави стверджувати, що інформаційні війни стають органічною частиною політики національної безпеки багатьох розвинутих країн.

Також можна зазначити на *метод моделювання*, за допомогою якого можна проводити навчання з інформаційної безпеки. Позитивний досвід цього є у США, де на базі однієї з відомих корпорацій постійно проводяться оперативно-дослідницькі навчання, щоб моделювати різні форми інформаційних атак в ході інформаційної війни.

Серед методів забезпечення інформаційної безпеки важливе значення відіграє *метод дихотомії*. Для протидії загрозам інформаційній безпеці вживаються необхідні заходи як у напрямку справляння певного впливу на джерело загрози, так і в напрямку зміцнення об'єкта безпеки. Відповідно виділяють дві предметні області протидії. Одна з них утворюється сукупністю джерел загроз, а інша – сукупністю заходів по забезпеченню інформаційної безпеки об'єкта.

Методи впливу на інформацію у формі повідомлень можна поділити також на *електронні та неелектронні*. Електронні методи впливу застосовуються у тих випадках, коли повідомлення закріплюються на електромагнітних носіях, котрі призначені для оброблення за допомогою засобів обчислювальної техніки. Вони полягають у знищенні, викривленні, копіюванні повідомлень, які зберігаються на цих пристроях. Такі дії можуть бути вчинені лише за допомогою технічного і програмного забезпечення. Неелектронні методи за своєю суттю мають той самий зміст, але реалізуються без використання засобів обчислювальної техніки для впливу на повідомлення, закріплення на інших, передусім паперових, носіях інформації.

Методи впливу на інформаційну інфраструктуру можуть бути розділені на *інформаційні та неінформаційні*. Інформаційні методи впливу орієнтовані на порушення формування інформаційно-телекомунікаційних систем, мереж зв'язку, засобів автоматизації управління, систем автоматизованої обробки інформації і таким чином, на попередження нанесення шкоди предметам суспільних відносин, що захищаються.

У цілому ж слід зазначити, що вибір цілей і методів протидії конкретним загрозам та небезпекам інформаційній безпеці становить собою важливу проблему і складову частину діяльності по реалізації основних напрямів державної політики інформаційної безпеки. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державної влади, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності.

### *3.4. Структура системи забезпечення інформаційної безпеки та компетенція її складових*

Таким чином, з урахуванням викладеного вище щодо поняття системи забезпечення інформаційної безпеки, основ її формування та функціонування, змісту та призначення, мети, завдань, функцій та методів забезпечення, а також з урахуванням напрацювань з даних та інших споріднених питань структура даної системи має такий вигляд:

• **стратегічний рівень** управління інформаційною безпекою – Рада національної безпеки і оборони України та Кабінет Міністрів України;

• **тактичний рівень управління** – центральні органи виконавчої влади.

*Міністерства:*

Міністерство аграрної політики України; Міністерство внутрішніх справ України; Міністерство охорони навколишнього природного середовища України, Міністерство економіки України, Міністерство закордонних справ України, Міністерство культури і туризму України, Міністерство оборони України, Міністерство охорони здоров'я України, Міністерство освіти і науки України, Міністерство у справах молоді та спорту, Міністерство палива та енергетики України, Міністерство вугільної промисловості України, Міністерство будівництва та архітектури України Міністерство праці та соціальної політики України, Міністерство промислової політики України, Міністерство транспорту та зв'язку України, Міністерство України з питань надзвичайних ситуацій, у справах захисту населення від наслідків Чорнобильської катастрофи, Міністерство фінансів України, Міністерство юстиції України;

*Центральні органи виконавчої влади зі спеціальним статусом:*

Державна судова адміністрація України, Головне управління державної служби України, Пенсійний фонд України, Державний комітет статистики України, Державна комісія з цінних паперів та фондового ринку України, Державна служба охорони України, Служба безпеки України, Фонд державного майна України, Національна комісія регулювання електроенергетики України, Державний комітет ядерного регулювання України, Державний комітет України з питань регуляторної політики та підприємництва, Державна податкова адміністрація України, Державна митна служба України, Антимонопольний комітет України, Державний департамент України з питань виконання покарань, Державна прикордонна служба України, Державна комісія з регулювання ринків фінансових послуг України, Державна служба експортного контролю України.

*Державні комітети та інші центральні органи виконавчої влади, статус яких прирівнюється до Державного комітету України:*

Державний комітет України з державного матеріального резерву, Державний комітет архівів України, Державний комітет України з нагляду за охороною праці, Державний комітет України з будівництва та архітектури, Державний комітет України з питань житлово-комунального господарства, Державний комітет України по водному господарству, Державний комітет України по земельних ресурсах,

Державний комітет телебачення і радіомовлення України, Державний комітет лісового господарства України, Державний комітет України у справах національностей та міграції, Державний комітет статистики України, Національне космічне агентство України, Державна служба автомобільних доріг України.

*Інші центральні органи та установи:*

Інформаційний центр Міністерства юстиції України, Головне контрольно-ревізійне управління України, Вища атестаційна комісія, Головне управління реєстрації та ліцензування, Державне казначейство України, Національний інститут стратегічних досліджень, Департамент спеціальних телекомунікаційних систем та захисту інформації, Український державний центр радіочастот, Укравіатранс, Департамент ДАІ МВС України, Центр медичної статистики, Національний олімпійський комітет, Рахункова палата України, Державний департамент продовольства України, Національний Депозитарій України, Експоцентр України, Національний банк України, Рада підприємців України при Кабінеті Міністрів України, Державний департамент інтелектуальної власності, Вища рада юстиції, Державна служба лікарських засобів і виробів медичного призначення.

*Центральні органи виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через відповідних міністрів:*

через Міністра економіки України: Державний комітет України з енергозбереження;

через Міністра праці та соціальної політики України: Державний комітет України у справах ветеранів;

через Міністра транспорту та зв'язку України: Державна служба автомобільних доріг України;

через Міністра фінансів України: Головне контрольно-ревізійне управління України, Державне казначейство України;

через Міністра юстиції України: Державний комітет України у справах релігій.

• **оперативний рівень** – місцеві органи виконавчої влади.

Основним змістом системи забезпечення інформаційної безпеки є реалізація сукупності науковообгрунтованих і апробованих на практиці з урахуванням світового і вітчизняного досвіду заходів у контексті реалізації державної політики інформаційної безпеки.

Суттєвим є той факт, що забезпечення інформаційної безпеки є обов'язковим для усіх інших державних органів і організацій, яке вони здійснюють у межах своєї компетенції самостійно, а також при зверненні основних суб'єктів забезпечення національної безпеки.

Систему забезпечення інформаційної безпеки складає певне коло суб'єктів, які діють відповідно до поставлених завдань і, виконуючи конкретні функції, ґрунтуючись при їх здійсненні визначеними принципами, застосовуючи адекватні методи, утворюють один з вагомих елементів загальної системи національної безпеки.

Розглянемо компетенцію основних складових компонентів системи забезпечення інформаційної безпеки.

*Кабінет Міністрів України* як вищий орган у системі органів виконавчої влади, відповідальний перед Президентом України та підконтрольний і підзвітний

Верховній Раді України у межах, передбачених статтями 85, 87 Конституції України, відповідно до ст. 116 Конституції України, а також ст. 9 Закону України "Про основи національної безпеки України":

• забезпечує інформаційний суверенітет України, здійснення внутрішньої і зовнішньої інформаційної політики держави, виконання Конституції і законів України, актів Президента України, що стосуються інформаційної безпеки;

• вживає заходів щодо забезпечення прав і свобод людини і громадянина в інформаційній сфері;

• забезпечує проведення державної політики інформаційної безпеки;

• спрямовує і координує роботу усієї системи органів державного управління з питань, що стосуються інформаційної безпеки.

Окрім цього, з аналізу нормативно-правової бази, що регулює діяльність Кабінету Міністрів України, можна виокремити інші функції та завдання в сфері інформаційної безпеки, серед яких можна виділити такі:

☐ визначає потреби в витратах на забезпечення інформаційної безпеки, забезпечує виконання затвердженого Верховною Радою України Державного бюджету України щодо фінансування заходів у сфері інформаційної безпеки у визначених обсягах;

☐ організовує розроблення і виконання державних програм з розвитку інформаційної інфраструктури органів державного управління;

☐ здійснює передбачені законодавством заходи щодо формування, розміщення, фінансування та виконання державного оборонного замовлення на поставку (закупівлю) продукції, виконання робіт, надання послуг для потреб органів, що забезпечують інформаційну безпеку;

☐ встановлює порядок надання суб'єктам забезпечення інформаційної безпеки у користування державного майна, засобів зв'язку і радіочастотного ресурсу, комунікацій, інших об'єктів інфраструктури держави, навігаційної, топогеодезичної, метеорологічної, гідрографічної та іншої інформації;

☐ здійснює загальнодержавні заходи щодо забезпечення живучості об'єктів інформаційної інфраструктури;

☐ забезпечує комплектування особовим складом сили забезпечення інформаційної безпеки;

☐ утворює, реорганізовує, ліквідовує науково-дослідні установи, навчальні заклади та окремі кафедри (відділення, факультети) суб'єктів забезпечення інформаційної безпеки;

☐ забезпечує реалізацію права на соціально-економічний захист відповідно до законодавства України, що регламентує діяльність окремих суб'єктів забезпечення інформаційної безпеки;

☐ здійснює у визначених законом випадках регулювання господарської діяльності у суб'єктах забезпечення інформаційної безпеки;

☐ встановлює відповідно до закону порядок реалізації та утилізації об'єктів інформаційної інфраструктури, інформаційних ресурсів;

☐ забезпечує здійснення передбачених законодавством заходів щодо цивільної оборони України, надання військової допомоги іншим державам, направлення

підрозділів Збройних Сил України до інших держав, допуску та умов перебування підрозділів збройних сил інших держав на території України та участі України в міжнародних миротворчих операціях;

☐ контролює виконання законів у сфері оборони, здійснює відповідно до законів інші заходи щодо забезпечення обороноздатності України, координує і контролює їх виконання та несе, в межах своїх повноважень, відповідальність за забезпечення оборони України.

