

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію

Завідувач кафедри УІКБ

доктор економічних наук, доцент

_____ С.В.Легомінова

«__» _____ 20__ р.

До захисту

Завідувач кафедри УІКБ

доктор економічних наук, доцент

_____ С.В.Легомінова

«__» _____ 20__ р.

ДИПЛОМНА РОБОТА
на тему:
НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

СТУДЕНТ:

Байда Ярослав Володимирович

(підпис)

КЕРІВНИК:

к.е.н., доц. Мордас Ірина Василівна

(підпис)

НОРМОКОНТРОЛЕР:

к.в.н., доц. Якименко Юрій Михайлович

(підпис)

Київ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
 Навчально-науковий інститут захисту інформації
 Кафедра управління інформаційною та кібернетичною безпекою
 Освітньо-кваліфікаційний рівень – бакалавр
 Спеціальність «Кібербезпека»
 Спеціалізація «Управління інформаційною та кібернетичною безпекою»

"ЗАТВЕРДЖУЮ"

Завідувач кафедри УІКБ

_____ С.В.Легомінова

(підпис)

“ ____ ” _____ 2020 р.

ЗАВДАННЯ

на дипломну роботу

студенту Байді Ярославу Володимировичу

1. **Тема роботи** «Нормативно-правове забезпечення інформаційної безпеки держави», затверджена наказом по університету 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** полягає у визначенні перспектив розвитку нормативно-правової бази забезпечення інформаційної безпеки в Україні.
6. **Перелік питань, які мають бути розроблені:**
 1. Провести аналіз основних проблем забезпечення інформаційної безпеки держави.
 2. Дослідити основні нормативно-правові акти щодо забезпечення інформаційної безпеки України.
 3. Визначити механізми забезпечення інформаційного суверенітету України.
7. **Дата видачі завдання** “ ____ ” _____ 20__ р.

КАЛЕНДАРНИЙ ПЛАН

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

№ з/п	Етапи бакалаврської роботи	Термін виконання етапів	Примітка
1.	Визначення об'єкту, предмету, мети та завдань дослідження.	11.03.2020	
2.	Збір та аналіз літератури.	18.03.2020	
3.	Написання 1-го розділу роботи.	01.04.2020	
4.	Написання 2-го розділу роботи.	15.04.2020	
5.	Написання 3-го розділу роботи.	29.04.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	06.05.2020	
7.	Оформлення роботи.	12.05.2020	
8.	Оформлення презентації.	14.05.2020	
9.	Отримання рецензії на роботу.	20.05.2020	
10	Захист в ДЕК.	___.06.2020	

Студент

(підпис)

Я.В.Байда

Науковий керівник

(підпис)

І.В.Мордас

РЕФЕРАТ

Дипломна робота присвячена дослідженню нормативно-правового забезпечення інформаційної безпеки держави. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел, що містить 11 найменувань. Загальний обсяг роботи становить 62 аркуші, з яких 1 аркуш займає список використаних джерел.

Об'єктом дослідження є інформаційна безпека держави.

Метою роботи є визначення перспектив розвитку нормативно-правової бази забезпечення інформаційної безпеки в Україні. Для цього у роботі використовуються методи системного аналізу, наукової абстракції, порівняння та ін.

Як результат у роботі проведено аналіз основних проблем забезпечення інформаційної безпеки держави; досліджено основні нормативно-правові акти щодо забезпечення інформаційної безпеки України; визначено механізми забезпечення інформаційного суверенітету України.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та удосконаленні нормативно-правового забезпечення інформаційної безпеки держави.

