МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ
ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

«До захисту допущено»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____20__ р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

на тему: **«НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ»**

Студент групи УБДМ-61 Тисячний Богдан Олегович _____
(підпис)

Науковий керівник: к.е.н., доцент Мордас Ірина Василівна _____
(підпис)

Нормоконтроль: к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

Київ – 2020

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

«Затверджую»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____20__ р.

ЗАВДАННЯ
на магістерську атестаційну роботу
студенту Тисячному Богдану Олеговичу

1. Тема роботи: «НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ» затверджена наказом ректора від «___» _____ 20__ р. № __.

2. Термін здачі студентом оформленої роботи: «___» _____ 20__ р.

3. Об’єкт дослідження: інформаційна безпека держави.

4. Предмет дослідження: нормативно-правове забезпечення інформаційної безпеки держави.

5. Мета дослідження: розробка пропозицій щодо покращення системи нормативно-правового забезпечення інформаційної безпеки держави.

6. Перелік питань, які мають бути розроблені:
1. Теоретичні засади забезпечення інформаційної безпеки держави.
2. Нормативно-правова основа забезпечення інформаційної безпеки України.
3. Пропозиції щодо покращення державної політики та нормативно-правового забезпечення у сфері інформаційної безпеки держави.

7. Дата видачі завдання: «___» _____ 20__ р.

Науковий керівник: Мордас І. В.

Завдання прийнято до виконання: Тисячний Б. О.

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

КАЛЕНДАРНИЙ ПЛАН
виконання магістерської атестаційної роботи
студентом Тисячним Богданом Олеговичем

Дата видачі завдання: «__» _____ 20__ р.

№ з/п	Етапи виконання магістерської атестаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2019	
2.	Збір та аналіз літератури.	18.10.2019	
3.	Написання 1-го розділу роботи.	31.10.2019	
4.	Написання 2-го розділу роботи.	14.11.2019	
5.	Написання 3-го розділу роботи.	28.11.2019	
6.	Формулювання висновків за результатами проведеного дослідження.	05.12.2019	
7.	Оформлення роботи.	12.12.2019	
8.	Оформлення презентації.	19.12.2019	
9.	Отримання рецензії на роботу.	26.12.2019	
10.	Захист в ДЕК.	__.01.2020	

Студент групи УБДМ-61 Тисячний Богдан Олегович _____
(підпис)

Науковий керівник: к.е.н., доцент Мордас Ірина Василівна _____
(підпис)

Нормоконтроль: к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

РЕФЕРАТ

Робота містить вступ, три розділи з підрозділами, висновки та список використаних джерел. Загальний обсяг роботи – 96 сторінок.

Об’єкт дослідження – інформаційна безпека держави.

Предмет дослідження – нормативно-правове забезпечення інформаційної безпеки держави.

Мета дослідження – розробка пропозицій щодо покращення системи нормативно-правового забезпечення інформаційної безпеки держави.

У магістерській атестаційній роботі досліджено теоретичні засади забезпечення інформаційної безпеки держави; проаналізовано нормативно-правову основу забезпечення інформаційної безпеки України; розроблено пропозиції щодо покращення державної політики та нормативно-правового забезпечення у сфері інформаційної безпеки держави.

БЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ЗМІСТ

ВСТУП

Актуальність теми. Початок третього тисячоліття – це народження суспільства нового типу – інформаційного, в якому основним стратегічним ресурсом стає інформація. Вплив інформаційних процесів на всі сфери життя суспільства, актуалізує найважливіші питання соціального буття, в тому числі питання інформаційних взаємодій, включаючи боротьбу за інформаційний простір і протидію різного роду інформаційним загрозам.

Інформаційна безпека займає одне з провідних місць у системі забезпечення життєво важливих інтересів усіх країн і, безумовно, України. Це, передусім, зумовлено нагальною потребою створення розвиненого інформаційного середовища українського суспільства, однак саме через таке середовище найчастіше здійснюються загрози національній безпеці.

В сучасних умовах система забезпечення інформаційної безпеки України, яка склалася раніше, явно не відповідає новим принципам забезпечення інформаційної безпеки й не може ефективно протидіяти інформаційним загрозам. Тому в сучасний період розвитку України гостро постало питання визначення пріоритетів у сфері забезпечення інформаційної безпеки й зосередження зусиль на найбільш важливих ділянках потенційних і реальних загроз.

В умовах розширення інформатизації українського суспільства, коли інформація стає товаром і ресурсом розвитку, та нарощування політичної, економічної, воєнної та духовної потужності держави, коли інформаційна сфера безпеки все більше й більше виступає системотворчим чинником усієї багаторівневої системи забезпечення безпеки особи, суспільства і держави, визначення й філософське обґрунтування пріоритетних напрямів суспільної та державної діяльності стосовно забезпечення інформаційної безпеки стає найважливішим теоретичним і практичним завданням.

Важливо підкреслити, що проблемі забезпечення інформаційної безпеки України постійно приділяється особлива увага з боку вчених і

практиків. Однак наукових праць, в яких безпосередньо досліджується інформаційна безпека України, явно недостатньо. У силу цього обрана тема покликана заповнити певну прогалину наукового знання в галузі інформаційної безпеки і його застосування на практиці.

Актуальність цієї роботи полягає в необхідності вирішення проблем забезпечення інформаційної безпеки України. Зокрема, розглядаються питання захисту інформаційного простору України, удосконалення вітчизняного законодавства у сфері управління інформаційною безпекою, зокрема охорони державної таємниці, службової інформації та ін.

Мета і завдання дослідження. Мета роботи – розробка пропозицій щодо покращення системи нормативно-правового забезпечення інформаційної безпеки держави.

Для досягнення цієї мети в роботі необхідно вирішити такі *завдання*:

1. Дослідити теоретичні засади забезпечення інформаційної безпеки держави.

2. Проаналізувати нормативно-правову основу забезпечення інформаційної безпеки України.

3. Розробити пропозиції щодо покращення державної політики та нормативно-правового забезпечення у сфері інформаційної безпеки держави.

Об'єкт дослідження – інформаційна безпека держави.

Предмет дослідження – нормативно-правове забезпечення інформаційної безпеки держави.

Методи дослідження. У роботі були використані загальнонаукові методи пізнання – аналіз, синтез, абстрагування, аналогії, теоретичного узагальнення та ін.

Практичне значення одержаних результатів. Результати роботи можуть бути використані для покращення системи забезпечення інформаційної безпеки держави.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Поняття інформаційної безпеки держави

Інформаційна безпека – це стан захищеності систем обробки і зберігання данних, при якому конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення (у цьому значенні частіше використовують термін «захист інформації» .

Інформаційна безпека держави – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Поняття інформаційної безпеки включає в себе з одного боку забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, а з іншого - контроль за непоширенням таємної інформації, сприяння цілісності суспільства, захисту від негативних інформаційних впливів тощо. Рішення цієї комплексної проблеми дозволить як захистити інтереси суспільства і держави, так і сприяти реалізації права громадян на отримання всебічної та якісної інформації.

Головним стратегічним завданням інформаційної безпеки України є створення потужного національного інформаційного простору, як головного аспекту присутності держави в світовому інформаційному просторі. Крім того, таке завдання включає створення системи протидії інформаційним

загрозам та захист власного інформаційного простору, інформаційної інфраструктури та інформаційних ресурсів держави.

Загалом, завданнями забезпечення інформаційної безпеки держави вважають:

– виявлення, оцінку та прогнозування поведінки джерел загроз інформаційній безпеці, що здійснюється шляхом оперативного моніторингу інформаційної обстановки;

– вироблення, координацію та введення єдиної державної політики у галузі інформаційної безпеки;

– створення та експлуатацію систем забезпечення інформаційної безпеки;

– розробку, координацію та запровадження єдиної державної політики у галузі міжнародних інформаційних відносин, зокрема у напрямку формування іміджу держави.

Забезпечення ІБ держави — згідно з українським законодавством [5], вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

– створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань;

– вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

– розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) по відношенню до небезпечних (дестабілізуючих, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

Проблема ефективного забезпечення безпеки інформації в державі передбачає вирішення таких масштабних задач, як:

– розроблення теоретичних основ забезпечення безпеки інформації;

– створення системи органів, відповідальних за безпеку інформації;

– вирішення проблеми керування захистом інформації і її автоматизації;

– створення нормативно-правової бази, що регламентує рішення всіх задач забезпечення безпеки інформації;

– налагодження виробництва засобів захисту інформації; організація підготовки відповідних фахівців та ін.

Комплекс питань інформаційної безпеки держави включає такі сфери державної діяльності, як:

– захист та обмеження обігу інформації;

– захист інформаційної інфраструктури держави;

– безпека розвитку інформаційної сфери держави; захист національного інформаційного ринку;

– попередження інформаційного тероризму та інформаційної війни.

Отже, система інформаційної безпеки є невід'ємною складовою системи безпеки будь_якої сучасної держави. Проблеми інформаційної безпеки зумовлені особливостями сьогоднішнього етапу розвитку світового науково- технічного прогресу, глобалізацією та інформатизацією. Проте вирішення цих вкрай важливих проблем потребує теоретичної бази та грунтовного нормативно-правового забезпечення, які на даний момент є недосконалими. Відсутність чітко визначеної термінології та єдиних підходів

до трактування понять гальмують вирішення задач в цій галузі і вимагають доопрацювання.

1.2. Структура управління інформаційною безпекою держави

Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. Створення розвиненого і захищеного інформаційного середовища є неодмінною умовою розвитку суспільства та держави. Останнім часом в світі відбуваються якісні зміни у процесах управління, зумовлені інтенсивним впровадженням сучасних інформаційних технологій. Разом з цим посилюється небезпека несанкціонованого втручання в роботу інформаційних систем, і вагомість наслідків такого втручання дуже сильно зросла. Як наслідок, в багатьох країнах все більше уваги приділяється проблемам захисту інформації та пошуків шляхів її вирішення. Країни, які не можуть забезпечити власну інформаційну безпеку, стають неконкурентоспроможними і, як наслідок, не можуть брати участь у боротьбі за розподіл ринків та ресурсів. Можна стверджувати, що зникнення великих держав відбувалося не в останню чергу через неспроможність ефективного управління на власній території та невідповідність інформаційної структури новим умовам існування. Отже, незаперечним є те, що в будь-якій розвиненій країні має існувати система забезпечення інформаційної безпеки, а функції та повноваження відповідних державних органів повинні бути закріплені законодавчо.

Існує два аспекти вивчення інформаційної безпеки в контексті національної безпеки. З одного боку, це самостійний елемент національної безпеки будь-якої країни, а з іншого - інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної і т.д.

Проблема забезпечення інформаційної безпеки України знайшла відображення в законах «Про основи національної безпеки України», «Про концепцію національної програми інформатизації», «Про національну

програму інформатизації», а також у Концепції національної безпеки України. Основними складовими останньої є: національна безпека, національні інтереси, національні цілі, пріоритети і принципи задоволення і захисту національних інтересів, загрози національній безпеці і система національної безпеки. [2, с. 5] Сутність інформаційної безпеки як невід'ємної складової національної безпеки України вперше була зазначена у Законі «Про основи національної безпеки України». Захист інформаційного суверенітету держави тісно пов’язаний із поняттям інформаційної безпеки, що може бути розглянута, як захищеність внутрішньої інформації як такої, тобто захищеність якості інформації, її надійність, захищеність різних галузей інформації від розголошення, а також захищеність інформаційних ресурсів. З іншого боку, інформаційна безпека означає контроль над інформаційними потоками, обмеження використання провокаційної, ворожої суспільної інформації, включаючи контроль над рекламою; захист національного інформаційного простору від зовнішньої інформаційної експансії.

Серед головних складових інформаційної безпеки держави виділяють: обсяг інформаційного продукту, що виробляється в державі і державою; здатність мереж витримувати зростаюче інформаційне навантаження; можливість держави керувати розвитком вироблення та розповсюдження інформації; можливість доступу народонаселення до усіх можливих інформаційних джерел, а також відкритість більшості з них [3].

Аналізуючи дослідження вітчизняних фахівців, головні цілі політики інформаційної безпеки України можна сформулювати таким чином: реалізація конституційних прав громадян, суспільства та держави на інформацію; захист інформаційного суверенітету України, зокрема, національного інформаційного ресурсу та систем формування суспільної свідомості; забезпечення рівня інформаційної достатності для прийняття рішень державним установам, підприємствам та громадянам; належна присутність країни у світовому інформаційному просторі [4, с. 129].

Крім того, розглядаючи актуальність формування, функціонування та безпеки національного інформаційного простору, експерти виділяють наступні цілі [3]:

– зміцнення інформаційної безпеки України, загалом її національної безпеки за рахунок більш ефективного використання національного потенціалу;

– підняття рівня і значення вітчизняного інформаційного продукту та технологій, національних інформаційних ресурсів, розвитку інформаційної інфраструктури України у відповідності до її національних інтересів на засадах державного суверенітету України;

– упорядкування інформаційних відносин у національному інформаційному просторі України, особливо зміна співвідношення розповсюдження в країні вітчизняної та зарубіжної інформаційної продукції та інформаційних технологій на користь вітчизняних;

– державна підтримка вітчизняних суб'єктів національного інформаційного простору, забезпечення інформаційної та духовної, культурної ідентифікації України в міжнародних інформаційних відносинах, піднесення міжнародного авторитету вітчизняного інформаційного продукту та технологій, його виробників.

– необхідність забезпечення інформаційної безпеки зумовлюється, багатьма факторами: потреба забезпечення національної безпеки України в цілому;

– існування загроз інформаційній сфері країни, що можуть завдати значної шкоди загальним національним інтересам;

– можливість впливу за допомогою інформації на свідомість і поведінку людей.

Оскільки національний інформаційний ресурс став одним з головних джерел економічної потужності держави та її суб'єктів, то необхідним є формулювання державних інтересів, факторів і загроз в інформаційній сфері,

аналіз ефективності існуючої системи безпеки та можливостей її удосконалення.

Отже, рішення ключових проблем інформаційної безпеки повинне здійснюватися на основі державної політики, при цьому [6] відповідно до вищеназваних принципів і положень забезпечення інформаційної безпеки держави вимагає рішення наступних ключових проблем:

– розвиток науково-практичних основ інформаційної безпеки, що відповідають сучасній геополітичній ситуації та умовам політичного і соціально-економічного розвитку держави;

– формування законодавчої і нормативно-правової бази забезпечення інформаційної безпеки, у тому числі розробка реєстру інформаційного ресурсу, регламенту інформаційного обміну для органів державної влади, підприємств, нормативного закріплення відповідальності посадових осіб і громадян за дотримання вимог інформаційної безпеки; розробка механізмів реалізації прав громадян на інформацію;

– формування системи інформаційної безпеки, що є складовою частиною загальної системи національної безпеки країни;

– розробка сучасних методів і технічних засобів, що забезпечують комплексне рішення задач захисту інформації;

– розробка критеріїв і методів оцінки ефективності систем і засобів інформаційної безпеки і їх сертифікація;

– дослідження форм і способів цивілізованого впливу держави на формування суспільної свідомості;

– комплексне дослідження діяльності персоналу інформаційних систем, у тому числі методів підвищення мотивації, морально-психологічній стійкості і соціальної захищеності людей, що працюють із секретною і конфіденційною інформацією.

На національному рівні інформаційна безпека держави розглядається як система заходів, спрямованих на недопущення несанкціонованого доступу до інформації, її модифікації та порушення цілісності. Вона включає:

- захист політичних, державних і громадських інтересів;

- захист моральних цінностей;

- заборона інформації, яка містить ідеї агресивної війни, насилля, дискримінації та посягання на права людини.