*Міністерства та інші центральні органи виконавчої влади* в межах своїх повноважень, наявних засобів бюджетного і позабюджетного фінансування:

• забезпечують реалізацію законів України, указів та розпоряджень Президента України, концепцій, доктрин, програм, постанов органів державного управління у сфері інформаційної безпеки;

• забезпечують створення, підтримку в готовності і застосування сил та засобів забезпечення інформаційної безпеки, а також управління їх діяльністю;

• у межах своєї компетенції розробляють нормативні правові акти в інформаційній сфері і подають їх Президентові України та Кабінету Міністрів України;

• вносять в органи виконавчої влади пропозиції по удосконалення функціонування системи забезпечення інформаційної безпеки України;

• керують діяльністю підвідомчих організацій по плануванню і проведенню заходів щодо забезпечення інформаційної безпеки;

• забезпечують дотримання прав і законних інтересів громадян, організацій і держави, законів та інших нормативно-правових актів в інформаційній сфері;

• притягують до відповідальності посадових осіб, дії яких призводять до порушення національних інтересів в інформаційній сфері, створюють умови для загрози або безпосередню загрозу інформаційній безпеці України.

Відповідно до ст. 13 Закону України "Про місцеві державні адміністрації" до відання *місцевих державних адміністрацій* у межах і формах, визначених Конституцією і законами України, належить вирішення питань:

1) забезпечення законності, охорони прав, свобод і законних інтересів громадян;

2) соціально-економічного розвитку відповідних територій;

3) бюджету, фінансів та обліку;

4) управління майном, приватизації та підприємництва;

5) промисловості, сільського господарства, будівництва, транспорту і зв'язку;

6) науки, освіти, культури, охорони здоров'я, фізкультури і спорту, сім'ї, жінок, молоді та неповнолітніх;

7) зовнішньоекономічної діяльності;

8) оборонної роботи та мобілізаційної підготовки;

9) соціального захисту, зайнятості населення, праці та заробітної плати.

Причому місцеві державні адміністрації вирішують й інші питання, віднесені законами до їх повноважень.

Цікавим є і той факт, що Кабінет Міністрів України в межах, визначених законами України, може передавати місцевим державним адміністраціям окремі повноваження органів виконавчої влади вищого рівня.

Передача місцевим державним адміністраціям повноважень інших органів супроводжується передачею їм відповідних фінансових, матеріально-технічних та інших ресурсів, необхідних для здійснення цих повноважень.

До безпосередньої компетенції місцевих державних адміністрацій в сфері забезпечення інформаційної безпеки можна віднести:

1) забезпечення виконання Конституції та законів України, рішень Конституційного Суду України, актів Президента України, Кабінету Міністрів України, інших органів державної влади у сфері забезпечення інформаційної безпеки;

2) забезпечення здійснення заходів щодо охорони громадської безпеки, громадського порядку, боротьби зі злочинністю в інформаційній сфері;

3) забезпечення розгляду звернень громадян та їх об'єднань, контроль за станом цієї роботи в органах місцевого самоврядування, на підприємствах, в організаціях і установах, розташованих на відповідній території;

4) здійснення заходів щодо організації правового інформування та інформаційного виховання населення;

5) проведення роботи, пов'язаної з розробленням та здійсненням заходів щодо інформаційного забезпечення біженців, а також депортованих осіб, які добровільно повертаються в регіони їх колишнього проживання;

6) забезпечення виконання законодавства щодо національних меншин і міграції, про свободу думки і слова, свободу світогляду і віросповідання;

7) оголошення у разі стихійного лиха, аварій, катастроф, епідемій, епізоотій, пожеж, інших надзвичайних подій зон надзвичайної ситуації; здійснення передбачених законодавством заходів, пов'язаних із забезпеченням інформаційної безпеки, захистом інформаційних прав особи;

8) здійснення інформаційного супроводження діяльності аварійно-рятувальних служб за місцем їх дислокації, під час прямування до зон надзвичайних ситуацій та під час ліквідації надзвичайних ситуацій, зокрема у наданні їм необхідної інформації, засобів зв'язку та інших матеріальних засобів і послуг;

9) погодження проекту плану проведення потенційно небезпечних заходів в умовах присутності цивільного населення за участю особового складу Збройних Сил України, інших військових формувань та правоохоронних органів з використанням озброєння і військової техніки; взаємодія з органами військового управління під час планування та проведення таких заходів з метою запобігання і недопущення надзвичайних ситуацій та ліквідації їх наслідків;

10) забезпечення своєчасного інформування населення про загрозу виникнення або виникнення надзвичайних ситуацій під час проведення потенційно небезпечних заходів в умовах присутності цивільного населення за участю особового складу Збройних Сил України, інших військових формувань та правоохоронних органів з використанням озброєння і військової техніки;

11) розгляд справ про адміністративні правопорушення, віднесені до відання місцевої державної адміністрації відання, утворення адміністративних та спостережних комісій, координація їх діяльності;

12) здійснення разом з відповідними виконавчими органами рад підготовк і внесення в установленому порядку на розгляд ради пропозицій, погоджених з

відповідними головними управліннями, управліннями Міністерства внутрішніх справ України в Автономній Республіці Крим, областях, містах Києві та Севастополі, щодо утворення, реорганізації або ліквідації місцевої міліції, чисельності її працівників згідно з нормативами, затвердженими Міністерством внутрішніх справ України, витрат на утримання та матеріально-технічне забезпечення діяльності місцевої міліції, навчання її працівників, створення для них необхідних житлово-побутових умов.

Основне завдання по реалізації державної політики у сфері інформаційної безпеки лягає на органи виконавчої влади, які здійснюють на основі законодавства державне управління.

*Компетенція органів виконавчої влади* в сфері забезпечення інформаційної безпеки полягає у виконанні законодавства України, рішень Президента України і Кабінету Міністрів України у зазначеній сфері. Предмети ведення органів виконавчої влади в області забезпечення інформаційної безпеки визначаються Президентом України і Кабінетом Міністрів України. Зміст владних повноважень органів виконавчої влади полягає у тому, щоб приймати в рамках предметів власного ведення відповідні нормативні правові акти, здійснювати правозастосовну практику, готувати пропозиції по реалізації спільно з іншими органами виконавчої влади основних напрямів політики національної безпеки в інформаційній сфері.

*Компетенція міжвідомчих і державних комісій* з різних аспектів забезпечення інформаційної безпеки, які створюються Президентом і Кабінетом Міністрів, полягає передусім у забезпеченні узгодженості діяльності усієї системи органів державного управління. Предмети їх ведення визначаються положеннями про них, а владні повноваження, як правило, обмежуються прийняттям рішень, що носять рекомендаційний характер.

Особливість реалізації функцій забезпечення інформаційної безпеки полягає у тому, що кожний орган держави здійснює власну діяльність на базі використання інформаційної інфраструктури суспільства, виробляє і споживає інформаційні ресурси, має певні відносини з громадянами і як власник інформаційних ресурсів та тих, що складають інформаційну інфраструктуру, має вживати певні дії по забезпеченню збереження ресурсів і безпеки функціонування інформаційних й телекомунікаційних систем, мереж зв'язку, систем управління.

## 4. Державна політика національної безпеки в інформаційній сфері

Відповідно до Закону України "Про основи національної безпеки України" до основних напрямів політики національної безпеки в інформаційній сфері належать:

☐ забезпечення інформаційного суверенітету України;

☐ вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх

технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

☐ активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;

☐ забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

☐ вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Державна політика національної безпеки в інформаційній сфері має створювати умови для реалізації конституційного права громадян своєї держави вільно отримувати і використовувати інформацію для вирішення таких важливих завдань, як формування національного інформаційного простору, включення його до світового інформаційного простору на засадах забезпечення інформаційного суверенітету та інформаційної безпеки і формування демократично орієнтованої свідомості.

Головною **метою державної політики національної безпеки в інформаційній сфері** є створення необхідних економічних і соціокультурних умов та правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах життєдіяльності особи, суспільства і держави як органічного організму.

У цілому ж напрями державної політики мають відповідати загрозам НБ в інформаційній сфері, а також враховувати потенціал системи забезпечення, тобто основні завдання, які вона не тільки зобов'язана, а й може виконувати. Відтак, напрями даної політики можуть також розглядатися крізь призму завдань системи забезпечення інформаційної безпеки, які ми розглядали вище.

Доцільно, з нашої точки зору, прискорити розроблення і прийняття Доктрини інформаційної безпеки України, яка має розвивати положення Концепції національної безпеки України відповідно до інформаційної сфери. Теоретичні питання щодо формування доктрин викладені нами у розділі 3.