Ключові слова: ІНФОРМАЦІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ.....	6
ВСТУП	7
РОЗДІЛ 1. ОСНОВНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ.....	9
1.1. Загрози інформаційній безпеці держави.....	9
1.2. Необхідність нормативно-правового забезпечення інформаційної безпеки при побудові інформаційного суспільства в державі.	18
1.3. Основні функції нормативної бази інформаційної безпеки держави.....	24
Висновки до першого розділу.....	28
РОЗДІЛ 2. ОСНОВНІ НОРМАТИВНО-ПРАВОВІ АКТИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ.....	30
2.1. Положення Закону України “Про інформацію”.	30
2.2. Вимоги Національної програми інформатизації.....	33
2.3. Особливості Доктрини інформаційної безпеки України.	43
Висновки до другого розділу	47
РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ	48
3.1. Механізми протидії загрозам у сфері інформаційної безпеки України. .	48
3.2. Забезпечення інформаційного суверенітету України.	54
Висновки до третього розділу.....	56
ВИСНОВОК.....	57
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	58

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	- інформаційна безпека
СУІБ	- система управління інформаційною безпекою
ІС	- інформаційна система
ІТС	- інформаційно телекомунікаційна система
КСЗІ	- комплексна система захисту інформації
ТЗ	- технічне завдання
НСД	- несанкціонований доступ
ПЗ	- профілі захисту
ІТ	- інформаційні технології
ПБ	- політика безпеки

ВСТУП

Актуальність теми. Інформація завжди була як найважливішим об'єктом, так і засобом боротьби між людьми. Неможливо заперечувати факти здійснення інформаційного впливу на широку аудиторію протягом усіх етапів історичного розвитку, хоча в різні періоди інтенсивність застосування тих чи інших способів впливу, як і досконалість його організації, значною мірою відрізнялися.

На сучасному етапі нормативно-правова база та закони України у сфері інформаційної безпеки формують основну поведінку держави у формуванні захищеності інформаційного простору та інформаційної війни; визначають вимоги та засоби забезпечення інформаційної безпеки та описують можливі загрози та шляхи їх вирішення.

Тому створення однозначних вимог до шляхів забезпечення інформаційної безпеки, що описані в нормативно-правовій базі є надзвичайно важливим в наш час.

З огляду на зазначене тема дипломної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки держави.

Мета і завдання дослідження. **Мета роботи** полягає у визначенні перспектив розвитку нормативно-правової бази забезпечення інформаційної безпеки в Україні.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання:**

1. Провести аналіз основних проблем забезпечення інформаційної безпеки держави.
2. Дослідити особливі нормативно-правові акти щодо забезпечення інформаційної безпеки України.

3. Визначити механізми забезпечення інформаційного суверенітету України.

Об’єкт дослідження – інформаційна безпека держави. **Предмет дослідження** – нормативно-правове забезпечення інформаційної безпеки держави.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу та теорії інформаційної безпеки.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та удосконаленні нормативно-правового забезпечення інформаційної безпеки держави.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформаційної інфраструктури держави у відповідності до цілей, можливостей та ресурсів.

Розділ 1

ОСНОВНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Загрози інформаційній безпеці держави

У сучасних умовах глобальних і регіональних інформаційних протистоянь, зіткнення різновекторних інформаційних національних інтересів, деструктивних комунікативних впливів, поширення інформаційної агресії та експансії, захист інформаційного національного простору і гарантування інформаційної безпеки є пріоритетними стратегічними завданнями всіх сучасних держав в системі інформаційних глобальних відносин.

Збереження інформаційного суверенітету та формування ефективної системи безпеки у інформаційній сфері є актуальним завданням і для України, яка досить часто є об'єктом інформаційної зовнішньої експансії, руйнівного інформаційного вторгнення та маніпулятивних пропагандистських технологій.

У сучасних умовах захист інформаційного національного простору від негативних впливів, операцій та війн інформаційно-психологічного характеру, гарантування інформаційної безпеки і інформаційного суверенітету набувають пріоритетного значення і стають чинниками забезпечення та збереження національної ідентичності України і функціонування її як незалежної та суверенної держави.