Серед пріоритетів національних інтересів України, визначених в Законі України «Про національну безпеку України», можна виділити ті, що мають відношення до сфери інформації:

– гарантування конституційних прав і свобод людини і громадянина;

– збереження та зміцнення науково-технологічного потенціалу, утвердження інноваційної моделі розвитку;

– забезпечення розвитку і функціонування української мови як державної в усіх сферах суспільного життя на всій території України, гарантування вільного розвитку, використання і захисту російської, інших мов національних меншин України;

– розвиток духовності, моральних засад, інтелектуального потенціалу Українського народу.

Важливою проблемою інформаційної безпеки, як вже зазначалося, є забезпечення захисту і контролю національного інформаційного простору, а також забезпечення інформації про країну в світовому інформаційному просторі.

Під інформаційним простором розуміється певне середовище, у якому здійснюється формування, збирання, збереження, опрацювання і поширення інформації, і на яке розповсюджується юрисдикція держави. Треба наголосити, що будь-яка інформаційна технологія складається з наступних елементів: створення інформації, її обробка, зберігання та споживання. З огляду на безпеку необхідно забезпечити надійність роботи всіх елементів цієї системи. Розглядаючи проблему в такому ракурсі, можна окреслити основну мету інформаційної діяльності – створення повноцінного відкритого інформаційного простору.

Важливий елемент інформаційного простору – засоби масової інформації. Умови їх функціонування в країні, законодавче забезпечення, стан захищеності журналістів є важливими чинниками для цього сектору інформаційного простору. В країнах, що розвиваються ЗМІ відіграють вирішальну роль для всього суспільства, бо вони дозволяють при відсутності законодавчих засобів стримування маніпулювати суспільною думкою та надавати некоректну інформацію, що є важливим порушенням стану національної інформаційної безпеки. У системі національної оборони дедалі більшого значення набуває інформація, яка заповнює вільний час і формує настрій нації. Такою інформацією і забезпечують суспільство ЗМІ та інші системи формування масової свідомості. Як зазначає Г. Почепцов: «як для тоталітарного, так і для будь-якого іншого сучасного суспільства інформаційна картина світу (уявлення про світ) важливіша, ніж сам реальний світ» [7, с. 43]. Ще більшого значення набуває довгостроковий вплив ЗМІ, який є одним з основних джерел формування системи соціально-політичних настанов та стереотипів. Відсутність відомостей, їх виключно або переважно негативний характер у сучасному світі впливає на зовнішньополітичну і економічну діяльність як держави в цілому, так і на окремих її громадян та їхніх організацій. Саме тому ця проблема набуває загальнодержавного значення, а в разі її нехтування створює загрозу національній безпеці. Саме тому створення належних умов для розширення інформаційної присутності у світовому інформаційному просторі є найважливішим завданням державної політики інформаційної безпеки.

Одним із основних елементів реалізації державної політики в інформаційній сфері є інформаційна інфраструктура, що є невід’ємною частиною стратегічних інформаційних ресурсів і має велике значення для обороноздатності держави і її інформаційного ринку. За Законом України „Про Концепцію національної програми інформатизації» до інформаційної інфраструктури входять: міжнародні та міжміські телекомунікаційні та комп’ютерні мережі; системи інформаційно-аналітичних центрів;

інформаційні ресурси; інформаційні технології; системи науково-дослідних установ з проблем інформатизації; виробництво та обслуговування технічних засобів інформації; система підготовки кваліфікованих фахівців у сфері інформатизації [8].

Інформаційна інфраструктура являє собою єдність наступних компонент: системи виробництва інформаційних продуктів, системи доставки їх до споживача, системи виробництва засобів виробництва інформаційних продуктів та їх доставки, системи виробництва інформаційних технологій, системи накопичення і збереження інформаційного продукту або інформаційного ресурсу, тобто системи сервісного обслуговування елементів інфраструктури і системи підготовки кадрів.

Вдосконалення суспільних відносин великою мірою залежить від розвитку інформаційних ресурсів, які є базовими для створення ефективних моделей державного управління. Отже, цей вид ресурсів є водночас об’єктом управління і предметом діяльності державної влади та її інститутів.

Інформайійні ресурси – це інформаційна інфраструктура та циркулююча в ній продукція інформаційної діяльності, яка дає змогу вирішувати відповідні завдання [9]. Найважливішим при цьому є розуміння того, що дві складові інформаційних ресурсів доповнюють одна одну і не можуть бути використані окремо. Темпи науково-технічного та економічного розвитку країни багато в чому визначаються такими факторами, як доступність та якість інформаційного забезпечення. А рівень забезпеченості нформацією визначає успіх держави і суспільства в цілому. Важливою проблемою є налагодження збирання, аналізу та ефективного використання науково-технічної інформації іноземного походження, тому доступ до неї – одна з критичних умов забезпечення прогресу. Величезне значення в сучасних умовах 94 надається інформаційному забезпеченню політичної діяльності. Наприклад, в нині діючій системі збирання та аналітичної обробки інформації США вирізняються такі три складові:

1) державні інформаційні органи, зокрема розвідувальні органи, установи держдепартаменту, адміністрації Президента, Ради національної безпеки;

2) інформаційні центри «прямої підтримки», зокрема такі установи, як Rand, Військовий університет національної оборони тощо;

3) громадські центри «широкої підтримки», такі, як Центр стратегічних і міжнародних досліджень, Американський підприємницький інститут, Фонд спадщини, Атлантична Рада, Центр з національної політики та ін. [4, с.131].

Перша складова системи забезпечує оперативне керівництво державою, інтереси другої зосереджені на оперативному рівні, а третя здійснює стратегічне планування зовнішньополітичної діяльності. При розгляді проблеми інформаційної безпеки важливим кроком є виділення загроз інформаційній безпеці, а також аналіз захисту від цих загроз.

Загроза інформаційній безпеці – явище, дії негативних чинників або процес, через які соціальні об’єкти інформаційної безпеки частково або повністю втрачають можливість реалізувати свої інтереси в інформаційній сфері; а також, порушується нормальне функціонування, здійснюється руйнація або стримується розвиток технічних об’єктів інформаційної безпеки. Як правило, виділяють такі типи інформаційних загроз: політичні, економічні, суспільні, військові та науково-технічні [1, с. 106].

В політичній сфері це:

– система державного управління;

– системи підготовки прийняття політичних рішень;

– виборчі системи; телекомунікаційні системи спеціального призначення.

В економічній:

– система прийняття рішень;

– банківська інфраструктура;

– управління економічним станом в умовах надзвичайних ситуацій;

– управління державними комунікаціями, які мають економічний характер;

– корпоративні війни і промисловий шпіонаж.

В суспільній:

– загрози для системи формування громадської думки;

– системи ЗМК;

– структури політичних партій, громадських рухів, релігійних організацій;

– структури забезпечення основних прав і свобод людини.

У військовій:

– інформаційні ресурси збройних сил;

– системи управління військами;

– системи постійного контролю і спостереження;

– канали надходження інформації стратегічного, оперативного і розвідувального характеру.

В науково-технічній:

системи накопичення ноу-хау;

– об’єкти інтелектуальної власності;

– структури фундаментальних і прикладних досліджень;

– структури аналізу та прогнозування тенденцій в науково-технічній сфері;

– бази і банки даних конфіденційного характеру.

Закон України «Про національну безпеку України» визначає наступні загрози національним інтересам і національній безпеці України в інформаційній сфері:

– 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 [5].

Вітчизняні експерти [10] як правило, загрози інформаційній безпеці України за своєю загальною спрямованістю, поділяють на такі види:

– загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України;

– загрози інформаційному забезпеченню державної політики України;

– загрози розвиткові вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікацій і зв'язку;

– загрози безпеці інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються. Серед загроз інформаційному забезпеченню державної політики України виділяють наступні: монополізація інформаційного ринку України, його окремих секторів вітчизняними і закордонними інформаційними структурами;

– блокування діяльності державних засобів масової інформації з інформування української і закордонної аудиторій;

– низька ефективність інформаційного забезпечення державної політики України внаслідок дефіциту кваліфікованих кадрів, відсутність системи формування і реалізації державної інформаційної політики.

Загрозами для безпеки інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються, можуть бути:

– протиправні збирання та використання інформації;

– порушення технології обробки інформації;

– впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби;

– розробка і поширення програм, що порушують нормальне функціонування інформаційно-телекомунікаційних систем, зокрема систем захисту інформації;

– знищення, пошкодження, радіоелектронне придушення або руйнування засобів і систем обробки інформації, телекомунікацій і зв'язку;

– вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації;

– компрометація ключів і засобів криптографічного захисту інформації; витік інформації по технічних каналах;

– впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, збереження та передачі інформації, а також у службові приміщення органів державної влади, підприємств, установ і організацій незалежно від форми власності;

– знищення, пошкодження, руйнування або розкрадання машинних та інших носіїв інформації;

– перехоплення інформації в мережах передачі даних і на лініях зв'язку, дешифрування цієї інформації і нав'язування помилкової інформації;

– використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації і зв'язку під час створення й розвитку української інформаційної інфраструктури;

– несанкціонований доступ до інформації, що знаходиться в банках і базах даних; порушення законних обмежень на поширення інформації [10].

Прикладами загроз інформаційній безпеці України, є, зокрема, протизаконна приватизація державних видавництв і поліграфічних комбінатів, свавільний розподіл радіочастот тощо [11]. Найбільш вражаючим є те, що одна з головних загроз інформаційній безпеці лежить в сфері діяльності органів державної влади: невиконанні або неналежному виконанні органами державної влади своїх повноважень у інформаційній сфері. Хоча, відповідно до Конституції України «забезпечення інформаційної безпеки є

однією з найважливіших функцій держави та справою всього Українського народу» [12].

Розглядаючи проблему інформаційних загроз неможливо обминути поняття джерел загроз інформаційній безпеці. Експерти розрізняють внутрішні та зовнішні джерела загроз [13, с. 211].

Під внутрішніми джерелами розуміють відсутність історичного, політичного та соціального досвіду життя у правовій державі, що торкається процесу практичної реалізації конституційних прав та свобод громадян, в тому числі в інформаційній сфері, а також посилення організованої злочинності та збільшення кількості комп'ютерних злочинів, зниження рівня освіченості громадян, що суттєво ускладнює підготовку трудових ресурсів для використання новітніх технологій, в тому числі інформаційних. Недостатню координацію діяльності вищого державного керівництва, органів влади та військових формувань в реалізації єдиної державної політики забезпечення національної безпеки теж можна вважати таким джерелом. До цього слід додати і відставання України від розвинутих країн за рівнем інформаизації органів державної влади, юридично-фінансової сфери, промисловості та побуту громадян.

До зовнішніх джерел належать діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері; політика домінування деяких країн в інформаційній сфері; діяльність міжнародних терористичних груп; розробка концепцій інформаційних війн будь-якими структурами; культурна експансія у відношенні до конкретної країни. В наш час стало очевидним, що під впливом інформації зростає потенційна вразливість суспільних процесів від інформаційного впливу. Інформація стала чинником, здатним призвести до велико-масштабних аварій, військових конфліктів, дезорганізації державного управління тощо.

Розгляд питань інформаційної безпеки дозволяє виділити чотири групи інформаційно-технологічних небезпек для суспільства і держави, зумовлених досягненнями науково-технічного прогресу [14, с. 2].

Перша група пов'язана з інтенсивним розвитком нового вигляду зброї інформаційної, здатної ефективно впливати на психіку людей і інформаційно технологічну інфраструктуру держави. Аналіз сучасних досліджень в цій області дозволяє говорити про ефективність програмування поведінки окремих людей під впливом на комп'ютерні банки даних знань і інформації.

Друга група являє собою новий вигляд соціальних злочинів, оснований на використанні досягнень сучасних інформаційних технологій: махінації з банківськими операціями; комп'ютерне хуліганство; незаконне копіювання технологічних рішень та інше. На думку провідних дослідників в цій області, комп'ютер стає провідним знаряддям злочину.

Третя група виявляється у вигляді електронного контролю за життям, настроєм, планами громадян, роботою політичних організацій, тотального комп'ютерного контролю за населенням країни. Інформаційні технології дозволяють накопичувати, зберігати і використовувати величезні масиви 96 даних про здоров’я, соціальну активність, політичні думки, зв'язки, фінансові справи населення.

Четверта група полягає у використанні інформаційних технологій в політичній боротьбі. Зростання впливу засобів масової інформації на хід і зміст політичних процесів, функціонування механізму влади - одна з домінуючих тенденцій сучасного суспільного розвитку. Перейдемо до розгляду питання, які ж засоби використовуються для захисту інформації від вищенаведених загроз.

Кожній із загроз безпеці в різних сферах інформаційного життя можна поставити у відповідність певні напрями, методи і заходи із забезпечення інформаційної безпеки. Так, Закон України «Про національну безпеку України» серед основних напрямів державної політики з питань національної безпеки в інформаційній сфері виділяє:

– 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 [5].

Враховуючи цілі та завдання політики інформаційної безпеки України, як правило, виділяють такі основні напрями забезпечення інформаційної безпеки: забезпечення інформаційної достатності для прийняття рішень; захист інформації, тобто захист інформаційного ресурсу; захист та контроль національного інформаційного простору, тобто систем формування масової свідомості; присутність у світовому інформаційному просторі.

Головним завданням заходів із забезпечення інформаційної безпеки є мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації [15].

Загалом, основні напрямки діяльності по забезпеченню інформаційної безпеки держави являють собою величезний комплекс заходів, до яких відносяться:

– розвиток науково-практичних основ інформаційної безпеки;

– розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки;

– розробка нормативно-правових і організаційно-методичних документів; розробка концепції інформаційної безпеки, спеціальних правових і організаційних заходів, що забезпечують збереження і розвиток інформаційних ресурсів;

– формування правового статусу суб'єктів системи інформаційної безпеки; розробка законодавчих і нормативних актів, що регулюють порядок ліквідації наслідків загроз інформаційній безпеці;

– відновлення порушеного права і ресурсів, реалізації компенсаційних мір; вдосконалення організації форм і методів запобігання і нейтралізації загроз інформаційній безпеці;

– розвиток сучасних методів забезпечення інформаційної безпеки [6].

Розвиток науково-практичних основ інформаційної безпеки включає в себе:

– розробку стратегії забезпечення інформаційної безпеки країни;

– обґрунтування державної політики в умовах глобалізації інформаційних процесів, формування світових інформаційних мереж, прагнення деяких країн до домінування в розвитку і використанні світового інформаційного простору;

– розробку науковопрактичних основ формування і проведення державної політики в області забезпечення інформаційної безпеки;

– обґрунтування пріоритетів національної безпеки, що відповідають довгостроковим інтересам суспільного розвитку.

Розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки означає визначення порядку розробки законодавчих і нормативно-правових актів, а також механізмів практичної реалізації прийнятого законодавства.

Розробка нормативно-правових і організаційно-методичних документів включає розробку документів, що регламентують:

– діяльність в області інформаційної безпеки органів державної влади;

– взаємини суб'єктів інформаційної діяльності для забезпечення інформаційної безпеки;

– регулювання державою процесів функціонування і розвитку ринку засобів інформації, інформаційних продуктів і послуг;

– інформаційні відносини в суспільстві і державі в умовах ринкової економіки тощо.