Основним призначенням доктрини інформаційної безпеки є закріплення методології і формування єдиної системної мети прийняття усього циклу законодавчих актів у сфері забезпечення інформаційної безпеки. Дані акти мають бути спрямовані на врегулювання суспільних відносин з такого кола ключових питань:

☐ використання інформаційної структури і телекомунікацій;

☐ доступу до інформації;

☐ захисту інформації від несанкціонованого доступу і від її витоку по технічних каналах;

☐ захисту громадян, суспільства і держави від хибної недобросовісної інформації;

☐ захисту інформації телекомунікаційних мереж від неправомірних дій;

□ забезпечення техногенної безпеки, у тому числі в області її інформаційних аспектів і боротьби з технологічним тероризмом.

До основних ***напрямів дій Кабінету Міністрів України*** можна віднести такі:

• розроблення та підписання двосторонніх і багатосторонніх угод у сфері інформаційної безпеки;

• розроблення та організація прийняття Доктрини інформаційної безпеки;

• здійснювати заходи щодо підготовки нормативно-правових актів і удосконалення існуючих, що забезпечують реалізацію законодавства у сфері інформаційної безпеки;

• з метою розвитку і удосконалення системи підготовки кадрів з інформаційної безпеки з України звернутися до Європейської комісії з питань включення даної системи до числа пріоритетних напрямів програми технічної допомоги TACIS.

До основних ***напрямів дій керівників органів виконавчої влади*** можна віднести такі:

• всіляко сприяти проведенню наукових досліджень з проблем забезпечення інформаційної безпеки;

• зосередити увагу на захисті матеріально-технічних об'єктів, які складають фізичну основу інформаційних ресурсів, а також інформаційних технологій;

• забезпечувати нормальне і безперебійне функціонування баз даних і телекомунікаційних систем;

• вживати заходів по захисту інформації від її витоку по технічних каналах, від несанкціонованого доступу, викривлення або знищення;

• виявлення технічних пристроїв та програм, які становлять небезпеку для нормального функціонування інформаційно-телекомунікаційних систем, попередження перехоплення інформації по технічних каналах зв'язку, застосування криптографічних засобів захисту інформації при її зберіганні, обробленні і передачі по каналах зв'язку, контроль за виконанням спеціальних вимог по захисту інформації;

• здійснювати розвиток систем сертифікації засобів інформатизації, програмних продуктів, засобів захисту інформації;

• розвивати та вдосконалювати систему ліцензування діяльності у сфері забезпечення інформаційної безпеки і міжнародного інформаційного обміну;

• здійснювати контроль за діями персоналу в захищених інформаційних системах;

• удосконалювати і розвивати систему підготовки і перепідготовки кадрів у сфері інформаційної безпеки з урахуванням передового міжнародного досвіду;

• завершити формування і удосконалення системи забезпечення інформаційної безпеки, підвищення її дієздатності;

• посилити правозастосовну діяльність органів державної влади, включаючи попередження і припинення правопорушень в інформаційній сфері, а також виявлення, викриття і притягнення до відповідальності осіб, що вчинили злочини або інші правопорушення у цій сфері;

• розробляти, розповсюджувати, використовувати і удосконалювати засоби захисту інформації і методи контролю ефективності цих засобів, розвивати захи-

щені телекомунікаційні системи, підвищувати надійність спеціального програмного забезпечення;

• розроблення і реалізація комплексних цільових програм забезпечення інформаційної безпеки, що стимулюють діяльність у сфері захисту інформації, і визначення порядку фінансування;

• удосконалення системи фінансування робіт, пов'язаних із реалізацією правових і організаційно-технічних методів захисту інформації, створення системи страхування інформаційних ризиків фізичних та юридичних осіб;

• забезпечення технологічної незалежності від зарубіжних виробників у найважливіших сферах інформатизації, телекомунікації та зв'язку.

Перелік напрямів державної політики не є вичерпним, водночас він має відображати реальний рівень інформаційної безпеки, котрий ґрунтується на виявлених і прогнозованих загрозах, а також відповідних заходах по управлінню ними.

## 5. Місце та роль Київського Національного університетувнутрішніх справ у підготовці та перепідготовці фахівців з інформаційної безпеки

Автор даного навчального посібника:

• ураховуючи серйозний як науковий, так і практичний потенціал провідного юридичного закладу України Київського Національного університету внутрішніх справ;

• будучи твердо переконаним і у необхідності побудови системи національної безпеки, складовою якої є система інформаційної безпеки;

• опікуючись проблемами забезпечення інформаційного суверенітету України;

• усвідомлюючи роль України в інформаційній цивілізації;

• дбаючи про надійний захист прав і свобод людини в Україні;

• вважаючи за доцільне організацію фахової підготовки та перепідготовки особового складу із забезпечення інформаційної безпеки,

висловлює пропозицію щодо надання КНУВС ліцензії з підготовки та перепідготовки фахівців у галузі забезпечення інформаційної безпеки.

У контексті наукової глобалізації, руху в напрямі приєднання до конструктивних положень Болонського процесу, утвердження Київського Національного університету як провідного Європейського закладу з підготовки та перепідготовки поліцейських XXI ст, вважаємо за потрібне всіляко сприяти створенню на базі даного закладу Європейського центру по впровадженню інноваційних технологій забезпечення інформаційної безпеки. Для цієї мети має бути розроблений цілий комплекс заходів.

**1.** Утворити загальноуніверситетську кафедру національної безпеки України.

**2.** Розробити на базі даної кафедри спеціальний курс "Інформаційна безпека України". Змістовно даний курс має слідувати після того, як студенти вивчать "Загальну теорію національної безпеки". Структурно даний курс має поділятися на

дві основні частини: загальну і особливу. У загальній частині викладатимуться теоретико-правові питання забезпечення інформаційної безпеки, у особливій – практичні питання забезпечення інформаційної безпеки.

**3.** Окрім даного предмету, стосовно опанування теоретичними знаннями щодо забезпечення національної безпеки в інформаційній сфері доцільно розробити і викладати наступні такі дисципліни: Державна інформаційна політика, Методика інформаційної безпеки, Інформаційне суспільство, Інформаційне протиборство, Управління інформаційної безпекою.

**4.** Необхідно передбачити систему підготовки та перепідготовки посадових осіб органів державного управління, де особливу увагу приділяти розглядові практичних питань удосконалення забезпечення інформаційної безпеки.

**5.** Досить складний та багатоаспектний характер інформаційних процесів вимагає проведення серйозних систематичних наукових досліджень з цієї проблеми. Головними напрямами цих досліджень мають бути:

☐ вивчення інформаційної ситуації в країнах та регіонах, в яких розповсюджена інформаційна інфраструктура, економічних, політичних, соціальних, правових та соціально-психологічних чинників інформаційної діяльності;

☐ з'ясування та аналіз чинників виникнення конфліктних ситуацій (міжнаціонального, релігійного або іншого характеру) як одного із головних чинників ескалації інформаційних загроз;

☐ визначення місця інформаційної безпеки в системі національної безпеки, окреслення її ознак, аналіз складових елементів, відмежування від подібних явищ;

☐ розроблення пропозицій щодо вдосконалення інформаційного законодавства про відповідальність за протиправну інформаційну діяльність;

☐ розроблення теоретико-методологічних засад формування інформаційного права;

☐ розроблення кримінологічної характеристики інформаційної безпеки, аналіз обставин проведення інформаційних операцій (місце, час, характер об'єктів, кількість правопорушників, характер та тактика їхніх дій, технічне обладнання та інші засоби, які використовувалися для здійснення інформаційних атак, встановлення соціальних та психологічних властивостей виявлених учасників здійснених інформаційних операцій, мотивів їхніх дій, аналіз об'єктів інформаційного впливу тощо);

☐ розроблення методики здійснення постійного моніторингу і визначення ситуацій, які є потенційно небезпечними у контексті їх можливого переростання у в інформаційні загрози, а також виявлення осіб, які виявляють схильність до вчинення інформаційних операцій, які загрожують національній безпеці України;

☐ аналіз та узагальнення сучасного досвіду забезпечення інформаційної безпеки, розроблення системи заходів забезпечення інформаційної безпеки;

☐ розроблення теоретичних і практичних проблем забезпечення внутрішньої інформаційної безпеки системи управління національною безпекою;

☐ вироблення економічних та соціальних заходів запобігання конфліктам, які можуть бути причиною проведення інформаційних операцій;

☐ розробка комплексу заходів щодо гармонізації відносин у суспільстві в цілому або в окремому регіоні, вдосконалення інформаційних процедур розв'язання соціальних конфліктів;

☐ вироблення ефективних заходів інформаційної пропаганди;

☐ створення оптимальної системи органів забезпечення інформаційної безпеки, визначення їх правового статусу, професійних вимог, яким мають відповідати працівники цих органів, оптимальної чисельності та процедури підбору, підготовки та перепідготовки;

☐ розроблення моделі системи забезпечення національної безпеки в інформаційній сфері;

☐ дослідження напрямів державної політики національної безпеки в інформаційній сфері;

☐ вивчення ролі недержавних структур в забезпеченні інформаційної безпеки;

☐ дослідження проблем забезпечення енергоінформаційної безпеки;

☐ розробка тактики виявлення, розкриття та розслідування здійснення або підготовки до здійснення інформаційних операцій, що загрожують національній безпеці України;

☐ розробка тактики проведення спеціальних інформаційних операцій по реалізації політики національної безпеки у будь-якій сфері життєдіяльності.