Проблеми захисту національного інформаційного національного простору та інформаційну безпеку загалом досліджували багато науковців. Зокрема, цю проблему відображено в працях А. Марущака, В. Ліпкана, Б. Кормича, В. Петрика, В. Почепцова і інших фахівців. Проблемні питання та аспекти забезпечення кібернетичної безпеки досліджували В. Бурячок, А.

Бабенко, Р. Лук'янчук, В. Гавловский, Д. Дубов, М. Погорецький, В. Шеломенцев, В. Номоконов та інші науковці. Однак, в працях вищезазначених науковців інформаційна безпека досліджувалася, радше, як складова частина національної безпеки та її невід'ємний компонент. За увагою науковців залишилися проблеми чіткого окреслення та аналізу інформаційних загроз, вивчення джерел їх появи, всебічне дослідження технологій проведення інформаційно-психологічних операцій і війн, а також визначення і обґрунтування методів протистояння негативним інформаційно-психологічним впливам [6].

Зважаючи на вищезазначені малодосліджені аспекти проблем інформаційної безпеки важливим сьогодні є всебічне дослідження проблем гарантування національної інформаційної безпеки, захисту інформаційного простору України з огляду на реальні та потенційні загрози й деструктивні пропагандистсько-маніпулятивні інформаційно-психологічні впливи.

Інформаційна безпека є складовою компонентою національної безпеки і її зазвичай розглядають як одну з пріоритетних функцій держави. З одного боку, інформаційна безпека передбачає забезпечення всебічного якісного інформування громадян та їх вільного доступу до різноманітних джерел інформації, а з другого – це контроль над непоширенням дезінформації, збереження інформаційного суверенітету, сприяння цілісності суспільства, протидія негативним пропагандистським інформаційно-психологічним впливам, а також захист національного інформаційного простору від інформаційних війн, операцій та маніпуляцій.

Вирішення комплексної проблеми забезпечення інформаційної безпеки дасть змогу і захисту інтересів суспільства держави та громадян, і гарантування прав останніх на отримання всебічної, якісної та об'єктивної інформації.

Існує два аспекти розуміння інформаційної безпеки в контексті національної безпеки держави. З одного боку, інформаційна безпека

розглядається як самостійний елемент системи національної безпеки будь-якої держави, а з другого – інтегрована складова будь-якого іншого виду безпеки: військової, політичної, економічної тощо.

Найповнішим визначенням інформаційної безпеки є таке: це ступінь захищеності життєво важливих інтересів суспільства, держави і особистості, при якому зводиться до мінімуму одержання збитків через неповноту, недостовірність і невчасність інформації, негативні наслідки функціонування інформаційно-телекомунікаційних технологій, негативний інформаційний вплив, а також через несанкціоноване розповсюдження інформації. Це визначення можна вважати оптимальним, так як воно відображає всі аспекти взаємодії між суб'єктами інформаційних відносин.

Сьогодні увага до проблеми гарантування інформаційної безпеки України обумовлена антиукраїнськими впливами, що пропагують ідеї насильства, національної ворожнечі, сепаратизму, і є спробами знищення міжнаціональної злагоди, руйнування національної ідентичності України, посягання на конституційний лад та територіальну цілісність України.

Проблеми гарантування інформаційної безпеки України особливо актуалізуються в контексті війни на Сході України, коли відбувається інформаційна експансія, тенденційне та упереджене висвітлення явищ і фактів, а технології інформаційно-психологічних пропагандистських операцій спрямовані на забезпечення присутності та домінування в українському (а також в глобальному) інформаційному середовищі та на утримання всебічної медійної переваги. Через інформаційно-психологічні пропагандистські кампанії, медіа заходи та акції відбувається вплив не тільки на суспільну свідомість українських громадян, але й на світову громадськість в цілому.

Один з представників об'єднання “Інформаційний супротив” В. Гусаров при дослідженні проблем інформаційної безпеки України, зазначає, що ворог здійснює інформаційно-психологічні атаки з метою активізації

ескалації конфлікту на Сході України, здійснення тиску на українське керівництво аби змусити його погодитися на свій власний сценарій врегулювання конфлікту [22].