Під розвитком сучасних методів забезпечення інформаційної безпеки мається на увазі:

– розробка форм і способів цивілізованого впливу держави на формування суспільної свідомості і практичних рекомендацій з реалізації їх на практиці;

– розробка методів комплексного дослідження діяльності персоналу інформаційних систем, у тому числі методів підвищення мотивації, морально-психологічній стійкості і соціальної захищеності людей, що працюють із секретною і конфіденційною інформацією;

– розробка практичних рекомендацій зі збереження і зміцнення політичної стабільності в суспільстві;

– забезпеченню прав і свобод громадян;

– зміцненню законності і правопорядку методами інформаційної безпеки;

– формування шляхів і способів забезпечення органів державної влади, підприємств і громадян достовірною, повною і своєчасною інформацією;

– розробка основних напрямків діяльності із запобігання негативних інформаційних впливів на індивідуальну, групову і суспільну свідомість;

– розробка цивілізованих, демократичних форм і методів впливу на засоби масової інформації;

– розробка механізмів розвитку інформаційних відносин у сфері підприємництва і включення інформаційного ресурсу у господарські відношення;

– дослідження основних шляхів послаблення криміногенної обстановки, зниження числа комп'ютерних злочинів, у першу чергу у кредитно-фінансовій сфері;

– розробка методів і практичних рекомендацій із контролю над експортом вітчизняних наукомістких технологій; обґрунтування напрямків протидії інформаційній зброї;

– удосконалення способів контролю за персоналом у захищених інформаційних системах.

Серед основних напрямків державної політики в сфері інформатизації виділяють: забезпечення умов для розвитку і захисту всіх форм власності на інформаційні ресурси; формування і захист державних інформаційних ресурсів; створення і розвиток федеральних і регіональних інформаційних систем і мереж, забезпечення їхньої сумісності і взаємодії в єдиному інформаційному просторі; створення умов для якісного й ефективного інформаційного забезпечення громадян, органів державної влади, організацій і суспільних об'єднань на основі державних інформаційних ресурсів; забезпечення національної безпеки в сфері інформатизації, а також забезпечення реалізації прав громадян, організацій в умовах інформатизації; сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій, засобів їхнього забезпечення; формування і здійснення єдиної науково-технічної і промислової політики в сфері інформатизації з обліком сучасного світового рівня розвитку інформаційних технологій; підтримка проектів і програм інформатизації; створення й удосконалювання системи залучення інвестицій і механізму стимулювання розробки і реалізації проектів інформатизації; розвиток законодавства в сфері інформаційних процесів, інформатизації і захисту інформації [6].

Існує багато різних засобів несанкціонованого доступу до інформації. Під захистом інформації від несанкціонованого доступу розуміють діяльність із запобігання одержання інформації, яка захищається, зацікавленим суб'єктом з порушенням установлених правовими документами чи власником інформації прав чи правил доступу до інформації, що захищається. Під системою захисту інформації 98 зазвичай розуміють сукупність органів і виконавців, техніку захисту інформації, а також об'єкти захисту, організовані і функціонуючі за правилами, установленими відповідними правовими, організаційно-розпорядницькими і нормативними документами про захист інформації.

1.3. Особливості нормативно-правового забезпечення в сфері інформаційної безпеки

Інституціоналізація – процес визначення і закріплення соціальних норм, правил, статусів і ролей, приведення їх в систему, здатну діяти у напрямі задоволення деякої суспільної потреби. Процес законодавчої інституалізації передбачає певне унормування організаційного і правового поля. В цьому контексті набуває актуальності аналіз стану та інноваційних зрушень в законодавчому забезпеченні інформаційної безпеки в Україні.

Серед сучасних доробок стосовно проблем функціонування суспільних інститутів, а також можливості використання інституціонального підходу в дослідженні державного управління можна виділити роботи таких вчених, як О. Оболенський, В.В.Цвєтков, О. Лазор, О. Бєляєв, В. Дементьєв, І. Кох, Л. Кирилов та ін.

Інституціональний підхід виник ще на початку XX ст. у США. Тоді зародився класичний інституціоналізм як новий підхід до аналізу економічних процесів. Його основоположником вважається Т. Веблен, а послідовниками інституціоналізму стали Дж. Гелбрейт, Р. Коуз, Д. Норт та ін.

Представники зазначеного підходу вважали, що поведінка «економічної людини» формується головним чином у рамках, і під впливом соціальних груп та колективів.

Взагалі, інституціоналізм – це напрям соціально-економічних досліджень, в основі якого лежать два аспекти – «інституції» – норми, звичаї поведінки в суспільстві, та «інститути» – закріплення норм та звичаїв у вигляді законів, організацій, установ. Але ці визначення досить вузькі і неповні.

Можемо погодимося з А. Туреном, що інституція сьогодні має позначати не те, що було інституційовано, а те, що є джерелом інституціювання, тобто, ті механізми, завдяки яким культурні орієнтири трансформуються в соціальну практику [10].

Поняття «інститут» (від лат. institutum – установлення, установа) запозичене з юриспруденції. Інститут – це усталена форма організації, регулювання та впорядкування суспільного життя, діяльності і поведінки людей, яка включає сукупність соціальних норм, зразків поведінки і діяльності, у праві – сукупність норм права, які регулюють будь-які визначені відносини [8].

Д. Норт, наприклад, в своїх працях виділяє інститути (як норми і правила) та організації (як інститути). «Інститути, за визначенням Д. Норта, створюють базові структури, за допомогою яких люди протягом всієї історії добилися порядку і таким чином знизили ступінь своєї невпевненості». Інститути за Д. Нортом – це «правила гри» в суспільстві, або створені людиною рамки обмеження, які організовують відношення між людьми [5, С.17]. У складі інститутів Д. Норт виділяє три головні елементи:

– формальні правила (закони, конституції, норми права тощо);

– неформальні обмеження (звичаї, традиції, домовленості, угоди тощо);

– механізми примусу, які забезпечують дотримання правил (правоохоронні органи, суди тощо).

Науковець А.Шастітко визначає інститут як «ряд правил, які виконують функцію обмежень поведінки економічних агентів і впорядковує взаємодію між ними, а також відповідні механізми контролю за дотриманням цих правил» [11, С.554]. Таким чином, кожен інститут має зовнішній механізм примусу, створений людьми, для виконання визначених «базових» правил в рамках інституту.

Отже, в широкому сенсі, інститут – це сформоване системне високоорганізоване утворення, яке об'єднує діяльність людей для досягнення певної суспільної мети (суб'єктний підхід). В вузькому сенсі, інститут – це сукупність ідей, правил, норм, механізмів, які формують та розвивають певну організацію (об'єктний підхід).

Поняття «інституціоналізація» в різних сферах діяльності вживається, як правило, для характеристики процесів упорядкування цієї діяльності через формування та закріплення відповідних інститутів, при чому сам інститут неперервно розвивається на фоні цих інституціональних змін.

За визначенням Н.Ільченко [2, с. 3], під інституціоналізацією варто розуміти становлення нових інститутів, правове та організаційне закріплення тих чи інших суспільних відносин. А інституціональний підхід доцільно трактувати як методологію наукового пізнання та практичної діяльності, яка розглядає механізми взаємодії та зв'язки суб'єктів суспільних відносин, оцінює їх поведінку у виконанні норм (формальних і неформальних) і дає оцінку ефективності структур (інститутів).

Дослідження та аналіз законодавства в сфері забезпечення інформаційної безпеки України дозволяє зробити висновок про те, що законодавство в сфері забезпечення інформаційної безпеки України перебуває на етапі формування та становлення. На цьому етапі дані процеси характеризуються значною кількістю прогалин і колізій. Одним із напрямів виходу з цієї ситуації, на нашу думку, є проведення систематизації адміністративного права, насамперед, шляхом його кодифікації. Відсутність системності в підходах до кодифікації інформаційного законодавства є

однією з важливих проблем реформування законодавства в сфері забезпечення інформаційної безпеки України. В той же час, варто зазначити, що формування нових суспільних відносин в інформаційному суспільстві передбачає створення відповідного комплексу правового забезпечення. В усьому світі ведеться робота над реформуванням (удосконаленням) чинного законодавства, розробленням нових нормативно-правових актів у сфері регулювання інформаційних відносин і забезпечення інформаційної безпеки держави. Усі елементи суспільного життя, пов'язані із забезпеченням інформаційної безпеки України, мають бути достатньо врегульовані чітко встановленими правилами поведінки (законодавством).

Отже, інституціоналізація на сьогоднішній день – основний соціальний механізм побудови і функціонування системи економічної безпеки. Формування інституційного середовища управління економічною безпекою є основною стратегією досягнення стабільності в будь-якому суспільстві. При цьому виділяється той факт, що інституційна система суспільства, обслуговуючи весь комплекс суспільних відносин, – це форма реалізації системи суспільних інтересів. Ефективна інституційна система, реалізуючи громадські інтереси, організовує та гармонізує їх у напрямку забезпечення національних інтересів вищого порядку, завдяки чому досягається ефективність усього суспільного розвитку країни та її повний та всебічний (тобто достатній) захист.

Висновки до першого розділу

Поняття інформаційної безпеки включає в себе з одного боку забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, а з іншого - контроль за непоширенням таємної інформації, сприяння цілісності суспільства, захисту від негативних інформаційних впливів.

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) по відношенню до небезпечних (дестабілізуючих, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

РОЗДІЛ 2. НОРМАТИВНО-ПРАВОВА ОСНОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Нормативні акти, які закріплюють концептуальні положення інформаційної безпеки України

Під час створення сучасної та ефективної системи забезпечення інформаційної безпеки істотного значення набуває наявність відповідної нормативно-правової бази, без якої неможливо охопити усі сфери життєдіяльності суспільства в рамках єдиного правового поля, розробити загальнонаціональну концепцію розвитку держави й ефективно реалізовувати політику національної безпеки в інформаційній сфері. Це означає, що всі без винятку дії щодо захисту й реалізації національних інтересів України в будь-якій сфері й на будь-якому рівні мають передусім спиратися на чинне законодавство України, підтверджувати законність функціонування системи національної безпеки. Водночас у демократичному суспільстві такі дії суб'єктів забезпечення національної безпеки повинні відповідати національному законодавству, а також загальновизнаним міжнародно-правовим нормам та бути під контролем громадськості.

З огляду на викладене законність функціонування є однією з головних вимог до системи забезпечення інформаційної безпеки. Ця законність повинна базуватися на сукупності законів і підзаконних нормативних актів, які спрямовані на створення необхідних умов для захисту національних інтересів в інформаційній та інших сферах життя країни.

Так, зокрема, наявність необхідної та достатньої нормативної бази і механізмів її реалізації та контролю дозволяє системі забезпечення національної безпеки України ефективно функціонувати в сучасних умовах.

Нормативна база інформаційної безпеки повинна виконувати в першу чергу три основні функції:

1. Регулювати взаємовідносини між суб'єктами інформаційної безпеки, визначати їх права, обов'язки та відповідальність.

2. Нормативно забезпечувати дії суб'єктів інформаційної безпеки на всіх рівнях, а саме - людини, суспільства, держави.

3. Встановлювати порядок застосування різних сил і засобів забезпечення інформаційної безпеки.

Найбільш актуальним завданням у сфері забезпечення інформаційної безпеки держави на сьогодні є формування відповідних положень національного інформаційного законодавства щодо правового забезпечення діяльності в інформаційній сфері відповідних суб'єктів, у першу чергу державних органів, на які державою покладено виконання пов'язаних з цим функцій.

За роки незалежності в Україні закладено законодавчі основи системи забезпечення інформаційної безпеки, зокрема було напрацьовано великий масив нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері. Акти національного законодавства, які регламентують діяльність державних органів, організацій і громадян в інформаційній сфері, встановлюють повноваження державних органів щодо забезпечення інформаційної безпеки України.

З огляду на викладене нормативну базу щодо забезпечення національної безпеки України в інформаційній сфері доцільно розглядати з урахуванням існуючої ієрархії нормативних актів. На найвищому рівні ми розглянемо норми Конституції України, які закріплюють концептуальні положення національної безпеки України в усіх сферах її існування, а також Концепцію національної безпеки України, Доктрину інформаційної безпеки України та Закон України "Про національну безпеку України". Ці документи враховують основні положення міжнародних договорів і угод, ратифікованих Україною, які стосуються її національної безпеки.

На Другому рівні розглянемо закони конститутивного напрямку, де визначаються важливі положення щодо забезпечення національної безпеки в

інформаційній сфері ("Про Основні засади розвитку інформаційного суспільства в Україні", "Про інформацію", "Про державну таємницю", "Про Національну програму інформатизації", "Про Концепцію Національної програми інформатизації", "Про радіочастотний ресурс", "Про телекомунікації", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про захист суспільної моралі").

На третьому рівні - закони України інституційного рівня, де закріплені основні форми діяльності державних органів у процесі забезпечення національної безпеки в інформаційній та інших сферах життєдіяльності особи, суспільства та держави (зокрема "Про оборону України", "Про Збройні Сили України", "Про Службу безпеки України", "Про Державну службу спеціального зв'язку та захисту інформації", "Про міліцію", "Про прокуратуру", "Про надзвичайний стан" тощо).

У структурі нормативно-правової бази забезпечення національної безпеки України в інформаційній сфері особливе місце посідають укази та розпорядження Президента України, а також акти (постанови, декрети) Кабінету Міністрів України. Ці нормативні акти є незаконними й видаються з метою конкретизації та підвищення якості вирішення завдань забезпечення інформаційної безпеки.

Міністерства й відомства України в межах визначеної законами компетенції та відповідальності на основі чинного законодавства про національну безпеку України, а також згідно з рішеннями Президента України, Кабінету Міністрів України розробляють відомчі накази, інструкції, положення, які спрямовані на реалізацію програм захисту життєво важливих інтересів людини, суспільства, держави в інформаційній сфері.

Важливу роль у системі законодавства України з питань національної безпеки відіграють акти нормативного і директивного характеру місцевих органів влади - рішення з питань забезпечення національної безпеки (про боротьбу з наслідками стихійних лих, техногенних аварій і катастроф, з епідеміями, про підтримання громадського порядку тощо), які є

обов'язковими для виконання всіма підприємствами, установами й організаціями, а також посадовими особами і громадянами на території, підпорядкованій цьому органу влади.

Значним кроком на шляху створення системи нормативно-правового регулювання забезпечення інформаційної безпеки України стало прийняття Верховною Радою України Конституції України від 28 червня 1996 р. В ній, зокрема, є норми, що стосуються забезпечення інформаційної безпеки України та які є визначальними для побудови національної системи інформаційної безпеки (статті 1-8; 15; 18; 19; 34; 78; пункти 2 і 9 ч. 1 ст. 85; пункти 19-20 ч. 1 ст. 106; ст. 182; пункти 7 і 10 ст. 138).

Так, зокрема, у ч. 1 ст. 17 Конституції України забезпечення інформаційної безпеки України оголошено "справою всього українського народу". При цьому з точки зору захисту прав людини і громадянина в інформаційній сфері найбільш знаковою є ст. 34 Конституції. Відповідно до цієї статті кожному гарантується " право на свободу думки й слова, на свободу вираження своїх поглядів і переконань", а також "право вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або іншим способом за своїм вибором ".

Реалізацію гарантованих ст. 34 Конституції України прав може бути "обмежено законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою попередження заворушень або злочинів, для охорони здоров'я населення, для захисту репутації або прав інших людей, для попередження розголошення інформації, отриманої конфіденційно, або для підтримки авторитету й неупередженості правосуддя". Як видно, коло обмежень досить широке, однак кожне з них повинне бути визначене законом.

У статті 107 Основного Закону закріплено законність функціонування Ради національної безпеки і оборони України як координаційного органу з питань національної безпеки при Президентові України.

Викладені положення Конституції України, в свою чергу, стали поштовхом до розробки всього пакета нормативно-правових актів, необхідних для ефективного забезпечення національної безпеки України в інформаційній та інших сферах її існування - зовнішньо-та внутрішньополітичній, державної безпеки, військовій та сфері безпеки державного кордону, економічній, соціальній, гуманітарній, науково-технологічній та екологічній.