Такі дослідження слід проводити на постійній основі, накопичуючи необхідний матеріал, вдосконалюючи їх методики і якісний рівень. Результати цих досліджень мають впроваджуватися у життя новоствореною структурою (наприклад: Департаментом інформаційного моніторингу), а також іншими суб'єктами забезпечення інформаційної безпеки. В якості базової установи здійснення таких досліджень пропонується визначити Національну академію внутрішніх справ України.

## Висновки

Аналіз проблем забезпечення інформаційної безпеки дав змогу дійти висновку, що найбільш важливими напрямами діяльності у цій галузі є всебічна оцінка загроз та небезпек, національної уразливості, ідентифікація критичної інфраструктури. У процесі забезпечення інформаційної безпеки важливо розуміти характер, природу, сутність і зміст загроз та небезпек, вміти своєчасно ідентифікувати джерело загрози.

Дії, пов'язані зі забезпечення інформаційної безпеки, мають включати:

• спостереження, аналіз, оцінку і прогноз загроз та небезпек, критичної інфраструктури, ступеня національної уразливості;

• відпрацювання стратегії і тактики, планування попередження нападу, зміцнення потенційних зв'язків, вирівнювання ресурсів забезпечення інформаційної безпеки;

• відбір сил і засобів протидії, нейтралізації, недопущення нападу, мінімізації шкоди від нападу;

• дії по забезпеченню інформаційної безпеки;

• управління наслідками інциденту (кібератаки, інформаційні операції, інформаційні війни).

Аналіз стану забезпечення інформаційної безпеки показує необхідність удосконалення системи адміністративно-правового регулювання інформаційної безпеки. Постає потреба у виробленні нових засобів, методів і способів забезпечення інформаційної безпеки державного управління, моніторинг інформаційного середовища, наявності загроз та небезпек.

Удосконалення забезпечення інформаційної безпеки потребує цілеспрямованого вивчення зарубіжного досвіду організації і проведення інформаційних операцій, методів, засобів здійснення кібератак, а також моделювання інформаційних нападів.

Проведений нами аналіз дає можливість стверджувати, що система забезпечення інформаційної безпеки має бути міжвідомчою і ієрархічно організованою. Її структура і організація має відповідати структурі державного управління з чіткою координацією дій окремих сегментів.

Організація ефективної системи забезпечення інформаційної безпеки передбачає централізоване управління із конкретними відомчо-розпорядницькими функціями, які забезпечують моніторинг і контроль за усіма компонентами національного інформаційного простору. Система забезпечення інформаційної безпеки має у будь-яких ситуаціях скоординованої багатобічної і багатоаспектної інформаційної операції володіти здатністю зберігати важливі параметри свого функціонування, тобто підтримувати стан гомеостазису.

У цілому систему забезпечення інформаційної безпеки можна представити такими компонентами:

• концептуальні положення державної політики національної безпеки в інформаційній сфері;

• цілі і завдання як відображення об'єктивних потреб особи, суспільства і держави в реалізації своїх інтересів;

• загрози і небезпеки, уразливість і критична інфраструктура, яка потребує найбільшого захисту;

• ресурси, сили і засоби забезпечення інформаційної безпеки, які створюються відповідно до законодавства України;

• суб'єкти, які забезпечують інформаційну безпеку на державному, регіональному і локальному рівнях;

• дотримання вимог інформаційної безпеки громадянами і суб'єктами України;

• стан інформаційних інфраструктур України і міжнародної спільноти;

• забезпеченість технічної, технологічної, інформаційної незалежності України в інформаційних телекомунікаціях.

Інформаційна безпека України як соціально-політичне явище включає в себе багато окремих складових і є сукупним процесом, який потенційно містить численні загрози та небезпеки, а також шляхи управління ними. Сучасна українська соціально-економічна ситуація, недосконалість організації державної влади і гро-

мадянського суспільства, загострення міжнародних і міжнаціональних проблем створюють широкий спектр внутрішніх і зовнішніх загроз інформаційній безпеці країни. Рівень розвитку і модернізації інформаційного простору визначає статус держави на геополітичній арені, а також необхідні умови для забезпечення її національної безпеки.

Інформаційна безпека – поняття комплексне, а отже, і забезпечена вона може бути лише за допомогою комплексного підходу в світлі бачення проблем забезпечення інформаційної безпеки в якості міждисциплінарних, комплексних і системних.

Управління забезпеченням інформаційної безпеки в цілому є однією з важливих функцій держави. Його сутність полягає в забезпеченні скоординованої національної стратегії на державному, регіональних і локальних рівнях при взаємоузгодженому розподіленні обов'язків, нормативно-правового, інформаційного, морально-психологічного, документаційного і ресурсного забезпечення. З боку держави необхідно постійно здійснювати співставлення загроз та небезпек із наявними ресурсами щодо управління ними. Потрібна всебічна деталізація прав, обов'язків, повноважень і відповідальності усіх складових системи управління національною безпекою. Важливо на додаток до тих функцій, що вже містяться у державному реєстрі, створити нові класифікатори функцій органів виконавчої влади на всіх рівнях системи державного управління стосовно питань забезпечення внутрішньої інформаційної безпеки.

Виняткове значення має зміцнення нормативно-правової бази функціонування інформаційного середовища, діяльності по забезпеченню інформаційної безпеки. Ми дійшли висновку, що динамізм відносин в інформаційній сфері постійно випереджає розвиток суспільної правосвідомості, встановлені регулятори суспільних відносин, ускладнює створення стабільної правової регламентації. Відставання, недосконаліть нормативно-правової бази дозволяє окремим суб'єктам реалізовувати свої протиправні наміри і можливості в інформаційній сфері щодо широкого спектра інтересів інших як суб'єктів, так і об'єктів національної безпеки.

Безперечним є удосконалення нормативно-правової бази забезпечення інформаційної безпеки України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам в інформаційній сфері. При чому важливою є не стільки статика окремих нормативно-правових актів, скільки динаміка доповнень, яка б містила механізми генерації нових рішень, проектів, що дозволяють діяти в темпі, які диктує інформаційне суспільство.

Україна потребує такі нормативно-правові акти, які б упорядкували відносини по формуванню і веденню інформаційних ресурсів державного, регіонального і локального рівнів. Актуальним є нормативне закріплення орієнтації державних і суспільних інформаційних ресурсів на діяльність органів державного управління. Також потребують вирішення проблеми правового регулювання інформаційних технологій, які створюють інфраструктуру інформаційного суспільства, питання інтелектуальної власності в сфері інформаційних відносин. Необхідні нормативно-правові акти, які б регулювали суспільні відносини у сфері обліку та моніторингу в інформаційній сфері.

Слід законодавчо встановити затверджені положення: про обов'язковий склад і основну технічну комплектацію виробничих і корпоративних мереж, які впливають на стан інформаційної безпеки; про обов'язкові вимоги по інформаційній безпеці систем, програмного і апаратного забезпечення; про безпечне ведення бізнесу із використанням нових інформаційних технологій і глобальних інформаційних мереж.

Потребують подальшого вирішення питання щодо розробки комплексу інформаційних стандартів із урахуванням забезпечення інформаційної безпеки, розвиток системи сертифікації інформаційних продуктів, систем і послуг, створення системи ліцензування діяльності організацій по окремих напрямах формування єдиного інформаційного простору України.

Усе це уможливлюється із розробленням і прийняттям Концепції національної безпеки України і відповідно Доктрини інформаційної безпеки як керівного документа для усіх законодавчих актів, що регулюють суспільні відносини в інформаційній сфері.

## Контрольні запитання для самоперевірки

1. Поняття та зміст інформаційної безпеки.
2. Стан правового забезпечення інформаційної безпеки України.
3. Основні загрози національній безпеці в інформаційній сфері на сучасному етапі розвитку України.
4. Зміст системи інформаційної безпеки.
5. Мета та завдання системи забезпечення інформаційної безпеки.
6. Основні напрями державної політики національної безпеки в інформаційній сфері.

## Завдання для самопідготовки

1. Розробити проект Доктрини інформаційної безпеки.
2. Характер та зміст сучасних інформаційних війн.
3. Інформаційні аспекти боротьби з техногенним тероризмом.

# Список рекомендованої літератури

## Нормативні джерела


1. ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".
2. ГОСТ 34.310-95 "Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма".
3. ГОСТ 34.311-95 "Информационная технология. Криптографическая защита информации. Функция хэширования".
4. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва. *Затверджені наказом Держкоммістобудування України від 02.09.96р. № 156.*
5. Декрет Кабінету Міністрів України від 10.05.93 № 46-93 "Про стандартизацію і сертифікацію".
6. Доктрина информационной безопасности Российской Федерации. Утверджена Президентом РФ 09.09.2000. – М., 2000.
7. ДСТУ 1.0-93 Державна система стандартизації України. Основні положення.
8. ДСТУ 1.3-93 Державна система стандартизації України. Порядок розроблення і побудови, викладення та оформлення технічних умов.
9. ДСТУ 1.4-93 Державна система стандартизації України. Стандарти підприємства. Основні положення.
10. ДСТУ 1.5-93 Державна система стандартизації України. Загальні вимоги до побудови. викладу, оформлення та змісту стандартів.
11. ДСТУ 1.6-97 Державна система стандартизації України. Порядок державної реєстрації галузевих стандартів, стандартів науково-технічних та інженерних товариств і спілок.
12. ДСТУ 2296-93 Національний знак відповідності. Форма, розміри, технічні вимоги та правила застосування.
13. ДСТУ 2462-94 Сертифікація. Основні поняття. Терміни та визначення.
14. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. *Затверджено наказом Держстандарту України від 11.10.96 р. № 423.*
15. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. *Затверджено наказом Держстандарту України від 11.04.97р. №200.*
16. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. *Затверджено наказом Держстандарту України від 19.12.96р. № 511.*
17. ДСТУ 3410-96 Система сертифікації УкрСЕПРО. Основні положення.