В. Гусаров диділяє ряд напрямів інформаційно-психологічних атак, спрямованих проти інформаційної безпеки України:

- 1) Нав'язування думок щодо неспроможності української влади здійснювати керування державою й приймати ефективні рішення;
- 2) Формування негативних суджень щодо воєнно-політичного керівництва України та щодо того, що хаотичні бойові дії спричиняють невинуваті жертви серед сил ООС;
- 3) Поширення поглядів щодо того, що на Сході України українська армія деморалізована і неспроможна вести ефективні бойові дії, а також щодо недовіри особового складу до керівництва держави;
- 4) Нав'язування думки щодо того, що Україна не зможе обійтися без російського газу й що сторонам потрібно повернутися до перегляду газового контракту [22].

Експерт зазначає і те, що цільовою аудиторією ворога зараз є населення власної країни, російськомовна діаспора за кордоном та населення України, зокрема у ОРДЛО (окупованих районах Донецької та Луганської областей), громадяни іноземних (західних) держав, а також країн Митного союзу та БРІКС, які є близькими за політичними поглядами. Відтак, Україна стала об'єктом пропагандистсько-маніпулятивних інформаційно-психологічних впливів, війн, операцій, а її інформаційна безпека опинилася під загрозою.

Отже, можна зазначити, що:

- 1) український інформаційний простір сьогодні є незахищеним від зовнішніх пропагандистсько-маніпулятивних інформаційно-психологічних впливів і є об'єктом інформаційної експансії;
- 2) щодо світового медіа простору, то в ньому не представлений національний український інформаційний продукт, який поширював би

неупереджену, актуальну та об'єктивну інформацію щодо подій в Україні.

Як наслідок цього – світова громадськість відчуває нестачу інформації або компенсує її з інших джерел, що часто дезінформують, надають спотворену, неповну або викривлену інформацію. Разом з тим проти України активно використовується потужний медіаресурс, відбувається експансія іноземних суб'єктів, які представлені на ринку інформаційних послуг, посилюються негативні інформаційно-психологічні впливи, що спрямовані на деформацію реальності та заниження міжнародного іміджу України;

3) діяльність українських ЗМІ щодо об'єктивного систематичного висвітлення фактів, явищ та подій є сьогодні недостатньою й позбавленою стратегічного планування, а інформаційно-комунікативна політика українського уряду в сфері національної безпеки загалом потребує невідкладного перегляду й удосконалення.

Сьогодні рівень інформаційної безпеки держави у значній мірі зумовлений рівнем інформаційної інфраструктури держави. На жаль, як відзначає В.Петрик, низький рівень інформаційної інфраструктури України в загальному сприяє експансії іноземних компаній на ринку інформаційних послуг, а це створює сприятливі умови для виділення та перерозподілу ефірного часу на перевагу іноземних програм, багато з яких засмічують інформаційний простір України своїм власним баченням подій та пропують певний спосіб життя й традиції, деструктивно впливаючи тим самим на державу та суспільство, руйнуючи при цьому морально-етичні засади генофонду української нації.

Недостатній інтелектуальний, професійний і творчий рівень українського виробника інформаційного продукту або послуги, його неконкурентоспроможність не тільки на світовому ринку, але й в Україні, приводять до того, що вітчизняна аудиторія, природно, надає перевагу іноземним інформаційним программам та послугам.

Недостатній контроль з боку держави за дотриманням законів України політичними силами, ЗМІ та окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, призводить до того, що нині трапляються непоодинокі випадки надання ефірного час у теле- та радіопрограмам, спрямованим на руйнування моральних цінностей, свідомості української нації.

Як зазначено у Законі України “Про національну безпеку України” однією з основних загроз інформаційній безпеці є “намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації” [36].

У Доктрині інформаційної безпеки України, визначено такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ, а також мережу Інтернет; деструктивні інформаційні впливи, які спрямовані на піддрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ, а також у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками [10].