Відповідно до ст. 34 Конституції України здійснення гарантованих нею прав - "права на свободу думки й слова, на свободу вираження своїх поглядів і переконань", "права вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або іншим способом за своїм вибором" - може бути "обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою попередження заворушень або злочинів, для охорони здоров'я населення, для захисту репутації або прав інших людей, для попередження розголошення інформації,, отриманої конфіденційно, або для підтримки авторитету й неупередженості правосуддя". Отже, коло обмежень досить широке, однак кожне з них повинне бути визначене законом.

У січні 1997 р. Верховна Рада України схвалила "Концепцію (основи державної політики) національної безпеки України" (далі - концепція). Цей документ нормативно закріпив загальні положення та принципи забезпечення національної безпеки України, національні інтереси і загрози національній безпеці, основні напрями державної політики національної безпеки, систему її забезпечення та повноваження основних суб'єктів цієї системи. Серед основних принципів її забезпечення названі пріоритет прав людини, верховенство права й демократичний цивільний контроль за військовою сферою й іншими структурами в системі забезпечення національної безпеки.

Поряд з іншими можливими загрозами національній безпеці зазначені й загрози в інформаційній сфері - "інформаційна експансія з боку інших

держав, витік інформації, що становить державну та іншу, передбачену законом, таємницю" а також конфіденційної інформації, що є власністю держави".

Серед основних напрямів реалізації державної політики національної безпеки в інформаційній сфері Концепцією були визначені:

- вживання комплексних заходів щодо захисту свого інформаційного простору й входження України у світовий інформаційний простір;

- усунення негативних факторів порушення інформаційного простору, інформаційної експансії з боку інших держав (протидія СІО, АІА та іншим деструктивним ІПВ);

- розробка та запровадження необхідних засобів І режимів одержання, зберігання, поширення й використання суспільно значимої інформації, створення розвинутої інфраструктури в інформаційній сфері.

Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 р, № 514/2009 (далі - Доктрина) визначає інформаційну безпеку як самостійну сферу забезпечення національної безпеки України та одночасно як невід'ємну складову кожної а її сфер.

Основною метою реалізації положень Доктрини задекларовано створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету.

Доктрина визначає принципи забезпечення інформаційної безпеки України, життєво важливі інтереси в інформаційній сфері України в контексті інтересів особи, суспільства, держави, а також реальні та потенційні загрози інформаційній безпеці України - у сфері державної безпеки та у зовнішньополітичній, воєнній, внутрішньополітичній, економічній, соціальній, гуманітарній, науково-технологічній, екологічній сферах.

Відповідно до положень Доктрини, діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути

зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства і людини за трьома головними напрямами: інформаційно-психологічному, технологічного розвитку та захисту інформації.

Держава для забезпечення інформаційної безпеки України має вживати відповідних заходів в усіх сферах, де існують реальні та потенційні загрози - у сфері державної безпеки та у зовнішньополітичній, воєнній, внутрішньополітичній, економічній, соціальній, гуманітарній, науково-технологічній, екологічній сферах.

У Законі України "Про національну безпеку України" від 21 червня 2018 р. № 2469-VIII нормативно закріплено компетенцію та функції усіх визначених законом суб'єктів забезпечення національної безпеки України в усіх сферах, зокрема в інформаційній.

Цей Закон відповідно до п. 17 ч. 1 ст. 92 Конституції України визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності, зокрема в інформаційній сфері.

Відповідно до ст. 3 Закону об'єктами національної безпеки в інформаційній сфері є: а) людина і громадянин - їхні конституційні права і свободи; б) суспільство - його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; в) держава - її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Основними принципами забезпечення національної безпеки в інформаційній сфері е: пріоритет прав і свобод людини і громадянина; верховенство права; пріоритет договірних (мирних) засобів у розв'язанні конфліктів; своєчасність і адекватність заходів захисту національних інтересів реальним і потенційним загрозам; чітке розмежування повноважень та взаємодія органів державної влади у забезпеченні національної безпеки;

демократичний цивільний контроль над Воєнною організацією держави та іншими структурами в системі національної безпеки; використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки.

Згідно зі ст. 4 Закону суб'єктами забезпечення національної безпеки в інформаційній сфері є: Президент України; Рада національної безпеки і оборони України; Верховна Рада України; Кабінет Міністрів України; міністерства та інші центральні органи виконавчої влади;

Збройні сили України, Служба безпеки України та інші військові формування, утворені відповідно до законів України; суди загальної юрисдикції; прокуратура України; місцеві державні адміністрації та органи місцевого самоврядування.

Повноваження суб'єктів забезпечення національної безпеки визначені у ст. 9 Закону України "Про національну безпеку України", а також у відповідних профільних законах та положеннях, що предметно регулюють правовий статус кожного з них.

Національна безпека України в інформаційній сфері забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах.

Вибір конкретних засобів і шляхів забезпечення національної безпеки України в інформаційній сфері обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам.

Основні напрями державної політики в інформаційній сфері, визначені в ст. 8 Закону:

- 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 протидії корупції, зловживанням службовим становищем, іншим явищами, які загрожують національній безпеці України;

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

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

Відповідно до Закону України "Про національну безпеку України" цільові настанови та керівні принципи державного будівництва в інформаційній сфері, а також напрями діяльності органів державної влади в конкретній обстановці визначаються Стратегією національної безпеки України з метою своєчасного виявлення, відвернення і нейтралізації реальних і потенційних загроз національним інтересам України в інформаційній та інших сферах життєдіяльності. Положення Стратегії національної безпеки України, які стосуються забезпечення інформаційної безпеки нашої держави, буде розкрито нами долі у характеристиці нормативно-правових актів Президента України.

2.2. Нормативні акти конституційного напрямку, які закріплюють визначальні положення щодо забезпечення інформаційної безпеки України

Для забезпечення інформаційної безпеки України важливим нормативним актом є Закон України "Про Основні засади розвитку інформаційного суспільства в Україні".

Зокрема, у п. 13 "Інформаційна безпека в інформаційному суспільстві" цього Закону визначено, що вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Ще одним важливим для забезпечення інформаційної безпеки України нормативним актом є Закон України "Про інформацію" від 2 жовтня 1999 р. № 2657-XII (далі - Закон). Цим Законом закладено правові основи інформаційної діяльності, стверджено інформаційний суверенітет України, закріплене право на інформацію та на доступ до неї, визначено систему відносин і зобов'язань у цій сфері, прийняту для демократичної держави, визначено правові форми міжнародного співробітництва в галузі інформації"

Під інформацією цей Закон (ст. 1) розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує П охорону, захищає особу та суспільство від неправдивої інформації. Дія цього Закону поширюється на інформаційні відносини, які виникають у всіх сферах життя і діяльності суспільства і держави під час одержання, використання, поширення та зберігання інформації (зокрема й використання мережі Інтернет).

Відповідно до ст. 7 Закону суб'єктами інформаційних відносив є: громадяни України, юридичні особи та держава. Ними можуть бути також Інші держави, їх громадяни та юридичні особи, міжнародні організації та особи без громадянства.

Об'єктами інформаційних відносин є документована або публічно оголошувана інформація про події та явища в галузі політики, економіки, культури, охорони здоров'я, а також у соціальній, екологічній, міжнародній та інших сферах (ст. 8 Закону).

Окрім того, Законом закріплене право на інформацію, гарантоване Конституцією України (ст. 34), а також гарантії цього права. Згідно зі ст. 9 Закону, всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій. Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України. Реалізація права на інформацію зазначеними суб'єктами не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Також Закон у ст. 12 дає визначення інформаційної діяльності: "Це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави". З метою задоволення цих потреб органи державної влади та органи місцевого і регіонального самоврядування створюють інформаційні служби, системи, мережі, бази і банки даних. Порядок їх створення, структура, права та обов'язки визначаються Кабінетом Міністрів України або інтими органами державної влади, а також органами місцевого і регіонального самоврядування.

Основними напрямами інформаційної діяльності е: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо (ст. 12 Закону).

Держава зобов'язана постійно дбати про своєчасне створення, належне функціонування і розвиток інформаційних систем, мереж, банків і баз даних у всіх напрямах інформаційної діяльності. Держава гарантує свободу інформаційної діяльності за цими напрямами всім громадянам та юридичним особам в межах їх прав і свобод, функцій і повноважень.

Відповідно до ст. 13 Закону основними видами інформаційної діяльності є одержання, використання, поширення та зберігання інформації. Одержання, використання, поширення та зберігання документованої або публічно оголошуваної інформації здійснюється у порядку, передбаченому цим Законом та іншими законодавчими актами в галузі інформації.

Окрім висвітлених вище положень, в Законі України "Про інформацію" також розкриваються: 1) галузі, види, джерела інформації та режим доступу до неї (Розділ III); 2) учасники інформаційних відносив, їх права та обов'язки (Розділ IV); 3) охорона інформації та загальні положення про відповідальність за порушення законодавства про інформацію (Розділ У); 4) міжнародна інформаційна діяльність, співробітництво з іншими державами, зарубіжними та міжнародними організаціями в галузі інформації (Розділ VI).

Іншим важливим законодавчим актом, що регулює інформаційну діяльність у сфері державної таємниці, є Закон України "Про державну таємницю" від 21 січня 1994 р. № 3855-XII.

Зокрема, цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

Дія цього Закону поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші органи державної влади, Верховну Раду АР Крим, Раду міністрів АР Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі - органи державної влади, органи місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці (ст. 3).

Відповідно до ст. 4 Закону державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики визначає Верховна Рада України. Окрім того, Законом визначено компетенцію органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці (ст. 5 Закону), здійснення права власності на секретну інформацію та її матеріальні носії (ст. 6 Закону), а також порядок фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею (ст. 7 Закону).

В розділі її Закону України "Про державну таємницю" розкрито низку положень щодо віднесення інформації до державної таємниці. Зокрема, відповідно до ст. 8 Закону, до державної таємниці у порядку, встановленому цим Законом, відноситься інформація: 1) у сфері оборони; 2) у сфері економіки, науки і техніки; 3) у сфері зовнішніх відносин; 4) у сфері державної безпеки та охорони правопорядку.

Не належить до державної таємниці інформація:

- про стан довкілля, про якість харчових продуктів і предметів побуту;

- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

- про факти порушень прав і свобод людини і громадянина;

- про незаконні дії органів державної, влади, органів місцевого самоврядування та їх посадових осіб;

- інша інформація, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена.

У статті 9 Закону розкрито компетенцію, права, обов'язки та відповідальність державних експертів з питань таємниць, а в ст. 10 - порядок віднесення інформації до державної таємниці.

Окремою нормою (ст. 12) в Законі визначено положення щодо Зводу відомостей, що становлять державну таємницю. Ці положення конкретизовані в наказі СБ України № 440 від 12 серпня 2005 р.р яким затверджено Звід відомостей, що становлять державну таємницю.

Відповідним розділом в Законі виділено положення щодо охорони державної таємниці (Розділ IV). При цьому в ст. 18 Закону розкриті основні організаційно-правові заходи щодо охорони державної таємниці.

Зокрема, з метою охорони державної таємниці впроваджуються:

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

- дозвільний порядок провадження органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею;

- обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

- обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;

- особливості здійснення органами державної влади їх функцій щодо органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею;

- режим секретності органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею;

- спеціальний порядок допуску та доступу громадян до державної таємниці;

- технічний та криптографічний захисти секретної інформації. Окремими нормами в Законі врегульовані обов'язки громадян України щодо збереження державної таємниці (ст. 28), обмеження їхправ у зв'язку з допуском та доступом до державної таємниці (ст. 29), а також положення щодо належної їм компенсації у зв'язку з виконанням робіт, які передбачають доступ до державної таємниці (ст. 30).

Закон України "Про державну таємницю" також містить низку важливих положень щодо встановлення обмежень на оприлюднення секретної інформації (ст. 31), щодо передачі державної таємниці іноземній державі чи міжнародній організації (ст. 32), а також обмежень, пов'язаних з державною таємницею, щодо перебування і діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, а також розташування та переміщення об'єктів і технічних засобів, що їм належать (ст. 33).

Технічний та криптографічний захисти секретної інформації здійснюються в порядку, встановленому нормативними актами Президента України.

Оперативно-розшукові заходи щодо охорони державної таємниці здійснюються Службою безпеки України відповідно до Закону України "Про оперативно-розшукову діяльність".

Положення щодо контролю за забезпеченням охорони державної таємниці та нагляду за додержанням законодавства про державну таємницю виділено в Законі в окремому Розділі V.

Відповідно до ст. 37 Закону керівники органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій зобов'язані здійснювати постійний контроль за забезпеченням охорони державної таємниці.

Органи державної влади, яким рішенням державного експерта з питань таємниць було надано право вирішувати питання про доступ органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій до конкретної секретної інформації, зобов'язані контролювати стан охорони державної таємниці в усіх органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, які виконують роботи, пов'язані з відповідною державною таємницею, або зберігають матеріальні носії зазначеної секретної інформації.

Служба безпеки України має право контролювати стан охорони державної таємниці в усіх органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, а також у зв'язку з виконанням цих повноважень одержувати безоплатно від них інформацію з питань забезпечення охорони державної таємниці. Висновки Служби безпеки України, викладені в актах офіційних перевірок за результатами контролю стану охорони державної таємниці, є обов'язковими для виконання посадовими особами підприємств, установ та організацій незалежно від їх форм власності.

Окрім висвітлених вище положень, в Законі України "Про державну таємницю" також розкриваються загальні положення про відповідальність за порушення законодавства про державну таємницю (Розділ VI), зміст яких конкретизовано у відповідних статтях Кримінального кодексу України та Кодексу України про адміністративні правопорушення.

Вагомим кроком для забезпечення інформаційної безпеки України на шляху впровадження та використання новітніх інформаційних технологій в усі сфери діяльності держави та суспільного життя стало прийняття законів України "Про Національну програму інформатизації" від 4 лютого 1998 р. № 74/98-ВР та "Про Концепцію Національної програми інформатизації" від 4 лютого 1998 р. № 75/98.

Базовим законом у сфері інформатизації на сучасному етапі е Закон України "Про Національну програму інформатизації" від 4 лютого 1998 р. № 74/98-ВР (далі - Закон), однією із двох головних цілей якої проголошене забезпечення інформаційної безпеки держави.

Врегульована цим Законом Національна програма інформатизації визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення.

Національна програма інформатизації спрямована на створення умов, необхідних для забезпечення громадян, суспільства та держави своєчасною, достовірною та повною інформацією шляхом широкого використання новітніх інформаційних технологій, забезпечення інформаційної безпеки держави.

Національна програма інформатизації включає положення про:

- Концепцію Національної програми інформатизації;
- сукупність державних програм з інформатизації;
- галузеві програми та проекти інформатизації;
- регіональні програми та проекти інформатизації;

- програми та проекти інформатизації органів місцевого самоврядування.

Призначенням законодавства про Національну програму інформатизації є запровадження правових, організаційних, науково-технічних, економічних, фінансових, методичних та гуманітарних засад регулювання процесу формування та виконання цієї Програми та окремих її завдань (проектів). Закон також встановлює основні функції органів державної влади у процесі інформатизації, зокрема:

- забезпечення інформаційної безпеки держави;

- встановлення стандартів, норм і правил використання засобів інформатизації;

- забезпечення доступу громадян та їх об'єднань до інформації органів державної влади та органів місцевого самоврядування, а також до інших джерел інформації;

- визначення пріоритетних напрямів інформатизації з метою подальшої її підтримки шляхом державного фінансування та пільгового оподаткування;

- інформатизацію науки, освіти, культури, охорони довкілля та здоров'я людини, державного управління, національної безпеки та оборони держави, пріоритетних галузей економіки;

- підтримку вітчизняного виробництва програмних і технічних засобів інформатизації;

- підтримку фундаментальних наукових досліджень для розроблення швидкісних математичних і технічних засобів обробки інформації;

- забезпечення підготовки спеціалістів з питань інформатизації та інформаційних технологій;

- організацію сертифікації програмних і технічних засобів інформатизації;

- державне регулювання цін і тарифів на використання телекомунікаційних та комп'ютерних мереж для потреб інформатизації у бюджетній сфері;

- захист авторського права на бази даних і програми, створені для потреб інформатизації та особистої інформації.