18. ДСТУ 3412-96 Система сертифікації УкрСЕПРО. Вимоги до випробувальних лабораторій та порядок їх акредитації.
19. ДСТУ 3413-96 Система сертифікації УкрСЕПРО. Порядок проведення сертифікації продукції.
20. ДСТУ 3417-96 Система сертифікації УкрСЕПРО. Процедура визнання результатів сертифікації продукції, що імпортується.
21. ДСТУ 3419-96 Система сертифікації УкрСЕПРО. Сертифікація систем якості. Порядок проведення.
22. Закон України "Про електронні документи та електронний документо обіг" // Відомості Верховної Ради України.– 2003.– № 36.– Ст. 275.
23. Закон України "Про державну таємницю" у редакції Закону від 21.09.99, №1079-XIV. – К., 1999.
24. Закон України "Про електронний цифровий підпис" // Відомості Верховної Ради України.– 2003.– № 36.– Ст. 276.
25. Закон України "Про захист інформації в автоматизованих системах" від - 05.07.94, №80/94 – ВР. – К., 1994.
26. Закон України "Про інформацію" // Відомості Верховної Ради України.– 1992.– № 48.– Ст. 650.
27. Закон України "Про місцеві державні адміністрації" // Відомості Верховної Ради України.– 1999.– № 20 – 21.– Ст. 190.
28. Закон України "Про науково-технічну інформацію" від 25.06.93, №3322 – XII. – К., 1993.
29. Закон України "Про національну програму інформатизації" від 04.02.98, - №74/98 – ВР. – К., 1998.
30. Закон України "Про підприємства" від 27.03.91. З доповненнями від 16.12.93, №3713-XII // Закони України, Т.1.– К., 1996.
31. Звід відомостей, що становлять державну таємницю України, затверджений наказом Державного комітету України з питань державних секретів від 31.07.95 №47 і зареєстрований у Міністерстві юстиції України 03.08.95 за № 278/814.
32. Інструкція про порядок забезпечення режиму безпеки, що повинен бути створений на підприємствах, установах та організаціях, які здійснюють підприємницьку діяльність у галузі криптографічного захисту конфіденційної інформації, що є власністю держави, затверджена наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 22.10.99 № 45 і зареєстрована в Міністерстві юстиції України 29.11.99 за № 817/4110.
33. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, затверджена постано вою Кабінету Міністрів України від 27.11.98 № 1893.
34. Концепція технічного захисту інформації в Україні. *Затверджено постановою Кабінету Міністрів України від 08.10.97р. №1126.*

35. Ліцензійні умови провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівлі криптосистемами і засобами криптографічного захисту інформації, затверджені наказом Державного комітету України з питань регуляторної політики та підприємництва, Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 29.12.2000 №88/66 і зареєстровані в Міністерстві юстиції України 20.01.2001 за №49/5240.
36. Ліцензійні умови провадження господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації. *Затверджено наказом Державного комітету України з питань регуляторної політики та підприємництва, ДСТСЗІ СБ України від 29.12.2000р. № 89/67.*
37. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. *Затверджено наказом ДСТСЗІ СБ України від 28.05.99р. № 26.*
38. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. *Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22.*
39. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. *Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22.*
40. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. *Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53.*
41. НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні технічні вимоги. *Затверджено наказом ДСТСЗІ СБ України від 13.06.2000. № 29.*
42. НД ТЗІ 1.6-001-96 Правила побудови, викладення, оформлення та позначення нормативних документів системи ТЗІ. *Затверджено наказом ДСТЗІ від 26.07.96р. № 51.*
43. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. *Затверджено наказом ДСТЗІ від 09.02.2001р. № 2.*
44. НД ТЗІ 2.3-001-2001 Радіовиявлювачі вимірювальні. Методи та засоби випробувань. *Затверджено наказом ДСТЗІ від 27.02.2001 р. № 5.*
45. НД ТЗІ 2.3-002-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань. *Затверджено наказом ДСТСЗІ СБ України від 06.04.2001р. №11.*

46. НД ТЗІ 2.3-003-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань. *Затверджено наказом ДСТСЗІ СБ України від 06.04.2001р. № 11.*
47. НД ТЗІ 2.3-004-2001 Радіовиявлювачі індикаторні. Методи та засоби випробувань. *Затверджено наказом ДСТСЗІ СБ України від 09.04.2001р. № 12.*
48. НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту. *Затверджено наказом ДСТСЗІ СБ України від 28.05.99р. № 26.*
49. НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту. *Затверджено наказом ДСТСЗІ СБ України від 28.05.99р. № 26.*
50. НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту. *Затверджено наказом ДСТСЗІ СБ України від 28.05.99р. № 26.*
51. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. *Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22.*
52. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. *Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22.*
53. НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки. *Затверджено наказом ДСТСЗІ СБ України від 26.07.99р. № 34.*
54. НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. *Затверджено наказом ДСТСЗІ СБ України від 28.05.99р. № 26.*
55. НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки. *Затверджено наказом ДСТСЗІ СБ України від 26.07.99р. № 34.*
56. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. *Затверджено наказом ДСТСЗІ СБ України від 20.12.2000р. № 60.*
57. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. *Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22.*
58. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова). *Затверджено наказом ДСТСЗІ СБ України від 28.05.99р. № 26.*
59. НД ТЗІ 4.7-001-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наяв-

ності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань. *Затверджено наказом ДСТСЗІ СБ України від 06.04.2001р. №11.*

60. НД ТЗІ Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації. *Затверджено наказом ДСТСЗІ СБ України від 04.09.2000 .№ 41.*
61. Питання Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України: Указ Президента України від 6 жовтня 2000 р. № 1120 // Офіційний вісник України. – 2000. – № 41.
62. Питання забезпечення діяльності Національної системи конфіденційного зв'язку: Указ Президента України від 4 липня 2002 р. № 614 // Офіційний вісник України. – 2002. – № 28.
63. Питання Національного інституту стратегічних досліджень: Указ Президента України від 16 грудня 2002 р. № 1158 // Уряд. кур'єр. – 2002. – 27груд. (№ 243).
64. Положення про державний експортний контроль в Україні, затверджене Указом Президента України від 13.02.98 № 117.
65. Положення про державну експертизу в сфері технічного захисту інформації. *Затверджено наказом ДСТСЗІ СБ України від 29.12.99.№ 62.*
66. Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. *Затверджено постановою Кабінету Міністрів України від 16.02.98р. № 180.*
67. Положення про контроль за функціонуванням системи технічного захисту інформації. *Затверджено наказом ДСТСЗІ СБ України від 22.12.99.№ 61.*
68. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22.05.98 № 505.
69. Положення про порядок контролю за експортом, імпортом і транзитом окремих видів виробів, обладнання, матеріалів, програмного забезпечення і технологій, що можуть використовуватися для створення озброєння, військової чи спеціальної техніки, затверджене постановою Кабінету Міністрів України від 22.08.96 № 1005.
70. Положення про порядок надання суб'єктам зовнішньоекономічної діяльності повноважень на право здійснення експорту, імпорту товарів військового призначення та товарів, які містять відомості, що становлять державну таємницю, затверджене постановою Кабінету Міністрів України від 08.06.98 № 838.
71. Положення про порядок опрацювання, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації. *Затверджено наказом ДСТЗІ від 01.07.96р. № 44.*
72. Положення про порядок проведення експертизи в галузі експортного контролю, затверджене постановою Кабінету Міністрів України від 15.07.97 № 767.
73. Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації, затверджене

наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 30. 11.99 №53 і зареєстроване в Міністерстві юстиції України 15.12.99 за № 868/4161.

74. Положення про технічний захист інформації в Україні. *Затверджено Указом Президента України від 27.09.99р. № 1229.*
75. Порядок видачі сертифікатів затвердження типу засобів вимірювальної техніки, сертифікатів відповідності засобів вимірювальної техніки затвердженому типу та свідоцтв про визнання затвердження типу засобів вимірювальної техніки, затверджений наказом Держстандарту України від 31.01.97 № 56 і зареєстрований у Міністерстві юстиції України 15.04.97 за № 137/1941.
76. Порядок проведення робіт із сертифікації продукції іноземного виробництва, що виготовляється серійно, затверджений наказом Держстандарту України від 18.08.98 №633 і зареєстрований у Міністерстві юстиції України 14.10.98 за № 657/3097.
77. Постанова Кабінету Міністрів України від 14.11.2000 № 1698 "Про затвердження переліку органів ліцензування".
78. Постанова Кабінету Міністрів України від 29.10.2000 № 1755 "Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу".
79. Правила визначення вартості робіт із сертифікації продукції та послуг, затверджені наказом Держстандарту України від 10.03.99 № 100 і зареєстровані в Міністерстві юстиції України 31.03.99 за № 194/3487.
80. Проект Закону України "Про інформаційний суверенітет та інформаційну безпеку України". Внесено на розгляд Верховної Ради України.
81. Проект Інформаційного кодексу України. Перша редакція Проекту на стадії узгодження із зацікавленими державними органами. 2001.
82. Тимчасова інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затверджена спільним наказом Держстандарту України та Служби безпеки України від 28.11.97 № 708/156 і зареєстрована в Міністерстві юстиції України 17.12.97 за №598/2402.
83. Тимчасове положення про категоріювання об'єктів (ТПКО-95). *Затверджено наказом ДСТЗІ від 10.07.95р. № 35.*
84. Тимчасові рекомендації з технічного захисту інформації вид витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ-ПЕМВН-95). *Затверджені наказом ДСТЗІ від 09.06.95р. № 25.*
85. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95). *Затверджені наказом ДСТЗІ від 09.06.95р. № 25.*
86. Указ Президента України від 06.12.2001 № 1193/2001 "Про рішення Ради національної безпеки і оборони України" від 31 жовтня 2001 року з питання "Про заходи щодо вдосконалення державної інформаційної політики".