Як зазначає Р. Р. Марутян, найсуттєвішою загрозою національній безпеці України в інформаційній сфері є здійснення іноземними державами негативного інформаційно-психологічного впливу на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій та кампаній, спеціальних інформаційних операцій. Це відбувається через систематичне поширення тенденційної, неповної або упередженої інформації про Україну та політичні процеси, що відбуваються на її теренах. Усе це впливає на зовнішню та внутрішню політику нашої держави, знижує її міжнародний імідж, має політичне та економічне підґрунтя [21].

Метою таких інформаційних операцій є забезпечення власних національних інтересів інших держав.

До загроз національній безпеці України в інформаційній сфері також варто зарахувати:

- прояви обмеження свободи слова та доступу громадян до інформації;
- викривлення, спотворення, блокування, замовчування упереджене та тенденційне висвітлення інформації;
- несанкціоноване її поширення; відкрити дезінформацію;
- інформаційну експансію з боку інших держав та руйнівне інформаційне вторгнення у національний інформаційний простір, коли країни з потужнішим інформаційним потенціалом отримали можливість розширити свій вплив через ЗМІ на населення і громадськість менш потужної держави;
- виникнення і функціонування у національному інформаційному просторі держави непідконтрольних їй інформаційних потоків;
- поширення засобами масової інформації культу насильства, жорстокості;
- повільність входження України у світовий інформаційний простір;
- невиваженість державної інформаційної політики та відсутність необхідної інфраструктури в інформаційній сфері;

розміщення дезінформації в Інтернеті.

Варто наголосити, що проти України з боку Російської федерації ведеться інформаційна війна, яка спрямована на нав'язування певних ідеологічних стереотипів, тієї чи іншої суспільної думки за допомогою засобів масової інформації, зокрема через електронні видання.

Війни такого типу є досить поширеними у глобальному інформаційному просторі та їх всебічно досліджують науковці та фахівці. Зокрема, Інститут національно-стратегічних досліджень США та деякі

західні експерти і вчені виокремлюють кілька складових елементів інформаційної війни. Один із них – ведення психологічної війни.

Головне завдання психологічної війни полягає в маніпулюванні масами. Метою такої маніпуляції є:

- внесення в суспільну та індивідуальну свідомість ворожих ідей та поглядів;
- дезорієнтація та дезінформація мас;
- послаблення певних переконань, залякування народу образом ворога;
- залякування супротивника власною могутністю.

У сучасному глобалізованому інформаційному суспільстві, де кіберпростір перетворюється на поле боротьби, вагомими загрозами інформаційній безпеці держави (і України, зокрема) є комп'ютерна злочинність, кібертероризм, кібервійни, які передбачають протистояння національних інтересів у просторі Інтернету, застосування комп'ютерних та інтернет-технологій для нанесення шкоди супротивнику.

Найчастіше технології кібервійни, кібертероризму спрямовані на сферу державної безпеки й оборони і становлять реальну загрозу суверенітету держави.

Отже, проти України широко використовують сучасні технології негативних інформаційно-психологічних впливів, які стають загрозою українському національному інформаційному простору та суверенітету держави.

Гарантування інформаційної безпеки України в умовах дестабілізвальних негативних інформаційно-психологічних впливів та експансіоністської агресивної інформаційної політики Російської федерації, потребує консолідації зусиль на усіх рівнях державної влади та громадянського суспільства.

До основних загроз інформаційній безпеці України, зазначають експерти, можуть бути віднесені обмеження свободи слова та доступу

громадян до інформації, руйнування системи цінностей, духовного та фізичного здоров'я особи, суспільства, негативні зміни їх цільових настанов, маніпулювання громадською думкою з боку державної влади, фінансово-політичних кіл, низький рівень інтегрованості України в світовий інформаційний простір тощо.