У законі визначено етапи формування і виконання, порядок здійснення експертизи, механізм контролю за виконанням Національної програми інформатизації, замовників, науково-технічну раду та виконавців програми, їх права та обов'язки.

В свою чергу, в Законі України "Про Концепцію Національної програми інформатизації" від 4 лютого 1998 р. № 75/98 (далі - Закон) важливим фактором подолання відставання України у сфері інформатизації названа ефективна державна політика інформатизації.

Окрім того, в цьому Законі закріплені принципи державної політики у сфері інформатизації, визначені основні завдання, напрями, порядок формування та виконання основних етапів програми, очікувані результати.

Зокрема, Законом визначені такі основні напрями інформатизації:

- вироблення державної політики у сфері інформатизації та організаційно-правове забезпечення інформатизації;

- формування національної інфраструктури інформатизації, яка включає: міжнародні та міжміські телекомунікаційні та комп'ютерні мережі; систему інформаційно-аналітичних центрів різного рівня;

- інформаційні ресурси; інформаційні технології; систему науково-дослідних установ з проблем інформатизації; виробництво та обслуговування технічних засобів інформатизації;

- створення системи підготовки висококваліфікованих фахівців у сфері інформатизації;

- інформатизація стратегічних напрямів розвитку державності, безпеки та оборони (із забезпеченням інформаційної безпеки);

- інформатизація процесів соціально-економічного розвитку; - інформатизація пріоритетних галузей економіки;

- інформатизація фінансової та грошової системи, державного фінансово-економічного контролю;

- інформатизація соціальної сфери;

- інформатизація в галузі екології та використання природних ресурсів;

- інформатизація науки, освіти і культури.

Окрім того, в Законі визначено також низку інших важливих положень щодо програми інформатизації в Україні.

2.3. Нормативні акти вищих та центральних органів виконавчої влади, які регулюють діяльність у сфері забезпечення інформаційної безпеки України

Розкривши основні положення законодавчих актів України, які визначають правові засади забезпечення інформаційної безпеки, розглянемо також положення нормативно-правових актів Президента України, Кабінету Міністрів України та Верховної Ради України, а також нормативні акти міністерств і відомств.

Визначальне значення для забезпечення інформаційної безпеки держави має Указ Президента України "Про Стратегію національної безпеки України" від 26 травня 2015 р. № 287/2015.

Стратегія національної безпеки України (далі - Стратегія) визначав принципи, пріоритетні цілі, завдання та механізми забезпечення життєво важливих інтересів особи, суспільства і держави від зовнішніх і внутрішніх загроз в інформаційній та інших сферах життєдіяльності.

Як головну мету Стратегії визначено необхідність забезпечити такий рівень національної безпеки, який би гарантував поступальний розвиток України, її конкурентоспроможність, забезпечення прав і свобод людини і

громадянина, подальше зміцнення міжнародних позицій та авторитету Української держави у сучасному світі.

Досягнення цієї мети можливе шляхом реалізації державної політики національної безпеки, яка передбачає забезпечення інформаційної безпеки, утвердження засад національної єдності задля розбудови демократичної, правової, конкурентоспроможної держави, формування соціально орієнтованої ринкової економіки, зміцнення науково-технологічного потенціалу, забезпечення інноваційного розвитку, зростання рівня життя і добробуту населення, екологічно і техногенно безпечних умов життєдіяльності суспільства.

В Стратегії національної безпеки України інформаційна сфера розглядається як важлива сфера життєдіяльності особи, суспільства та держави та одночасно як одна з ключових сфер національної безпеки України. До стратегічних пріоритетів політики національної безпеки в інформаційній сфері Стратегія (п. 3.10) серед інших відносить також забезпечення сприятливих зовнішніх умов для розвитку та безпеки держави шляхом забезпечення інформаційної безпеки при інтеграції до структур глобального інформаційного суспільства, одним із елементів яких е глобальна інформаційна мережа Інтернет.

Окрім того, Стратегією у п. 2.7 як виклики та загрози життєво важливим національним інтересам України в інформаційній сфері додатково виділяються: посилення негативного зовнішнього впливу на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності; недостатні обсяги вироблення конкурентоспроможного національного інформаційного продукту, а також наближений до критичного стан безпеки інформаційно-комп'ютерних систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо.

Згідно з п. 4.1 Стратегії, подальший розвиток системи управління національною безпекою України в інформаційній та інших сферах життєдіяльності має здійснюватися, зокрема, у таких напрямах:

1) вдосконалення законодавства з питань національної безпеки, насамперед шляхом:

- розвитку правових засад управління національною безпекою через розробку відповідних законів, концепцій, доктрин, стратегій і програм, зокрема Національної програми протидії тероризму і екстремізму, Концепції розвитку національної інноваційної системи, Національної стратегії формування інформаційного суспільства, Доктрини інноваційного та науково-технологічного розвитку тощо;

- розробки та прийняття нових редакцій Кримінального і Кримінально-процесуального кодексів, законів України "Про Службу безпеки України", "Про контррозвідувальну діяльність", інші органи сектора безпеки, нових законів "Про профілактику злочинності", "Про перехоплення телекомунікацій" тощо;

- усунення наявних протиріч, неузгодженостей і прогалин у чинних законах та інших нормативно-правових актах з питань національної безпеки і оборони;

- розробки та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами Конвенції про кіберзлочинність, ратифікованої Верховною Радою України;

- приведення законодавства з питань охорони державної таємниці до європейських стандартів;

2) підвищення ефективності планування, координації і контролю за діяльністю суб'єктів забезпечення національної безпеки в інформаційній сфері та їх відповідальності шляхом:

- підвищення ефективності діяльності суб'єктів забезпечення національної безпеки з упереджувального отримування інформації для своєчасного виявлення існуючих і нових типів внутрішніх і зовнішніх загроз в інформаційній сфері, розробка дієвих заходів щодо їх запобігання та нейтралізації;

- інформаційно-аналітичної підтримки діяльності органів державної влади, насамперед в умовах кризових і надзвичайних ситуацій, в тому числі особливого періоду;

- впровадження захищених інформаційно-телекомунікаційних мереж в органах державної влади;

- розробки та впровадження загальнодержавної системи визначення та моніторингу порогових значень показників (індикаторів), що характеризують рівень захищеності національних інтересів в інформаційній сфері та інших сферах життєдіяльності, виникнення реальних загроз національній безпеці.

Стратегія національної безпеки України є документом, обов'язковими для виконання, і основою для розробки конкретних програм за складовими державної політики інформаційної безпеки.

Правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства, визначає Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 р. № 1229 (зі змінами та доповненнями).

Водночас з огляду на наявність гострих проблем, явищ та чинників, що негативно впливають на реалізацію державної політики забезпечення національної безпеки в інформаційній сфері, чим породжують нові загрози національній безпеці та національним інтересам України в цій сфері та негативно впливають на розвиток вітчизняного громадянського суспільства й української держави та реалізацію її євро інтеграційних прагнень, РНБО України 21 березня 2008 р. було прийняте рішення про доцільність вжиття невідкладних заходів щодо забезпечення інформаційної безпеки України. Це

рішення було затверджене Указом Президента України "Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року "Про невідкладні заходи щодо забезпечення інформаційної безпеки України від 23 квітня 2008 р. № 377/2008.

Відповідно до прийнятого Радою національної безпеки і оборони України рішення, на Кабінет Міністрів України зокрема було покладено завдання у тримісячний термін розробити за участю Служби безпеки України і внести на розгляд Верховної Ради України законопроект щодо правових механізмів виявлення, фіксації, кваліфікації, блокування та видалення з українського сегмента мережі Інтернет інформації, поширення якої заборонено законодавством України (пп. "г" п. 1 Рішення).

Цим Указом Президента України одним із заходів передбачено розробку за участю Антимонопольного комітету України, Національної ради України з питань телебачення і радіомовлення, Фонду державного майна України, а також затвердження заходів зі сприяння розвитку конкуренції та запобігання монополізму у сферах телекомунікацій, телебачення, радіомовлення і друкованих засобів масової інформації.

В Указі передбачено необхідність розробити за участю Служби безпеки України і внести у тримісячний строк на розгляд Верховної Ради України законопроекти щодо:

- посилення кримінальної відповідальності за незаконне збирання, зберігання, використання або поширення персональних даних особи без її згоди, а також установлення відповідальності за незабезпечення захисту персональних даних, що піддаються автоматизованій обробці;

- ратифікації Конвенції про захист осіб стосовно автоматизованої обробки даних особистого характеру;

- обов'язкового віднесення до інформації з обмеженим доступом персональних даних, а також відомостей, що надаються фізичними та юридичними особами органам державної влади, підприємствам і

організаціям у зв'язку з виконанням їхніх повноважень та розголошення яких може завдати шкоди зазначеним особам;

- правових механізмів виявлення, фіксації, кваліфікації, блокування та видалення з українського сегменту мережі Інтернет інформації, поширення якої заборонено законодавством України.

Також в Указі Президента поставлено завдання перед компетентними суб'єктами розробити і внести на розгляд Верховної Ради України проект Концепції національної інформаційної політики, яка визначатиме основні напрями, засади і принципи національної політики та механізми її реалізації, а також пріоритети розвитку інформаційної сфери, буде спрямована на створення умов для побудови в Україні розвинутого інформаційного суспільства, забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури, впровадження новітніх інформаційних технологій, захист національних моральних і культурних цінностей, забезпечення конституційних прав людини і громадянина на свободу слова та вільний доступ до інформації.

Окрім того, Національній раді України з питань телебачення і радіомовлення запропоновано вжити невідкладних заходів щодо посилення контролю за додержанням телерадіоорганізаціями та провайдерами програмної послуги вимог законодавства про телебачення і радіомовлення, зокрема вимог щодо частки національного продукту в загальному обсязі мовлення телерадіоорганізацій та обов'язкової частки мовлення українською мовою.

Одним із визначальних нормативних актів, яким було закладено підвалини для забезпечення захисту та здійснення контролю інформації в мережах передачі даних є Концепція технічного захисту інформації (ТЗІ), затверджена Постановою Кабінету Міністрів України від 8 жовтня 1997 р. № 1126.

Відповідно до змісту Концепції, ТЗІ - діяльність, спрямована на забезпечення інженерно-технічними засобами порядку доступу, цілісності й

доступності (неможливості блокування) інформації, що становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності й доступності відкритої інформації, важливої для особистості, суспільства й держави.

Це визначення уточнює розкритий у зазначеній Концепції один із принципів формування і проведення державної політики в сфері технічного захисту інформації: "Обов'язковість захисту інженерно-технічними засобами інформації, що становить державну й іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для суспільства й держави, якщо ця інформація циркулює в органах державної влади й органах місцевого самоврядування, Національний академії наук. Збройних силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, у державних установах і організаціях".

Серед згаданих у цьому переліку термінів законодавцем чітко визначено лише поняття державної таємниці. Водночас "інша, передбачена законом таємниця" насправді ніяким законом України не визначена, малозрозумілим є поняття "конфіденційної інформації, що е власністю держави": згідно зі ст. 30 Закону України "Про інформацію" вона може бути власністю тільки юридичних і фізичних осіб, але не держави. Також розмитим є поняття "відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює".

Тому закономірним буде висновок про те, що рішення, яку інформацію потрібно захищати, будуть приймати державні службовці за своїм переконанням, не обмеженим жодними правовими рамками. Концепція передбачає створення підрозділів ТЗІ всюди, де необхідно захищати інформацію. Аналіз положень Концепції ТЗІ наводить на думку про те, що реалізація цієї концепції фактично спрямована на обмеження доступу до офіційної інформації, однак не визначає чітких підстав та умов проведення в

Україні діяльності щодо контролю за інформацією, що циркулює в інформаційних мережах.

Іншим важливим документом щодо контролю інформації в інформаційних мережах в Україні стала "Інструкція про порядок обліку, зберігання й використання документів, справ, видань і інших матеріальних носіїв інформації, що містять конфіденційну інформацію, що є власністю держави", затверджена Постановою Кабінету Міністрів України від 27 листопада 1998 р.

Відповідно до п. 1 Інструкції до таких переліків може ввійти не лише інформація, що створюється самим органом влади, але й інформація, що перебуває в його розпорядженні й користуванні. Тому будь-яка інформація, що потрапила в поле зору державного органу, може бути за бажанням його керівника оголошена конфіденційною.

Згідно з п. 2 Постанови центральні й місцеві органи виконавчої влади й органи місцевого самоврядування повинні розробити в шестимісячний строк і ввести в дію переліки конфіденційної інформації, що є власністю держави, цій інформації привласнюється гриф "Для службового користування" (ДСК). Відповідно до п. 3 Постанови виконувати Інструкцію повинні не лише органи влади, але й підприємства, установи й організації незалежно від форм власності.

Документи органів законодавчої влади, вищих органів виконавчої влади й судової влади, що вийшли у світ в І991 році й пізніше без грифа обмеження доступу, але не опубліковані в офіційній пресі, розглядаються як матеріали, що містять відомості обмеженого поширення із грифом "ДСК" (п. 5 Інструкції).

Умови зберігання, розмноження й розсилання документів із грифом "ДСК" не менш жорсткі, аніж для документів, що містять відомості, що становлять державну таємницю: реєстрація й знищення всіх чернеток і варіантів документів, заборона на позначення прізвищ і навіть посад керівників організації тощо (пункти 17-28 Інструкції). Ознайомлення

представників ЗМІ з документами із грифом "ДСК" дозволяється тільки за письмового дозволу керівника організації в кожному конкретному випадку й лише після розгляду цього питання експертною комісією, що приймає письмове рішення про доцільність передачі документа журналістові. Зі змісту Інструкції видно тільки, що до складу зазначеної експертної комісії входять "співробітники канцелярії, РСП та інших структурних підрозділів".

Одним із недоліків Інструкції стало те, що в ній конкретно не визначено, хто саме та на підставі яких критеріїв, вирішує, які відомості є конфіденційними, а які ні. Також зі змісту Інструкції не зрозуміло, чи будуть доступні для широкого використання самі переліки, тим більше, що кожне відомство може мати свій перелік.

Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах врегульовані Постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах".

Правила, затверджені зазначеною постановою, визначають загальні вимоги та організаційні засади забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Дія цих Правил не поширюється на захист інформації в системах урядового та спеціальних видів зв'язку.

Відповідно до п. 2 Правил, захисту в системі підлягає:

- відкрита інформація, яка є власністю держави та відповідно до Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру й використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність

зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами. Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту системи від несанкціонованих дій, які можуть призвести до випадкової або умисної модифікації чи знищення такої інформації;

- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу. Під час обробки такої інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення;

- інформація, що становить державну або іншу передбачену законом таємницю. У процесі її обробки повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації не ідентифікованих осіб чи користувачів з непідтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права.

Вимоги до захисту в системі інформації, що становить державну таємницю, визначаються цими Правилами та законодавством у сфері охорони державної таємниці. Вимоги до захисту в системі інформації від несанкціонованого блокування визначаються її власником (розпорядником), якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством (пункти 9 і 10 Правил).

Згідно з п. 11 Правил, у системі здійснюється обов'язкова реєстрація:

- результатів ідентифікації та автентифікації користувачів;

- результатів виконання користувачем операцій з обробки інформації;

- спроб несанкціонованих дій з інформацією;

- фактів надання та позбавлення користувачів права доступу до інформації та її обробки;

- результатів перевірки цілісності засобів захисту інформації. Така реєстрація інформації здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки. Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.