## Доктринальні джерела


1. An Introduction to Computer Security: The Nist Handbook.Draft. – National Institute of Standart and Technology, Technology Administration U. S. Department of Comerce, 1994.
2. *Аверьянов В.Б.* Функции и организационная структура органов государственного управления.– К.: Наукова думка, 1979.
3. *Азаров Д.С.* Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : Автореф. дис. … канд. юрид. наук: НАН України; Ін-т держави і права ім. В. М. Корецького. – К., 2003 – 18 с.
4. *Айламазян А. К., Стась Е. В.* Информатика и теория развития. – М.: Знание, 1989. – 132 с.
5. Актуальні проблеми інформаційної безпеки України. Аналітична доповідь УЦЕПД / /Національна безпека і оборона. –К., 2001.– №1. – С.2-59.
6. Актуальні проблеми інформаційної безпеки України: аналіт. доп. УЦЕПД) // Нац. безпека і оборона. – 2001. – №1 (13). – С . 2–50.
7. *Алешенков М.С., Родионов Б.Н.* Секьюритология: Монография. – М.: МГУЛ, 2000. С. 72–97.
8. *Андреев В.* Развитие информационного пространства Украины и цивилизованное вхождение в информационное общество XXI века // Техника спец. назначения. – 2002. – № 1-2. – С. 16–17.
9. *Анохин П.К.* Теория функциональной системы // Успехи физиологических наук. – М.: Наука, 1970. – С. 33.
10. *Антимонов С.* Для борьбы с компьютерным терроризмом требуются согласованные и скоординированные усилия разных государств и ведомств // «Безпека інформації в інформаційно-телекомунікаційних системах»: Тези доп. учасників 6-ї Міжнар. наук.-практ. конф. 13-16 трав. 2003 р. – К.: Інтерлінк, 2003. – С.15–16.
11. *Арістова І.В.* Державна інформаційна політика: організаційно-правові аспекти / МВС України, Ун-т внут. справ. За заг. ред. О.М. Бандурки.– Х., 2000. – 366 с.
12. *Аркуша Л.І.* Проблеми взаємодії та інформаційного забезпечення правоохоронних органів у боротьбі з економічною організованою злочинною діяльністю // Информационное обеспечение противодействия организованной преступности: Сб.науч.ст. / Под ред. М. Ф. Орзиха, В. Н. Дремина. – О.: Фенікс, 2003. – С. 109–117. – Библиотека журнала "Юридический вестник".
13. *Атаманчук Г.В.* Новое государство: поиски, иллюзии, возможности. – М.: Славян. диалог,1996. – 223 с.
14. *Афанасьев В. Г.* Социальная информация / Под. ред. Л. Ф. Пирожкова. – М.: Гран, 1994. – 164 с.
15. *Базанов Ю., Баранов О., Брижко В.* Права человека и защита персональных данных. – К.: Госкомитет связи и информатизации Украины, 2000. – 84 с.

16. *Бакуменко В.Д.* Теоретико-методологічні засади формування державно-управлінських рішень: Автореф. дис... д-ра. наук з держ.упр: / Укр. акад. держ. упр. при Президентові України – К., 2001, – 36 с.
17. *Бандурка А.М., Бочарова С.П., Землянская Е.В.* Психология управления. – Х.: ООО "Фортуна-пресс", 1998. – 464 с.
18. *Бандурка А.М., Бочарова С.П., Землянская Е.В.* Основы психологии управления: Учебник. – Харьков: Ун-т внутр. дел, 1999. – 528 с.
19. *Баранов А.* Информационный суверенитет или информационная безопасность ? // Нац. безпека і оборона. – 2001. – № 1 (13). – С.70–76.
20. *Баранов А.* Информационный суверенитет или информационная безопасность? // Національна безпека і оборона. –К., 2001. – С.70–76.
21. *Бачило И. Л.* Правовое регулирование процессов информатизации // Государство и право. – 1994. – № 12. – С.72.
22. *Бачило И. Л., Лопатин В. Н., Федотов М. А.* Информационное право / Под ред. Б. Н. Топорнина. – СПб: Юрид. центр «Пресс». – 2001. – 328 с.
23. Без свободи слова немає демократії // Уряд. кур'єр. – 2001. – 17 січн. – С. 1-2.
24. Безопасность современных информационных систем ДСТСЗИ СБ Украины: Материалы науч.- практ. семинара. – на 2-х компакт-дисках. – К.: НПФ «ЕнранТелеком», 2001–2002.
25. Безпека комп'ютерних систем: злочинність у сфері комп'ютерної інформації та її попередження / За ред. О. П. Снігерьова. – Запоріжжя, 1998. – 316 с.
26. *Белл Д.* Грядущее постиндустриальное общество: Опыт социального прогнозирования / Пер. с англ. В. Иноземцев. – М.: Academia, 1999. – 956 с.
27. *Беляков К.И.* Управление и право в период информатизации: Моногр. – К.: Изд.-во «КВІЦ», 2001. – 308 с.
28. *Березин А.С., Петренко С.А.* Сейф для бизнеса // Защита информации. Конфидент. – 2002. – № 4-5. – С. 132.
29. *Білорус О. Г.* Глобалізація і національна стратегія України.– Броди: Просвіта, 2001. – 299 с.
30. *Білорус О. Г.* Глобалізація і безпека розвитку / [Білорус О. Г., Гончаренко М. О., Зленко В. А. та ін.]: НАН України, Київ. нац. екон. ун-т. – К.: КНЕУ, 2001. – 733 с.
31. *Білоус В. Т.* Координація боротьби з економічною злочинністю : Монографія. – Ірпінь: Акад. держ. податков. служби України, 2002. – 449 с.
32. *Богданович В.Ю.* Роль та місце воєнно-політичної моделі держави у розробленні та здійсненні політики забезпечення її воєнної безпеки // Наука і оборона. – 1999.– №1.– С. 34–37.
33. Большой словарь иностранных слов.– М.: ЮНВЕС, 1998. – С. 520.
34. *Бондаренко В. О., Литвиненко О. В.* Глобальна ідейно-політична гегемонія та становлення нових незалежних держав//Стратегічна панорама.–К., 2000.– №3-4. – С.156–160.

35. *Брижко В.М., Гальченко О.М., Цимбалюк В.С.* і ін. Інформаційне суспільство. Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція. – К.: Інтеграл, 2002. – 220 с.
36. *Брыжко В. М., Орєхов А.А., Гальченко О.Н.* и др. Е-будущее информационное право / Под ред. Р.А. Калюжного, М.Я. Швеца. – К.: Интеграл, 2002. – 264 с.
37. Великий тлумачний словник української мови / Уклад. і голов. ред. В. Т. Бусел. – К., Ірпінь: ВТФ „Перун", 2001. – 1440 с.
38. *Винер Н.* Кибернетика и общество. – М.: Наука, 1958. – 282 с.
39. Виступ на зустрічі з членами Кабінету Міністрів України, Главами обласних, Київської та Севастопольської міських державних адміністрацій 25 черв. 2001 р. // Кучма Л. Україна – європейська держава. – К., 2001. – Т. 2. – С. 348.
40. Виявлення та розслідування злочинів, що вчиняються з використанням комп'ютерних технологій / За ред. Я. Ю. Кондратьєва. – К., 2000. – 64 с.
41. *Гавловський В. Д., Романюк Б. В., Цимбалюк В. С.* Проблеми організації боротьби з правопорушеннями, що вчиняються з використанням сучасних інформаційних технологій // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2001. – № 3. – С.163–169.
42. *Гавловський В. Д., Калюжний Р.А., Крупчан О. Д.* та ін. Інформатизація, право, управління (організаційно-правові питання). – К.: Вид. Дім "Ін-Юре", 2002. –191 с.
43. *Гавловський В. Д., Корочанський О. Е., Цимбалюк В. С.* Проблеми юридичної деліктології в інформаційних відносинах // Бізнес і безпека.– 1998. – № 6. – С. 19-21.
44. *Гавловський В. Д., Романюк Б. В., Цимбалюк В. С.* Про результати вивчення проблем боротьби з правопорушеннями, які вчиняються з використанням комп'ютерних технологій // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2000. - № 2. – С. 122–127.
45. *Гавловський В. Д., Цимбалюк В. С.* Суспільні інформаційні відносини – об'єкт кримінально-правової охорони і захисту: кримінолого-когніто логічні аспекти // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2001. – № 4. – С. 158–167.
46. *Гавловський В. Д., Цимбалюк В.С.* Щодо проблем боротьби із злочинами, що вчиняються з використанням комп'ютерних технологій // Боротьба з контрабандою: проблеми та шляхи їх вирішення.– К., 1998. – С. 148–154.
47. *Гавловський В. І.* ін. Організаційно-правові питання формування державної інформаційної політики в Україні // Наук. вісн. зб. наук. пр. Акад. держ. податков. служби України. – 2002.– № 3. – С. 177–182.
48. *Гавловський В., Гуцалюк М., Калюжний Р.* та ін. Питання концепції реформи інформаційного законодавства України // Правове, нормат. та метрол. забезпечення системи захисту інформації в Україні.– 2000.– № 1 – С. 17–21.