Всі загрози інформаційній безпеці поділяють на наступні основні групи:

1. загрози шкідливого впливу відповідної інформації (недостовірної, шкідливої, дезінформації) на особистість, суспільство, державні інтереси;
2. загрози несанкціонованого чи неправомірного впливу сторонніх осіб до інформації й інформаційних ресурсів фізичних та юридичних осіб, органів державної влади та місцевого самоврядування;
3. загрози обмеженню інформаційних прав особистості, механізмам їх реалізації.

Явища та процеси природного й штучного походження, що породжують інформаційні загрози, називають дестабілізуючими факторами.

Джерелами дестабілізуючих факторів можуть бути: окремі особи, організації, різного роду об'єднання, інші держави та відповідно їх органи, організації, громадяни тощо; інформаційні системи та засоби, що є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей та інших причин; природне середовище (катаклізми, природні стихії, катастрофи тощо).

1. Види дестабілізуючих факторів можна поділити на: внутрішньодержавні дестабілізуючі фактори;
2. Правовий вакуум у більшості питань забезпечення інформаційної безпеки;

3. порушення законодавства з питань інформаційної безпеки; політичні конфлікти;
4. відмови, збої, технічні помилки інформаційних систем (засобів);
5. природні явища, що ускладнюють передачу, прийом і зберігання інформації або руйнують інформаційні системи;
6. міждержавні дестабілізуючі фактори, що виникли в результаті конфліктів міждержавних масштабів і проявів (між державами, організаціями та державами, організаціями чи особами різних держав): воєнні, економічні, політичні, терористично-ідеологічні тощо.

1.2. Необхідність нормативно-правового забезпечення інформаційної безпеки при побудові інформаційного суспільства в державі

Сьогодні глобальні тенденції суспільного розвитку варто охарактеризувати такими термінами й поняттями як постіндустріальне суспільство, суспільство, постекономічне суспільство, суспільство знань, інформаційне суспільство споживання, сервісна економіка, нова економіка, інноваційна економіка та низкою інших, подібних до них.

Починаючи із 50-х рр. XX ст. у розвинутих країнах відбувається зміна стадій історичного розвитку однієї на іншу та поступовий перехід до постіндустріального від індустріального суспільства.

У кінці 60-70-х рр. XX ст. запропоновано було багато різноманітних концепцій постіндустріального суспільства. У відповідності до даних концепцій, зміна різних технологічних епох та стадій, галузевий і професійний поділ праці розглядаються як основа поступального розвитку суспільств. Провідна роль у постіндустріальному суспільстві відводиться науці, освіті та сфері послуг.

Постіндустріальне суспільство насамперед характеризується тим, що

при досягненні людством певного рівня економічного добробуту на перший план виступають і набувають особливого значення не економічні свободи і права, а нематеріальні блага, які спрямовані на повний та вільний розвиток людини.

Таким чином, сучасний етап розвитку світової спільноти характеризується суттєвим підвищенням ролі інформації в усіх сферах життєдіяльності. Інформація та знання стають одним зі стратегічних ресурсів соціального та економічного розвитку держави, обов'язковими умовами успішного ведення бізнесу та розвитку особистості. Інформація сьогодні перетворилася у фактор, що істотно впливає практично на усі сфери суспільного життя.

Мьогодні дослідники виділяють низку концепцій, які визначають природу інформації.

Перша концепція має назву лінгвістичної. Вона являє собою визначення інформації за допомогою використання інструментів мовознавчих традицій.

Друга концепція знаходить своє відображення у фізико-математичних науках. У відповідності до цієї концепції, інформація трактується у суто науковому значенні даного поняття. В кожного дослідника цієї концепції свій власний погляд на природу інформації, відмінності потрібно розглядати не як протиріччя та неузгодженості, а скоріше як різноманітність та багатоплановість самої природи інформації, а це зайвий раз підкреслює складність і актуальність даної проблеми.