Відповідно до п. 13 Правил передача конфіденційної і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації. Порядок підключення систем, в яких обробляється конфіденційна і таємна інформація, до глобальних мереж передачі даних (зокрема до мережі Інтернет) визначається законодавством.

Окрім того, Правилами у п. 15 передбачено здійснення контролю за цілісністю програмного забезпечення системи, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації. Також контролюється цілісність програмних та технічних засобів захисту інформації, уразі порушення якої обробка інформації в системі припиняється.

Для забезпечення захисту інформації в інформаційній (телекомунікаційній чи інформаційно-телекомунікаційній) системі створюється комплексна система захисту інформації (п. 16 Правил), яка призначається для захисту інформації.

Серед загальних положень цієї постанови, на нашу думку, ключовими є вимоги:

- щодо заборони підключення до глобальної мережі Інтернет локальних обчислювальних мереж, а також окремих електронно-обчислювальних машин, на яких обробляють або зберігають інформацію з обмеженим доступом, що є власністю держави й охороняється законами України (п. 7);

- щодо зобов'язання абонента укладати договір про надання послуг із доступу до глобальної мережі Інтернет та протягом 15 робочих днів повідомляти про це Державний комітет зв'язку та інформатизації України (п. 8).

Окрему увагу, на нашу думку, необхідно звернути на нормативні акти Кабінету Міністрів України, що регулюють порядок висвітлення діяльності органів виконавчої влади в мережі Інтернет. Це, зокрема, постанови Кабінету Міністрів України від 24 лютого 2003 р. № 208 "Про заходи щодо створення електронної інформаційної системи "Електронний Уряд", а також від 4 січня 2002 р. № 3 "Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади" та від 11 лютого 2004 р. № 150 "Про офіційне оприлюднення регуляторних актів, прийнятих місцевими органами виконавчої влади, територіальними органами центральних органів виконавчої влади та їх посадовими особами, і внесення змін до Порядку оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади".

Інформаційне наповнення та технічне забезпечення веб-порталів органів виконавчої влади врегульоване Порядком інформаційного наповнення та технічного забезпечення Єдиного веб-порталу органів виконавчої влади та Порядком функціонування веб-сайтів органів виконавчої влади, затвердженими Наказом Державного комітету інформаційної політики, телебачення і радіомовлення України, Державного комітету зв'язку та інформатизації України від 25 листопада 2002 р. № 327/225,

Розпорядженням Голови Верховної Ради України від 24 травня 2001 р. № 462 "Про затвердження Положення про веб-сайт Верховної Ради України у глобальній інформаційній мережі Інтернет" та іншими нормативно-правовими актами.

Іншим важливим нормативно-правовим актом у зазначеній сфері є Порядок надання інформаційних та інших послуг з використанням електронної інформаційної системи "Електронний Уряд", затверджений Наказом Державного комітету зв'язку та інформатизації України від 15 серпня 2003 р. № 149. Порядок визначає процедуру надання органами виконавчої влади інформаційних та інших послуг громадянам і юридичним особам з використанням електронної інформаційної системи "Електронний Уряд".

Види інформаційні послуг, що надаються з використанням електронної інформаційної системи "Електронний Уряд", визначені в Переліку інформаційних та інших послуг електронної інформаційної системи "Електронний Уряд". Можливості надання органом виконавчої влади певної послуги визначаються готовністю цього органу надавати відповідну державну послугу в електронній формі та потребою громадян і юридичних осіб у такій послузі.

Разом із зазначеними законами України та нормативними актами Президента України та Кабінету Міністрів України, важливими нормативними актами, що регулюють забезпечення інформаційної безпеки держави є загальнообов'язкові нормативно-технічні документи - Державні стандарти України (ДСТУ), а також нормативні акти міністерств, відомств та інших органів державної влади.

До них відносяться, зокрема, ДСТУ 3254-95 "Радіозв'язок. Терміни та визначення", ДСТУ 3560-97 "Радіозв'язок космічний та супутниковий. Терміни та визначення", ДСТУ 4361:2004 "Системи стільникового радіозв'язку цифрові. Терміни та визначення понять" тощо. Закріплений в

них понятійний апарат є обов'язковим для використання в усій галузі телекомунікацій.

Окрім того, потребують врахування й акти компетентних державних органів та установ, які регулюють діяльність у цій сфері:

1. Комплексна система захисту інформації в автоматизованій системі Міністерства. Інструкція користувача автоматизованої системи третього класу. Затверджена наказом Міністерства економіки від 23 квітня 2002 р. № 121.

2. Порядок контролю за додержанням ліцензійних умов 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; розроблення, виробництва, впровадження, обслуговування, дослідження ефективності систем і засобів технічного захисту інформації, надання послуг в галузі технічного захисту інформації; розроблення, виробництва, впровадження, сертифікаційних випробувань, ввезення, вивезення голографічних захисних елементів. Затверджений наказом Держпідприємництва, Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 12 грудня 2001 р. № 151/72.

3. Наказ Ліцензійної палати України та Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про затвердження Інструкції про умови і правила провадження підприємницької діяльності (ліцензійні умови), пов'язаної з розробленням, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів технічного захисту інформації, а також з наданням послуг із технічного захисту інформації, та контроль за їх дотриманням".

4. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про затвердження Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації".

5. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про затвердження Інструкції 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".

6. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про затвердження Положення про контроль за функціонуванням системи технічного захисту інформації".

7. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про затвердження Положення про державну експертизу в сфері технічного захисту інформації".

8. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах" від 24 грудня 2001 р. № 76.

9. Наказ Державного комітету зв'язку та інформатизації України "Про затвердження Порядку складання та ведення переліку підприємств (операторів), які надають послуги з доступу до глобальних мереж передачі даних органам виконавчої влади, іншим державним органам, підприємствам, установам та організаціям, які одержують, обробляють, поширюють і зберігають інформацію, що є об'єктом державної власності та охороняється згідно із законодавством" від 17 червня 2002 р.№ 122.

Висновки до другого розділу

За роки незалежності в Україні закладено законодавчі основи системи забезпечення інформаційної безпеки, зокрема було напрацьовано великий масив нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері.

На найвищому рівні - норми Конституції України, які закріплюють концептуальні положення національної безпеки України в усіх сферах її існування, а також Концепцію національної безпеки України, Доктрину інформаційної безпеки України та Закон України "Про національну безпеку України". Ці документи враховують основні положення міжнародних договорів і угод, ратифікованих Україною, які стосуються її національної безпеки.

На другому рівні - закони конститутивного напрямку, де визначаються важливі положення щодо забезпечення національної безпеки в інформаційній сфері ("Про Основні засади розвитку інформаційного суспільства в Україні" та інші).

На третьому рівні - закони України інституційного рівня, де закріплені основні форми діяльності державних органів у процесі забезпечення національної безпеки в інформаційній та інших сферах життєдіяльності особи, суспільства та держави (зокрема "Про оборону України", "Про Збройні Сили України тощо).

У структурі нормативно-правової бази забезпечення національної безпеки України в інформаційній сфері особливе місце посідають укази та розпорядження Президента України, а також акти (постанови, декрети) Кабінету Міністрів України. Ці нормативні акти є незаконними й видаються з метою конкретизації та підвищення якості вирішення завдань забезпечення інформаційної безпеки.

РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО ПОКРАЩЕННЯ СИСТЕМИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

3.1. Пропозиції щодо покращення державної політики у сфері забезпечення інформаційної безпеки України

Інформаційна безпека є необхідною умовою існування як особи, так і держави та суспільства загалом. Виходячи з цього доцільно виокремити такі рівні забезпечення інформаційної безпеки:

– рівень особи (формування раціонального, критичного мислення на основі принципів свободи вибору);

– суспільний (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність в отриманні інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам);

– державний (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої та зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам).

При виробленні та реалізації державної політики у сфері забезпечення інформаційної безпеки необхідно враховувати ряд принципових позицій.

По-перше, правове регулювання у сфері інформаційної безпеки тією чи іншою мірою стосується закріплених у Конституції прав особи на інформацію, положень про демократичний устрій, плюралізм думок тощо, законодавств про інформацію, про забезпечення національної (державної) безпеки, охорону державної та комерційної таємниці, діяльність засобів масової інформації, Інтернету, а також питань захисту інформації з обмеженим доступом.

По-друге, питання, пов'язані зі зміною чинного законодавства України в цій сфері, були, є і будуть заручниками внутрішньої політичної боротьби у державі. Будь-який розгляд у стінах Верховної Ради України питань, пов'язаних зі становленням демократичних інститутів, плюралізму, статусу ЗМІ, їх незалежності, неминуче буде предметом гострих дискусій.

По-третє, важливою складовою державної політики в будь-якій сфері необхідно визнати інформаційне забезпечення. Така діяльність буде важливим компонентом інформаційної безпеки України протягом всього періоду інтеграції. Якщо українські політики не спроможуться сформувати чіткі цілі, які відповідатимуть національним інтересам, і адекватно донести їх до громадськості -тоді за них це обов'язково зроблять зовнішні суб'єкти. А вже потім під організованим ззовні тиском громадськості відповідні рішення таки будуть ухвалені (через, наприклад, процедуру референдуму, як це було у Словаччині в 1997 р.). але чи будуть вони відповідати інтересам України.

Діяльність у такому напрямі повинна включати постійний моніторинг громадської думки, який доцільно проводити за допомогою соціологічних досліджень та технологій контент-аналізу.

По-четверте, хоча громадська думка є досить піддатливою для впливу (маніпулювання), події в Україні листопада 2004-січня 2005 року свідчать на користь методів роз'яснювальної роботи та переконання, а не агресивної пропаганди.

По-п'яте, пріоритетною аудиторією для інформаційного впливу доцільно визначити представників ЗМІ та педагогічний склад вищих навчальних закладів, інших освітніх установ. Досвід країн східної Європи переконливо свідчить, що саме ці суспільні групи є неформальними лідерами та виразниками позицій у процесі формування громадської думки.

Основними напрямами державної політики в інформаційній сфері національної безпеки визнано (ст. 8 Закону України "Про основи національної безпеки"):

– забезпечення інформаційного суверенітету України;

– вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури й 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.

Адекватне реагування на загрози інформаційній безпеці виходить за межі чинної нормативної бази і можливе лише за умови прийняття політичних рішень компетентними органами. Необхідно визнати, що в умовах української демократії формування державної політики у будь-якому напрямі залежить не тільки від експертних оцінок та об'єктивного врахування національних інтересів, але й від політичної кон'юнктури у певний період. Тому основна рекомендація до процесу ухвалення політичних рішень може бути сформульована таким чином: урахування довгострокових стратегічних національних інтересів.

Зазначену ознаку довгостроковості може і повинно забезпечити законодавче регулювання найважливіших суспільних відносин. При цьому необхідно виходити із спрямованості нормативно-правових актів на досягнення практичного результату - формування ефективного механізму

забезпечення інформаційної безпеки. Останній є системою взаємопов'язаних елементів, які забезпечують захист та розвиток інформаційного простору відповідно до національних інтересів.

У цьому механізмі повинні бути враховані національні інтереси в інформаційному середовищі, внутрішні та зовнішні загрози цим інтересам і передбачена система засобів із виявлення та нейтралізації загроз.

З огляду на структуру інформаційного середовища (простору) забезпечення інформаційної безпеки передбачає захист таких елементів:

– інформації з обмеженим доступом;

– систем і засобів передавання та зберігання інформації;

– інформаційного простору від поширення інформації, зміст якої через неповноту, недостовірність тощо суперечить національним інтересам держави.

До елементів системи забезпечення інформаційної безпеки (у вузькому розумінні) відносяться:

– нормативно-правові акти, які регламентують суспільні відносини в інформаційній сфері та встановлюють юридичну відповідальність у випадку їх порушення;

– державні та недержавні організації, які забезпечують продукцією ринок інформаційних послуг (ЗМІ, інформаційні агенції, служби, аналітичні та дослідні організації, власники каналів електронного зв'язку, Інтернет-провайдери, кіноіндустрія та індустрія розваг тощо);

– сукупність спеціально уповноважених органів держави, які контролюють дотримання інформаційного законодавства (окремі підрозділи СБУ, Міністерство транспорту та зв'язку, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Національна експертна комісія України з питань захисту суспільної моралі, органи прокуратури);

– практична діяльність зазначених суб'єктів, спрямована на розвиток вітчизняного інформаційного простору.

У широкому розумінні до системи забезпечення Інформаційної безпеки необхідно віднести Верховну Раду України та її законодавчу діяльність, Президента України, регуляторні та контролюючі державні органи, споживачів інформації та інших суб'єктів.

Правове регулювання у сфері інформаційної безпеки буде тією чи іншою мірою стосуватися закріплених у Конституції прав особи на інформацію, положень про демократичний устрій, плюралізм думок тощо, законодавства про інформацію, про забезпечення національної (державної) безпеки, охорону державної та комерційної таємниці, діяльність засобів масової інформації, інтернету, а також питань захисту інформації з обмеженим доступом.

3.2. Пропозицій щодо покращення нормативно-правового забезпечення інформаційної безпеки держави

1. Доцільним убачається об'єднання (інкорпорації чи кодифікації) нормативних актів, які регламентують інформаційну діяльність в Україні:

– Закон України "Про інформацію";

– Закон України "Про телебачення і радіомовлення";

– Закон України "Про систему Суспільного телебачення і радіомовлення України";

– Закон України "Про друковані засоби масової інформації (пресу) в Україні";

– Закон України "Про захист суспільної моралі";

– Закон України "Про рекламу";

– Закон України "Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації";

– Закон України "Про інформаційні агентства";

– підзаконні нормативно-правові акти, які стосуються питань ліцензування, державної підтримки ЗМІ тощо.

2. Пропонується трирівнева система кримінально-правового захисту інформаційної безпеки: безпека інформації, безпека від інформаційних впливів, забезпечення реалізації прав суб'єктів інформаційних відносин:

- Злочини, що посягають на безпеку інформації.
  - Злочини, що посягають на безпеку інформації з обмеженим доступом.
  - Злочини, що посягають на безпеку відкритої інформації
  - Злочини, що посягають на безпеку інформації, котра належить до об'єктів інтелектуальної власності, а також безпеку "ноу-хау".
  - Злочини, що посягають на безпеку інформації про особу.
  - Злочини, що посягають на безпеку суспільних відносин та їх суб'єктів від Інформаційних впливів.
  - Злочини, що посягають на безпеку суспільних відносин та їх суб'єктів від впливів за допомогою недостовірної інформації.
  - Злочини, що посягають на безпеку суспільних відносин та їх суб'єктів від впливів за допомогою забороненої до поширення інформації.
  - Злочини, що посягають на безпеку суспільних відносин та їх суб'єктів унаслідок приховування необхідної інформації.
- Злочини, вчинювані в телекомунікаційному середовищі (так звані "комп'ютерні злочини").

Визначення родовим об'єктом інформаційних злочинів інформаційної безпеки в усіх трьох її складових дасть змогу урахувати перспективи видозміни інформаційних злочинів та появи їх нових видів, які посягатимуть на безпеку суспільних відносин та їх суб'єктів від інформаційних впливів.

3. Оптимізувати систему державного управління теле-, радіоінформаційною сферою (Національна рада України з питань

телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Державний департамент зв'язку та інформатизації Міністерства транспорту та зв'язку України).