49. *Гавловський В., Гуцалюк М., Калюжний Р.* Інформаційному суспільству України – інформаційне законодавство (щодо питань реформування законодавства у сфері суспільних інформаційних відносин) // Правове, нормат. та метрол. забезпечення системи захисту інформації в Україні. – 2001.– № 2. – С. 7–11.
50. *Гавловський В., Гуцалюк М., Цимбалюк В.* Удосконалення інформаційного законодавства як засіб оптимізації протидії комп'ютерній злочинності // Наук. вісн. Нац. акад.внутр. справ України.– 2001.– № 3. – С. 20–24.
51. *Гавловський В., Калюжний Р., Цимбалюк В.* та ін. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права // Прав., нормат. та метрол. забезпечення системи захисту інформації в Україні. – 2001. – № 4.
52. *Гавловський В., Калюжний Р., Цимбалюк В.С.* та ін. Інформаційне законодавство України: концептуальні основи формування // Право України. – 2001.– № 7. – С. 88–91.
53. *Гавловський В.Д, Голубєв В.О., Цимбалюк В.С.* Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій – Х.: Фоліо, 2002. – 284 с.
54. *Гавловський В.Д., Гуцалюк М.В., Калюжний Р.А.* та ін. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії й практики. – Запоріжжя: Просвіта, 2002. – С.38.
55. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. – 400 с.
56. *Голубєв В. О.* Захист банківської інформації від несанкціонованого доступу // Правове, нормат. та метрол. забезпечення системи захисту інформації в Україні: Матеріали міжнар. наук.-практ. конф. – К., 1998. – С. 50–53.
57. *Голубєв В. О.* Правові аспекти захисту інформаційних технологій // Вісн. Запоріз. юрид. інст-ту МВС України. –1997. – № 2. – С. 35–40.
58. *Голубєв В. О.* Правові аспекти захисту інформації // Правове, нормат. та метрол. забезпечення системи захисту інформації в автоматизованих системах України. – К., 1998. – С. 44.
59. *Голубєв В. О., Гавловський В. Д., Цимбалюк В. С.* Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / За заг. ред. Р.А. Калюжного, М.Я. Швеця. – Запоріжжя: Просвіта, 2001. – 252 с.
60. *Голубєв В.О., Юрченко О.М.* Злочини в сфері комп'ютерної інформації. – Запоріжжя. – 1998. – 157 с.
61. *Гордієнко С. Г.* Забезпечення економічної безпеки України Службою безпеки України // Економічні злочини: попередження і боротьба з ними. – К., 2001. – С.121.
62. *Гриньов С. В.* Война в четвертой сфере: Превосходство в киберпространстве будет определять победу в конфликтах XXI века // Независимое воен. обозрение. – 2000. – № 3. – С. 7–8.

63. *Грушо А. А., Тимонина Е. Е.* Теоретические основы защиты информации. – М.: Изд-во агентства „Яхтсмен", 1996. – 192 с.
64. *Гурковський В. І.* Взаємовідносини органів державної влади у сфері забезпечення інформаційної безпеки України: організаційно-правові питання // Вісн. УАДУ. – 2002. – № 3. – С. 27–32.
65. *Гурковський В. І.* Інформаційна безпека в Україні як складова національної безпеки // Зб. наук. пр. УАДУ – 2002. – № 2. – С. 9–18.
66. *Гурковський В. І.* Принципи міжнародного права у сфері суспільних відносин стосовно інформаційної безпеки // Боротьба з організованою злочинністю і корупцією (теорія і практика) – 2001. – № 4. – С . 187–193.
67. *Гурковський В.І.* Організційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: Дис. ... канд. юрид. наук: 25.00.02 / Нац. Акад. держ. управл. при Президентові України.– К., 2004.– 226 с.
68. *Гуцалюк М. В.* Координація боротьби з комп'ютерною злочинністю // Право України. – 2002.– № 5. – С.121–126.
69. *Гуцалюк М. В.* Протидія комп'ютерній злочинності // Право України. – 2003.– № 6. – С. 114–117.
70. *Гуцалюк М.В.* Протидія міжнародній комп'ютерній злочинності // Вісн. прокуратури.– 2003.– № 9. – С. 60–64.
71. *Девятнин П. Н., Михальский О. О., Правиков Д. И., Щербаков А. Ю.* Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000. – 192 с.
72. *Дешко А. І., Слівак А. Є.* Проблеми організації единого інформаційного простору України // Науково-технічна інформація.– К., 2000.– №3. – С. 14–18.
73. Доктрина информационной безопасности Российской Федерации // Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. М.: Академический Проект; Фонд „Мир", 2003. С. 344.
74. *Зайчик О., Онищенко Н.* Правові системи сучасності та тенденції їх розвитку // Право України. – 2002. – № 11. – С. 23-26.
75. *Землянова Л. М.* Современная американская коммуникативистика: теоретические концепции, проблемы, прогнозы. – М.: Изд-во МГУ, 1995. – 84 с.
76. *Зіма І. І., Ніколаєв І. М.* Інформаційна війна та інформаційна безпека (огляд думок зарубіжних політологів та воєнних спеціалістів) // Наука і оборона. – № 1. – 1998. – С. 56–58.
77. Информационное пространство // Hi-Tech (Панорама высоких технологий). – 2002.– № 9. – С.6.
78. *Ібрагімова І.* Інформаційна політика крізь призму національної безпеки // Зб. наук. пр. УАДУ. – К.: Вид-во УАДУ, 2000. – Вип.1 – С.26–40.
89. Інформатизація та відкритість влади як засоби демократизації суспільства: Матеріали "круглого столу". – К.: Альтпрес, 2003. – 160 с.
80. Інформація буде захищена // Уряд. кур'єр.– 2003.– № 122.– 5 липня. – С.11.
81. *Калюжний Р. А., Цимбалюк В. С.* Координація діяльності органів влади у

боротьбі з організованою кіберзлочинністю // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2002. – № 6. – С. 105–111.

82. *Кара-Мурза С. Г.* Манипуляция сознанием. – К.: Діалектика, 2000. – 448 с.
83. *Карчевський М. В.* Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину): Автореф. дис. ... канд. юрид. наук: 12.00.08 / Нац. юрид. акад. України ім. Я. Мудрого. – Х.; 2003. – 19 с.
84. *Князєв В., Павлов М.* Розвиток муніципального управління в Україні: визначення завдань, практика роботи й форми організації // Вісн. УАДУ. – 2001.– № 2. – С . 51–63.
85. *Кокошин А.А.* О системе стратегического управления в КНР // Вопросы стратегического руководства обороной России. Краткий очерк.– М.: ИПМБ РАН, 2001. С. 36–38.
86. *Колосков В. В.* Проблеми взаємодії правоохоронних органів держав Європи у боротьбі з міжнародним тероризмом на сучасному етапі // Тероризм і національна безпека України: Матеріали міжнар. конф.– К.: Нац. акад. внутр. справ України, 2003. – С. 86-90.
87. *Колосов Ю.П.* Энергоинформационная безопасность // Бизнес и безопасность.– 2003.– № 1.– С. 97–100.
88. Комп'ютерна злочинність: Навч. посіб. / За ред. П.Д. Біленчука, Б.В. Романюка, В.С. Цимбалюка та ін. – К., 2002. – 240 с.
89. Комп'ютерна підтримка прийняття рішень на різних рівнях державного управління: Метод. рекомендації та зб. завдань / Укр.Акад. держ. упр. при Президентові України [Уклад.: В.П.Тронь та ін.]. – К, 1998. – 54 с.
90. *Копылов В. А.* Информационное право. – М.: Юрист, 1997. – 297 с.
91. *Кравець Є.* Національна безпека України: до концепції законодавства // Вісн. АН України.– 1994.– №1.– С. 83–90.
92. *Крупчан О. Д.* Організація виконавчої влади. – К.: Вид-во УАДУ, 2001.– 132 с.
93. *Крусян А. Р.* Взаимодействие органов исполнительной власти и органов местного самоуправления: Дис. ... канд. юрид. наук. 12.00.02. / Одес. гос. юрид. академия. – О., 1999.– 221 с.
94. *Крылов К. Н.* Информация правит миром // Служба безопасности. – 1994. – № 2. – С. 14–17.
95. *Кунц Г., О'Доннел С.* Управление: системный и ситуационный анализ функций управления: Пер. с англ. – М.: Прогресс, 1981. – С.117.
96. *Курило А.П.* К вопросу о проекте концепции законодательного обеспечения информационной безопасности // Компьютерная безопасность: Тез. докл. учасников семинара 15–17 дек. 1992 г. – М., 1993. – С. 3–7.
97. *Лазарев Б. М.* Государственное управление на этапе перестройки. – М . : Юрид. лит., 1988. – С.160.
98. *Лазарєв Г.* Захист інформації в інформаційно-телекомунікаційних системах//Національна безпека і оборона.–К., 2001.–№1. – С. 80–83.
99. *Лисюченко В. П., Плішкін В. М., Цимбалюк В. С.* Управління органами внутрішніх справ.– К., 1996. – С.149.

100. *Литвак О.* М. Державний вплив на злочинність (кримінологічно-правове дослідження). – К.: Юрінком-Інтер. – 277 с.
101. *Литвиненко О. В.* Спеціальні інформаційні операції та пропагандистські кампанії: Моногр. – К., 2000. – 222 с.
102. *Литвиненко О.* Інформація і безпека // Нова політика. – 1998. – № 1. – С. 47.
103. *Литвиненко О., Чукут.С.* Інформаційна політика: Навч.посіб. – К.: Вид-во НАДУ, 2003. – Ч. 2. – 100 с.
104. *Литвиненко О.В.* Проблеми забезпечення інформаційної безпеки в пострадянських країнах ( на прикладі України та Росії): Автореф. дис. ... канд. політ. наук . 23.00.04. – К., 1997 – 18 с.
105. *Литвиненко О.В.* Спеціальні інформаційні операції.– К.: Рада національної безпеки і оборони України; Національний ін-т стратегічних досліджень, 1999.– 163 с.
106. *Ліпкан В.А.* Теоретичні основи та елементи національної безпеки України: Монографія.– К.: Текст, 2003.– С. 333–343.
107. *Логінов О.В.* Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління // Науковий вісник Юридичної академії Міністерства внутрішніх справ: Збірник наукових праць.– 2003.– № 3.– С. 199–204.
108. *Лопатин В.Н.* Информационная безопасность: Человек. Общество. Государство: Санкт-Петербург. ун-т МВД России. – СПб.: Фонд "Университет", 2000. – 426 с.
109. *Лопатин В.Н.* Информационная безопасность в системе государственного управления: Теоретические и организационно-правовые проблемы: Дис. ... канд. юрид. наук: 12.00.02.– СПб., 1997.– 193 с.
110. *Мазур М.* Качественная теория информации. – М.: Прогресс, 1982.– 249 с.
111. *Матвеев М. М.* Взаимодействие представительных и исполнительных органов в системе местного самоуправления: Автореф. дис. ... канд. юрид. наук. 12.00.02. – М., 1992. – 18 с.
112. Національна безпека України 1994 – 1996 рр. / Ред. О.Ф.Белов. – К.: НІСД, 1997. – 200 с.
113. *Нечипоренко В. П.* Информационный капитал научно-технической деятельности // НТИ. – 1998. – Сер.1.– № 11. – С. 2–8.
114. *Нижник В. Н., Ситник Г.П., Білоус В. Т.* Національна безпека України (методологічні аспекти, стан і тенденції розвитку ): Навч. посіб. / За заг.ред. П.В. Мельника, Н.Р. Нижник. – Ірпінь, 2000. – 304 с.
115. *Нижник Н. Р., Машков О.А.* Системний підхід в організації державного управління: Посіб. / За ред. Н. Р. Нижник. – К.: Вид-во УАДУ, 1998. – С. 85.
116. Общая теория национальной безопасности: Учебник / Под общ. ред. А.А.Прохожева.– М.: Изд-во РАГС.– 2002.– 320 с.
117. *Олійник О.В., Соснін О.В.* Правові проблеми регулювання інформаційної діяльності // Стратег. панорама. – 2002. – № 4.– С. 166–174.

118. Оцінка електронної готовності України /Стратегічні рекомендації/ Доповідь у рамках проекту Уряду України / ПРООН – "Інноваційний трамплін: ІКТ задля добробуту України". – К.: Держ. ком. зв'язку та інформатизації України, 2002.– 8 с.
119. *Павлютенкова М.* Информационная война: реальная угроза или современный миф? // Власть. 2001. № 12. С. 19 – 23.
120. *Панов М., Тихий В.* Право людини на безпеку (конституційно-правові аспекти) // Вісн. Конституц. Суду України. – 2000. – № 6. – С. 57.
121. *Перегудов Ф.И., Тарасенко Ф.П.* Введение в системный анализ: Учебное пособие для вузов.– М.: Высш. шк., 1989.– 367 с.
122. *Перепелица Г.* Информационные войны и национальная безопасность // Зеркало недели. – 30 апр. 1999. – № 17 (238).
123. *Поздняков А. И.* Информационная безопасность личности, общества, государства // Воен. мысль. – 1993. – № 10.
124. *Політі А.* Злочинність у сфері інформатики і відмивання грошей // Нові транснаціональні ризики і європейська безпека. – К.: 1997.– С. 22–23.
125. *Почепцов Г.Г.* Национальная безопасность Украины в контексте вопросов и парадоксов // Зеркало недели. – 1997. – 7–14 нояб.
126. *Почепцов Г.Г.* Национальная безопасность стран переходного периода: Учеб.пособие для студентов спец. "Международная информация" / Ин-т содерж.методов обучения. Ин-т междунар. отношений К. Нац. ун-т им. Т. Шевченко.– К., 1996. –134 с.
127. Правовая информатика и кибернетика: Учебник // Под ред. *Н.С.Полевого*. М.: Юрид. лит., 1993.– 528 с.
128. *Расторгуев С.П.* Философия информационной войны. М.: Вузовская книга, 2001. 468 с.
129. *Рибак М. І., Атрохов А. В.* До питання про інформаційні війни // Наука і оборона. – № 2.– 1998. – С. 65–68.
130. *Рогожин М. В.* Организация обратной связи от общества к власти //Інформаційні технології та безпека: Матеріали 3-ї міжнар. конф. 23–27 черв. 2003 р. в м. Партеніт.– К.; 2003.– № 5.– С. 69–73.
131. *Розенфельд Н. А.* Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: Автореф. дис. ... канд. юрид. наук. 12.00.08. – К., 2003. – 17 с.
132. *Скородумов Б., Иванов В.* Стандарты информационной безопасности // www.stcarb.comcor.ru
133. *Скуратівський В.А., Шевченко М.Ф.* Соціальні системи та соціальні методи дослідження: Навч. посіб. – К.: Вид-во УАДУ,1998. –188 с.
134. *Стишенко И.К., Богатырёв А.И.* К вопросу об информационной безопасности // Захист інформації. – 2002. – № 2. – С.4–9.
135. Третейский информационный суд и первые свободные выборы: Сб. норматив. актов и док. / Под общ. ред. Ю.М. Батурина. – М.: Юрид. лит., 1994. –110 с.

136. *Українчук О.В.* Забезпечення національної безпеки в умовах формування в Україні громадянського суспільства та демократичної, правової, соціальної держави: Автореф. дис. ... канд. юрид. наук 12.00.01 / Нац. юрид. акад. України ім. Ярослава Мудрого. – Х., 1994. – 17 с.
137. Україна 2000 і далі: геополітичні пріоритети та сценарії розвитку/Редкол: Бєлов О.Ф.(голова), Гончаренко Н.М., Марченко Б.О. та ін. Монографія. –К.:НІСД, 1999. –384с.
138. *Урсул А.Д.* Природа информации: Филос. очерк. – М.: Мысль, 1968. – 284 с.
139. *Урсул А.Д., Цырдя Ф.Н.* Информационная безопасность. Сущность, содержание и принципы её обеспечения: Материалы конференции. – М., 1999. – С. 1.
140. *Файоль А.* Учение об управлении // Научная организация труда управление.– М.: Экономика, 1965. – С. 362–363
141. *Фатьянов А.А.* Правовое обеспечение безопасности информации: Дис.... д-ра юрид. наук: 12.00.02. М., 1999. – 503 с.
142. *Фомін В. О., Рось А. О.* Сутність і співвідношення понять "інформаційна безпека", "інформаційна війна" та "інформаційна боротьба"//Наука і оборона. – К.,1999.–№4.– С. 23–32.
143. Хроніка вірусної атаки на Укртелеком – Інформац. мережа Інтернет: htth: // www. ukrtel. net.
144. *Цимбалюк В.* Проблеми латентності комп'ютерної злочинності // Правове, нормат. та метрол. забезпечення системи захисту інформації в Україні.– К., 2000.– С. 57–61.
145. *Цыганов В.* Медиа-терроризм.– К.: Нико-Центр, 2004.– 124 с.
146. *Чубукова О.* Правова основа інформатизації суспільства // Право України.– 2000.– № 4. – С. 96–99.
147. Юридична енциклопедія: В 6 т. / Редкол.: Ю.С. Шемшученко (відп. ред.) та ін.– К.: Українська енциклопедія ім. М.П. Бажана, 1998.– Т.1: А-Г.– С. 455.
148. *Юсупов Р. М., Заболотский В. П.* Научно-методологические основы информатизации. – СПб.: Наука, 2000. – С. 438. – 455 с.
149. *Ярочкин В.И.* Информационная безопасность: Учебник для студентов вузов.– М.: Академический Проект. Фонд „Мир", 2003.– 640 с.

## Інтернет ресурси

www.niss.gov.ua
www.pccip.gov
www.korrespondent.net.
www. ukrtel. net.