Системною відповіддю на зовнішню інформаційну агресію може бути створення міжвідомчого консультативного комітету "добровільної самоцензури ЗМІ" (на зразок британського Defence, Press and Broadcasting Advisory Committee -DPBAC - консультативного комітету з оборони, преси і теле-, радіомовлення). До складу комітету доцільно включити вищих посадовців апарату розвідки, контррозвідки, правоохоронців (Прокуратура, МВС), виконавчої влади, а також провідних представників журналістського співтовариства і власників засобів масової інформації. Представників ЗМІ знайомлять з наявними інформаційними загрозами, тенденціями, офіційною позицією з найбільш гострих проблем з точки зору забезпечення національних інтересів. Після обговорення приймається колегіальне рішення у вигляді рекомендацій, виконання яких контролюється. Невиконання не передбачає прямої юридичної відповідальності, але зарубіжний досвід свідчить, що високий рівень представництва членів комітету забезпечує авторитетність рішень.

4. Як комплексний захід протидії комерціалізації ЗМІ реалізувати ідею створення громадського мовлення.

5. Пріоритетною аудиторією для внутрішньодержавного інформаційного впливу доцільно визначити представників ЗМІ та педагогічний склад ВНЗ, інших закладів освіти. Саме ці суспільні групи є неформальними лідерами та виразниками позицій у процесі формування громадської думки.

6. Важливо також широко використовувати вже досить потужні можливості вітчизняних неурядових організацій (аналітичних, соціологічних центрів тощо). Логіка проста: якщо їх потенціал не використає українська влада - то це зроблять іноземці. Прикладів роботи виключно за іноземними грантами (отримання та аналіз інформації з усіх сфер) маємо достатньо.

7. З метою забезпечення фінансової незалежності ЗМІ передбачити державне фінансування тих із них, які пропонують інформаційні, аналітичні, навчальні та просвітницькі програми (останні здебільшого є нерентабельними).

8. Для забезпечення інформаційної безпеки суспільства та особи від деструктивних зовнішніх впливів (суб'єктом яких може виступати і власне держава) на законодавчому рівні передбачити функціонування незалежних аналітичних, дослідницьких, інформаційних організацій, наділивши їх відповідними правами й визнавши їх діяльність неприбутковою (що дозволить уникнути податкового тиску та забезпечити фінансову незалежність). Зазначену проблему доцільно вирішити шляхом прийняття окремого закону.

9. Під неурядовою організацією визнати громадську, незалежну, неприбуткову (некомерційну), дослідну організацію зі статусом юридичної особи, що вивчає різноманітні проблеми суспільного, державного життя, займається інформаційною діяльністю, спрямованою на лобіювання, здійснення впливу на владу шляхом подання обґрунтованих пропозицій, критики, проектів рішень.

10. З метою обмеження можливого деструктивного впливу іноземного елементу на діяльність вітчизняних неурядових організацій у законі про неурядові організації передбачити диверсифікацію джерел фінансування останніх та визначити обмеження (відсоткову межу) фінансування діяльності з іноземних джерел та на гранти інших держав й іноземних організацій.

11. Розглянути можливість поширення зазначених вище правил діяльності неурядових організацій і на представництва іноземних неурядових організацій в Україні: надати їм статусу юридичної особи, розширити національний режим фінансування (а отже й обмеження щодо частки фінансування).

12. Окремо передбачити обов'язкову участь громадян України в керівних органах неурядових організацій за схемою: керівник - українець, заступники - іноземці або керівник - іноземець, заступники - українці.

13. З метою забезпечення колегіальності при прийнятті рішень, демократичності в діяльності ЗМІ передбачити обов'язковість створення спостережної ради у ЗМІ, створених у формі акціонерного товариства (а це більшість телекомпаній та друкованих ЗМІ), навіть якщо кількість акціонерів - до 50 осіб (ст. 46 Закону України "Про господарські товариства").

За напрямом захисту інформації з обмеженим доступом пропонуємо:

1. Підготувати цілісний законодавчий акт або доповнити Закон України "Про інформацію" щодо захисту приватної інформації, у якому визначити поняття такої інформації, повноваження органів державної влади щодо захисту приватної інформації, права та обов'язки осіб щодо захисту власних інтересів стосовно приватної інформації, побудувавши його таким чином: розділ 1 - загальні положення, розділ 2 - перелік персональних даних як об'єкта захисту, розділ 3 - перелік суб'єктів доступу до персональних даних та їх повноваження, розділ 4 - режим охорони персональних даних, розділ 5 - відповідальність за порушення законодавства про персональні дані.

У законопроекті необхідно визначити, що держава здійснює регулювання роботи з персональними даними в формах: ліцензування роботи з персональними даними, реєстрації баз персональних даних, сертифікації інформаційних систем персональних даних, укладення міждержавних угод щодо транскордонної передачі персональних даних.

2. Законодавчо закріпити поняття службової таємниці. При цьому необхідно внести зміни до Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, затвердженої постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893.

3. Підготувати Закон України "Про участь України в міжнародному інформаційному обміні" з метою створення умов для ефективної участі України в міжнародному інформаційному обміні в межах єдиного світового інформаційного простору, захисту інтересів держави, а також законних прав й інтересів фізичних та юридичних осіб при здійсненні цього обміну. Об'єктами міжнародного інформаційного обміну відповідно до зазначеного закону мають бути: документована інформація, інформаційні ресурси, інформаційні продукти, інформаційні послуги, засоби міжнародного інформаційного обміну.

У цьому законі слід передбачити порядок передачі секретної інформації за кордон, запровадження обліку секретної інформації, яка передається іноземним державам та міжнародним організаціям і одержана від них, який би детально регламентував процедуру взаємного обміну таємною інформації між Україною та іноземними державами та міжнародними організаціями.

4. Уніфікувати з країнами Європи категорії розмежування доступу до інформації.

5. У Законі України "Про інформацію" передбачити виключний перелік видів таємної інформації, до якого віднести: державну, комерційну й банківську таємниці. Усі інші види інформації з обмеженим доступом слід відносити до конфіденційної інформації. Враховуючи важливість та складність проблеми, а також необхідність залучення до її вирішення всіх зацікавлених органів державної влади, доцільно обговорити питання можливої координації цієї діяльності РНБО України.

Для забезпечення захисту інформаційного простору від негативного зовнішнього впливу, необхідно ухвалити Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", який би містив:

– вимоги та правила захисту інформації в електронних мережах, яка є власністю держави, або інформації з обмеженим доступом, захист якої гарантується державою;

– обов'язкові умови захисту інформації при наданні послуг передачі даних, зокрема з використанням Інтернету;

– механізми проведення моніторингу мереж передачі даних виключно на засадах національного та міжнародного законодавства, зокрема положень резолюцій Ради Європи;

– обов'язкове збереження Інтернет-провайдерами відомостей про Інтернет-трафік протягом півроку та надання інформації про нього за рішенням суду.

На сьогодні однією із загроз у сфері інформаційної безпеки в Україні є незаконне виробництво, поширення та продаж спеціальних технічних засобів негласного отримання інформації (СТЗ). Стрімкий розвиток інформаційних технологій дає змогу спрогнозувати кількісне і якісне зростання злочинності у сфері високих технологій, зокрема злочинів з використанням спеціальних технічних засобів.

Враховуючи викладене, з метою протидії незаконному обігу та використанню СТЗ пропонуємо:

1. Встановити кримінальну відповідальність за несанкціоновану торгівлю, виробництво та розроблення СТЗ (чинним законодавством передбачено відповідальність за незаконне використання, придбання або зберігання спеціальних технічних засобів негласного отримання інформації - ст. 359 КК України та ст. 195-5 КУпАП).

2. Обмежити кількість державних структур, до складу яких входять підрозділи технічного документування - залишити право мати такі підрозділи лише СБ України.3. Запровадити обов'язкове ліцензування ДССЗІ електронно-обчислювальної техніки для організацій, підприємств, установ, де обробляється інформація з обмеженим доступом, яка є власністю держави, (ІзОД). Посилити контроль за дотриманням вимог щодо категорування технічного обладнання та приміщень, де проводиться обробка ІзОД.

4. Розглянути можливість регулярного проведення ДССЗІ перевірок об'єктів, де обробляється ІзОД, яка є власністю держави;

5. СБ України організувати тісну взаємодію з органами МВС, Державної митної служби, СЗР та ГУР МО (Головним управлінням розвідки Міністерства оборони) України з метою виявлення каналів незаконного ввезення в державу СТЗ іноземного виробництва.

Транснаціональний характер комп'ютерної злочинності зумовив прийняття та ратифікацію країнами-членами Ради Європи Конвенції про кіберзлочинність, прийнятої 23 листопада 2001 р. (далі Конвенція). Україна ратифікувала її у вересні 2005 року. Отже, українське законодавство (зокрема, норми чинного КК України) згідно з ч. 1 ст. 9 Конституції України, повинно бути приведено у відповідність до її положень. Вважаємо за необхідне висунути такі пропозиції з удосконалення українського законодавства з протидії кіберзлочинності:

1. Розділ XIV Кримінального кодексу України "Злочини у сфері охорони державної таємниці, недоторканості державних кордонів, забезпечення призову та мобілізації" потребує розмежування на окремі групи. Злочини, безпосереднім об'єктом яких є інформація з обмеженим доступом, доцільно помістити в окремий розділ (це буде відповідати положенням Конвенції), або об'єднати з розділом XVI (скоригувавши при цьому назву розділу XIV, виключивши слова "охорони державної таємниці"). Відповідно назву розділу пропонується викласти в такій редакції: "Злочини проти інформаційної безпеки".

При конструюванні диспозицій статей зазначеного розділу слід використовувати кримінально-правові норми бланкетного характеру, що дозволить значно скоротити чисельність статей у межах розділу та уникнути необхідності постійної синхронізації норм кримінального та Інформаційного законодавства.

2. В новий розділ "Злочини проти інформаційної безпеки" КК України включити норми про відповідальність за:

– умисне перехоплення технічними засобами, без права на це, інформації шляхом фіксації електромагнітних випромінювань комп'ютерної системи, яка містить в собі такі дані (ст. 3 Конвенції);

– умисне несанкціоноване уведення, зміні, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних (ст. 7 Конвенції).

3. Доповнити чинні КК України та КУпАП України нормами, які б передбачали відповідальність юридичних осіб, якщо злочинне діяння вчинено в їхніх інтересах відповідно до ст. 12-13 Конвенції (наприклад, розповсюдження вірусів в інтересах організації-власника та розробника антивірусних програм, загальні підстави відповідальності за яке передбачені ст. 361-1 КК України). За вчинення таких діянь вбачається за можливе передбачити штраф, позбавлення ліцензії на право заняття окремими видами діяльності або ліквідацію юридичної особи. Як підставу для розмежування злочинів і адміністративних правопорушень, а також диференціації покарань можна використати граничну межу розмірів збитків, спричинених діянням (наприклад, збитки на суму 100 неоподаткованих мінімумів доходів громадян).

Отже, ефективна реалізація нових норм вітчизняного законодавства потребує вжиття відповідних організаційних заходів, зокрема:

– розвитку з огляду на транснаціональний характер комп'ютерних злочинів міжнародної взаємодії правоохоронних та спеціальних органів у цій сфері;

– створення спільного для правоохоронних органів обліку осіб (фізичних та юридичних), які робили спроби або без установленого дозволу проникали в комп'ютерні системи, а також причетних до інших правопорушень у сфері інформаційних технологій;

– створення спеціалізованої лабораторії для обробки електронних доказів, проведення спеціалізованої експертизи з метою удосконалення розслідування комп'ютерних злочинів;

– сприяння розробленню національних програмних продуктів, створенню перспективних інформаційних технологій із метою зменшення залежності від програмного та апаратного забезпечення іноземного виробництва, що містить загрозу застосування недокументованих можливостей;

– вирішення питання щодо підготовки фахівців у сфері інформаційних технологій виключно у профілюючих освітніх закладах у кількості, що відповідає потребі, а також подальшого працевлаштування найкращих випускників у державних установах на пільгових умовах з метою недопущення відпливу за кордон кваліфікованих кадрів.

З огляду на посилення процесів глобалізації необхідно внести зміни та доповнення до законів України "Про друковані засоби масової інформації (пресу) в Україні", "Про телебачення і радіомовлення", якими встановити, що ЗМІ, котрі мають закордонні аналоги, повинні містити не менше 50% інформації українського походження.

Водночас, забезпеченню поширення у світі об'єктивних уявлень про нашу країну сприяла б допомога держави провідним українським агентствам, національним теле- і радіокомпаніям, окремим друкованим засобам масової інформації у відкритті кореспондентських пунктів за кордоном та розширенні кількості зарубіжних споживачів їх продукції.

З метою посилення захисту інформації, що стоновить державну таємницю, на об'єктах інформаційної діяльності необхідно:

– посилити контроль із боку міністерств та відомств за підпорядкованими установами щодо питання охорони державної таємниці;

– передбачити в державному бюджеті статті видатків з технічного та криптографічного захисту інформації;

– розробити систему державної підтримки та інвестування вітчизняних виробництв і проектів, спрямованих на створення якісно нових інформаційно-технічних засобів і технологій захисту;

– поліпшити якість підготовки спеціалістів у галузі захисту інформації, що становить державну таємницю.

– Існує нагальна потреба відкрити науково-дослідну роботу (НДР) "Шляхи та механізми забезпечення інформаційної безпеки", замовником якої має бути, на нашу думку, РНБО України. Серед основних наукових завдань, які мають бути вирішені у межах НДР, зокрема, необхідно забезпечити:

– наукове обґрунтування методологічних основ розробки Концепції інформаційної безпеки, Національної стратегії інформаційної безпеки й інших керівних документів у сфері забезпечення інформаційної безпеки;

– удосконалення методики інформаційного забезпечення розробки, прийняття та впровадження державно-управлінських рішень на стратегічному рівні управління;

– розроблення методики та моделі оцінки ефективності інформаційної політики держави, складовою якої має бути методика прогнозування негативних наслідків державно-управлінських рішень, у разі їх впровадження;

– визначення методології, технології та розробки програмно-методичного комплексу виявлення АЗА та СЮ, спрямованих на дискредитацію вищого політичного керівництва;

– вироблення єдиного понятійно-категорійного апарату у сфері забезпечення інформаційної безпеки.

До виконання НДР необхідно залучити: Національну академію СБ України, Державний університет інформаційно-комунікаційних технологій (ДУІКТ), Інститут СЗР України, Інститут військової розвідки МО України, Національний інститут стратегічних досліджень, Військовий інститут Київського національного університету ім. Тараса Шевченка (ВІКНУ), Національну академію МО України, Інститут міжнародних відносин та ін. Необхідно ввести у вищих спеціальних навчальних закладах системи СБ, СЗР, гур МО України, ВІ КНУ та ДУІКТ спецкурс з метою підготовки кваліфікованих фахівців із захисту інформаційного простору від

деструктивного інформаційного впливу, а також налагодити взаємодію щодо обміну науковими і навчально-методичними розробками з протидії СІО та АЗА.

Особливої актуальності у забезпеченні інформаційної безпеки в сучасних умовах набувають технології інформаційного менеджменту, тобто управління інформацією. Переваги цього підходу полягають у тому, що він може використовуватися як для атаки, так і для захисту інформаційного простору держави.

Висновки до третього розділу

Існуюча система нормативно-правових актів у сфері забезпечення інформаційної безпеки України потребує удосконалення, оскільки в Україні поки що немає нормативних актів концептуального рівня, які б предметно стосувалися регулювання інформаційної сфери та забезпечення інформаційної безпеки держави. Значна кількість нормативних актів (як законів, так і підзаконних актів, неузгоджених не лише з нормами міжнародного законодавства, але й між собою) суттєво знижує ефективність цієї діяльності.

Одним з найважливіших чинників національної безпеки країни є її економічний потенціал, під яким треба розуміти сукупність матеріальних і духовних сил суспільства, а також спроможність держави мобілізувати ці сили для забезпечення своєї безпеки. В свою чергу, інформація охоплює всі сфери людської діяльності і підвищує цей економічний потенціал країни, забезпечуючи зростання матеріальних і духовних сил суспільства і створюючи умови для можливостей, пов’язаних з координацією та мобілізацією. Крім того, вона створює матеріальні і інтелектуальні ресурси країни для ефективного захисту від агресивних в інформаційному відношенні держав. З вищесказаного очевидно, що державна політика в сфері формування інформаційних ресурсів і інформатизації повинна бути

спрямована на створення умов для ефективного і якісного інформаційного забезпечення рішення задач соціально-економічного розвитку країни.

Розгляд проблем інформаційної безпеки держави дає можливість стверджувати, що забезпечення інформаційної безпеки покладається на інформаційну організацію держави. Ця організація повинна гарантувати інформаційну безпеку держави та її суб'єктів в наш час глобалізації та зростання загроз з боку міжнародного тероризму. На жаль, в Україні існує дуже багато негативних факторів, які перешкоджають чи утруднюють створення такої інформаційної організації, і не останнім з них є неузгодженість органів державної влади щодо забезпечення інформаційної безпеки. Отже, наукове осмислення комплексу проблем, пов'язаних з розробкою та втіленням у життя державної політики в інформаційній сфері, сьогодні набуває особливого значення, оскільки їх розв'язання сприятиме розвитку в Україні інформаційного суспільства і, таким чином забезпеченню національної та інформаційної безпеки нашої держави.

ВИСНОВКИ

За результатами роботи:

1. Досліджено теоретичні засади інформаційної безпеки держави. Поняття інформаційної безпеки включає в себе з одного боку забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, а з іншого - контроль за непоширенням таємної інформації, сприяння цілісності суспільства, захисту від негативних інформаційних впливів.

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) по відношенню до небезпечних (дестабілізуючих, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

2. Проаналіовано нормативно-правову основу забезпечення інформаційної безпеки України. За роки незалежності в Україні закладено законодавчі основи системи забезпечення інформаційної безпеки, зокрема було напрацьовано великий масив нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері.

На найвищому рівні - норми Конституції України, які закріплюють концептуальні положення національної безпеки України в усіх сферах її існування, а також Концепцію національної безпеки України, Доктрину інформаційної безпеки України та Закон України "Про національну безпеку України". Ці документи враховують основні положення міжнародних договорів і угод, ратифікованих Україною, які стосуються її національної безпеки.

На другому рівні - закони конститутивного напрямку, де визначаються важливі положення щодо забезпечення національної безпеки в

інформаційній сфері ("Про Основні засади розвитку інформаційного суспільства в Україні" та інші).

На третьому рівні - закони України інституційного рівня, де закріплені основні форми діяльності державних органів у процесі забезпечення національної безпеки в інформаційній та інших сферах життєдіяльності особи, суспільства та держави (зокрема "Про оборону України", "Про Збройні Сили України тощо).

У структурі нормативно-правової бази забезпечення національної безпеки України в інформаційній сфері особливе місце посідають укази та розпорядження Президента України, а також акти (постанови, декрети) Кабінету Міністрів України. Ці нормативні акти є незаконними й видаються з метою конкретизації та підвищення якості вирішення завдань забезпечення інформаційної безпеки.

3. Проаналізувавши стан інформаційної безпеки України можна зазначити, що:

- державна політика щодо захисту національних інтересів в інформаційному просторі не відповідає сучасним вимогам;

- практично відсутній громадський контроль за суб'єктами негативних інформаційних впливів на людину, суспільство і державу;

- державні посадовці, які уповноважені приймати рішення із захисту інформаційного простору, недостатньо усвідомлюють важливості цієї сфери як інтегруючої складової національної безпеки;

- нагальною потребою на сучасному етапі є кардинальне удосконалення інформаційних взаємозв'язків і взаємовідносин між людиною, суспільством та державою;

- проблема захисту національних інтересів в інформаційному просторі має стратегічний, комплексний, довгостроковий характер і потребує свого вирішення спільних зусиль з боку держави, суспільства і бізнесу.

В результаті нашої роботи були наведені такі пропозицій щодо покращення системи управління інформаційною безпекою держави в Україні.

Ефективна реалізація стратегічних пріоритетів, основних принципів і завдань державної політики інформаційної безпеки потребує вдосконалення правових та організаційних механізмів управління інформаційною безпекою, його відповідного інтелектуально-кадрового і ресурсного забезпечення, зокрема вдосконалення законодавства з питань національної безпеки, насамперед шляхом:

− розвитку правових засад управління національною безпекою через розробку відповідних законів, концепцій, доктрин, стратегій і програм, зокрема антикорупційного законодавства, Національної програми протидії тероризму та екстремізму, Концепції розвитку Воєнної організації держави, Національної стратегії формування інформаційного суспільства, Доктрини інноваційного та науково-технологічного розвитку тощо;

− розробка та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними європейськими стандартами, зокрема з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність;

− приведення законодавства з питань охорони державної таємниці до європейських стандартів;

− розробка та впровадження загальнодержавної системи визначення та моніторингу порогових значень показників (індикаторів), що характеризують рівень захищеності національних інтересів у різних сферах життєдіяльності та виникнення реальних загроз національній безпеці.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Богунов В. С. Щодо проблеми законодавчого врегулювання моніторингу телекомунікацій / В. С. Богунов // Матер, наук.-практ. конф. 29 червня 2014 р. "Концептуальні засади забезпечення державної безпеки України". - К.: НА СБУ, 2014. - С. 53-56.

2. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: Навч. посібник / В. А. Ліпкан, Ю. Є. Максименко, Л. В. Желіховськии. - К.: КНТ, 2010. - 280 с. (Серія: Національна і міжнародна безпека).

3. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності: Навч. посібник / А. І. Марущак. - К.: Скіф, КНТ, 2018. - 344 с.

4. Марущак А. І. Правомірні засоби доступу громадян до інформації: Науково-практичний посібник / А. І. Марущак. - Біла церква: Буква, 2016. - 432 с.

5. Петрик В. М. Соціально-правові основи інформаційної безпеки: Навч. посібник / В. М. Петрик, А. М. Кузьменко, В. В. Остроухов / За ред. В. В. Остроухова. - К.: Росава, 2010. - 496 с.

6. Приватне життя і поліція. Концептуальні підходи. Теорія та практика / Відп. ред. Ю. І. Римаренко. - К.: КНТ, 2006. - 740 с. - (Людина. Суспільство. Поліція)

7. Савельев Д. Некоторые проблемы международного права телекоммуникаций [Електронний ресурс] // Інтернет-сторінка "Право та інтернет".

8. Системна інформатизація законотворчої та правоохоронної діяльності: Монографія / Кер. авт. кол. М. Я. Швець; за ред. В. В. Дурдинця, О. В. Зайчука, В. Я. Тація. - К.: Навчальна книга. - 2015. - 639 с.

9. Фронтов В. Регулирование телекоммуникаций в России и странах СНГ: Монография / В. Фронтов, В. Тихвинский. – К.: Горячая линия Телеком, 2013. - 368 с.

10. Юдін О. К. Інформаційна безпека держави: Навчальний посібник / О. К. Юдін, В. М. Богуш. - Х.: Консул, 2015. - 576 с.

11. Конституція України: ухвалена на п'ятій сесії Верховної Ради України 28 червня 1996 р. // Відомості Верховної Ради (ВВР) України - 1996. - № 30. - Ст. 141.

12. Закон України "Про національну безпеку України" від 21 червня 2018 р. № 2469-VIII // ВВР України. - 2008. - № 31. - Ст. 241.

13. Закон України "Про інформацію" від 2 жовтня 1992 р. // ВВР України. - 1992. - № 48. - Ст. 650.

14. Закон України "Про державну таємницю" від 21 січня 1994 р. // ВВР України. - 1994. - № 16. - Ст. 93.

15. Закон України "Про телекомунікації" від 18 листопада 2003 р. // ВВР України. - 2004. - № 12. - Ст. 155.

16. Закон України "Про зв'язок" від 16травня 1995 р. (в редакції від 5 червня 2003 р.) // ВВР України. - 2006. - № 30. - Ст. 258.

17. Закон України "Про радіочастотний ресурс" від 1 червня 2000 р. // ВВР України - 2000. - № 36. - Ст. 298.

18. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" // ВВР України. - 2007. - № 12. - Ст. 102.

19. Закон України "Про Національну програму інформатизації" від 4 лютого 1998 р. // ВВР України. -1998. - № 27-28. - Ст. 181.

20. Закон України "Про концепцію Національної програми інформатизації" // ВВР України. -1998. -№ 75 -110 с.

21. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 р. // ВВР України. -2006.-№26. - Ст. 347.

22. Закон України "Про захист суспільної моралі" // ВВР України. - 2004. - № 14. - Ст. 192.

23. Закон України "Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації" від 23 вересня 1997 р. // ВВР України. - 1997. - № 49. - Ст. 299.

24. Закон України "Про підприємництво" від 7 лютого 1991 р. № 698-ХП // ВВР України. - 1991. - № 14. - Ст. 168.

25. Закон України "Про ліцензування певних видів господарської діяльності" від 1 червня 2000 р. // ВВР України. - 2000. - № 36. - Ст. 299.

26. Закон України "Про банки і банківську діяльність" від 7 грудня 2000 р. № 2121-ПІ // ВВР України. - 2001. - № 5-6. - Ст. 30.

27. Указ Президента України № 663/97 "Про рішення Ради національної безпеки і оборони України від 17 червня 1997 року "Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин" [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

28. Указ Президента України від 27 вересня 1999 р. № 1229 "Про затвердження Положення про технічний захист інформації в Україні" [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

29. Указ Президента України "Про впровадження системи стратегічного планування" від 30 квітня 1999 р. № 460 [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

30. Указ Президента України "Про заходи щодо захисту інформаційних ресурсів держави" від 10 квітня 2000 р. // Офіційний вісник України. - 2000. - № 15.

31. Указ Президента України "Про удосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади" від 14 липня 2000 р. // Урядовий кур'єр. - 2000. - 18 лип.

32. Указ Президента України "Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних" від 24 вересня 2001 р. № 891 [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

33. Указ Президента України "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 " від 23 серпня 2001 р. № 731/2001 // Офіційний Вісник України. - 2001. - № 35. -Ст. 1622.

34. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року з питання "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки" від 6 грудня 2001 р. № 1193/2001 // Офіційний Вісник України 2001. - № 50. - Ст. 2228.

35. Указ Президента України "Про заходи щодо забезпечення інформаційної безпеки держави" від 18 вересня 2002 р. // Офіційний Вісник України. - 2002. - № 38. - Ст. 1771.

36. Указ Президента України від 23 квітня 2008 р. № 377/2008 "Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року "Про невідкладні заходи щодо забезпечення інформаційної безпеки України" [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

37. Указ Президента України "Про удосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади" від 14 липня 2000 р. // Урядовий кур'єр. - 2000. -18 лип.

38. Постанова Кабінету міністрів України від 27 листопада 1998 р. № 1893 "Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави" [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

39. Постанова Кабінету Міністрів України "Про затвердження Порядку підключення до глобальних мереж передачі даних" від 12 квітня 2002 р. № 522 [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

40. Постанова Кабінету Міністрів України "Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади" від 4 січня 2002 р. № 3 [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

41. Постанова Кабінету Міністрів України "Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах" від 16 листопада 2002 р. № 1772 [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

42. Постанова Кабінету Міністрів України від 19 липня 2006 р. № 1000 "Деякі питання обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави" [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

43. Наказ Служби безпеки України та Державної податкової адміністрації України "Про взаємодію Служби безпеки України та органів державної податкової служби України з профілактики, виявлення, припинення, розкриття та розслідування злочинів, інших правопорушень у сфері розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації та торгівлі ними" від 9 липня 2001 р. № 176/278 // Офіційний Вісник України. - 2001. - № 31. - Ст. 1432.

44. Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України № 440 від 12 серпня 2005 р. [Електронний ресурс]. - Режим доступу: www.rada.gov.ua

45. Бєляков К. І. Проблеми законодавчого регулювання у сфері користування інформацією з обмеженим доступом в Україні / К. І. Бєляков, Ю. П. Мірошник // Стратегічна панорама. - 2014. - № 3. - С. 171-177.

46. Кормич Б. А. Правова регламентація інформаційної безпеки держави / Б. А. Кормич // Держава і право: зб.наук. пр. Юридичні і політичні

науки. - Вип. 17. - К.: Ін-т держави і права ім. В.М. Корецького НАН України, 2002. - С. 193-198.

47. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки / В. К. Конах // Стратегічні приоритети. - 2012. - № 3(24). - С. 152-157.

48. Демський Е. Співвідношення адміністративної ігосподарської відповідальності / Е. Демський // Юридична Україна. - 2015. - № 9. - С. 24-30.

49. Масляниця Й. У. Інформаційні ресурси України :проблеми державного управління: монографія / Й. У. Масляниця, О. В. Соснін, Л. Є. Шиманський. - К.: НІСД, 2002. - 141 с.

50. Про Воєнну доктрину України: указ Президента України від 15.06.2004 р. № 648/2004 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/648/2004.

51. Про основні засади розвитку інформаційного суспільства в Україні: закон України від 09.01.2007 р. № 537-V // ВВР України. - 2007. - № 12. - Ст. 102.

52. Про основи національної безпеки України: закон України (із змінами, внесеними згідно із законами від 15.12.2005 р. № 3200-IV // ВВР. - 2006. - № 14. - Ст. 116; від 01.07.2010 р. № 2411-VI // ВВР. - 2010. - № 40. - Ст. 527) // Відомості Верховної Ради України. - 2003. - № 39. - Ст. 351.

53. Про Стратегію національної безпеки України: указ Президента України від 26.05.2015 р. № 287/2015 [Електронний ресурс]. – Режим доступу:http://www.president.gov.ua/documents/5728.html.

54. Про Доктрину інформаційної безпеки України: указ Президента України від 8.07.2009 р. № 514/2009 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/9570.html.

55. Про Концепцію державної інформаційної політики : проект Закону України від 13.10.2010 р. № 7251 [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb_n/webproc4_1

56. Виноградова Г. В. Інформаційне право: Навч. посібник / Г. В. Виноградова. - К.: МАУП, 2011. - 144 с.

57. Галамба М. Інформаційна безпека України: поняття, сутність та загрози / М. Галамба [Електронний ресурс]. - Режим доступу: http://www.justinian.com.ua/article.php?id=2463

58. Гуцалюк М. В. Організація захисту інформації: Навч. посібник / М. В. Гуцалюк. - К. : Альтерпрес, 2012. - 224 с.

59. Дмитренко М. Проблеми інформаційної безпеки України / М. Дмитренко [Електронний ресурс]. - Режим доступу: http://social-science.com.ua/article/807

60. Василенко Д. П. Законодавство провідних країн світу в сфері захисту інформації / Д. П. Василенко [Електронний ресурс] – Режим доступу: http://www.kdu.edu.ua/statti/2010-2-1(61)/128.PDF

61. Про захист інформації в автоматизованих інформаційних системах: Закон України [Електронний ресурс]: офіц. вид. станом на 5.07.94 р.; № 80. – Режим доступу: URL: http://rada.gov.ua.

62. Про інформацію: Закон України [Текст]: офіц. вид. станом на 2 жовтня 1992 р. // ВВР України. - 1992. - № 48. [Зміни внесено Законами України № 1642-III від 06.04.2000 р. // ВВР України. - 2000. - № 27; № 304–III від 07.02.2002 р.]

63. Про національну безпеку України: Закон України [Електронний ресурс]: офіц. вид. станом на 21.06.2018 р.; № 2469-VIII. - Режим доступу: URL: http://rada.gov.ua.

64. Черненко Т. В. Пріоритети державної інформаційної політики в умовах гібридної війни / Т. В. Черненко // Стратегічні пріоритети. - № 4 (37), 2015. - С. 83-92.