Третя концепція розуміння природи інформації - соціальна (суспільствознавча) – пов'язана з соціальним і філософським сприйняттям даного феномена. Для прихильників цієї концепції особливий інтерес складають соціальні аспекти інформації. Відкриття і дослідження у цій галузі привели багатьох дослідників до висновку, згідно якого природа інформації міститься у площині теорії відображення й інформаційної взаємодії

нематеріальних та матеріальних об'єктів [39, с. 21].

Одним з найважливіших елементів інформаційної парадигми суспільства є його мережева структура, в основі якої містяться глобальні обчислювальні мережі різноманітного масштабу. Становлення інформаційної парадигми невіддільно пов'язане з якісними і принциповими змінами у житті людей. Це передбачає створення єдиного суспільства і інформаційного простору. В зв'язку з цим, проведення ефективної державної інформаційної політики сьогодні стає важливим стратегічним завданням.

Завдяки розвитку інформаційних телекомунікацій відбувається поява нових можливостей, які сприяють формуванню, становленню й розвитку світового інформаційного суспільства, у якому не лише різноманітні організації, установи, відомства та підприємства володіють й користуються персональними комп'ютерами, що підключені до транскордонних інформаційних мереж, а й практично кожна сім'я має у своїй власності даний технічний пристрій.

Розвиток техніки також сприяє появі нових форм та трансформації існуючих видів діяльності із використанням інформаційних телекомунікаційних мереж: робота, торгівля, виховання, розваги, освіта й інше. У даний час абсолютно кожен член будь-якого суспільства має можливість вільно та у доступі своєчасно одержувати достовірну об'єктивну інформацію, незалежно від того, у якому місці географічного простору він перебуває. Сьогодні також надається можливість вільного спілкування всіх членів суспільства один із одним, перебуваючи у різних місцевостях світу.

В процесі комунікацій відбувається встановлення зв'язків між різними соціальними системами суспільства. Тому комунікація є основним інструментом для формування інформаційного суспільства. В свою чергу Інтернет та засоби масової інформації є провідниками для реалізації політики держави у інформаційній сфері. Передачу інформації, яка транслюється за їх допомогою, можливо розглядати як засіб маніпуляції зі свідомістю людей. За

допомогою цієї маніпуляції нерідко досягаються військові, політичні, комерційні й інші цілі.

В «Стратегії розвитку інформаційного суспільства», що була затверджена Президентом України, зазначається, що інформаційне суспільство в Україні характеризується високим рівнем розвитку телекомунікаційних і інформаційних технологій та їх інтенсивним використанням органами державної влади, громадянами та бізнесом [38, с. 144].

Поняття «інформаційна безпека» можна розглядати з різних точок зору.

Офіційне визначення даного поняття міститься у Доктрині інформаційної безпеки України, що затверджена Президентом України, у відповідності до якої під інформаційною безпекою України розуміють стан захищеності національних інтересів України в інформаційній сфері, які визначаються сукупністю збалансованих інтересів держави, суспільства і особистості.

Аналіз дефініції «інформаційна безпека», що запропонований науковими діячами або закріплений у нормативно-правових актах, засвідчує її визначення як стан захищеності національних інтересів у інформаційній сфері.

Конкретизуючи поняття «інформаційна сфера», сформулюємо його наступним чином: інформаційна безпека – це стан захищеності національних інтересів у інформаційній сфері України, який представляє собою сукупність інформаційної інфраструктури, інформації, суб'єктів, що здійснюють збір, формування, використання та розповсюдження інформації, а також системи врегулювання суспільних відносин, які виникають при цьому [31].

Деякі автори обґрунтовують даний термін через наявність загроз, тобто трактують інформаційну безпеку як ступінь захищеності національних інтересів у інформаційній сфері від зовнішніх і внутрішніх загроз [31].

Один із підходів знайшов своє відображення у роботах учених

технічного профілю. Вони в основному зводять інформаційну безпеку до діяльності щодо захисту властивостей інформаційної інфраструктури та інформації за допомогою технічних та організаційних заходів, ґрунтуючись на положеннях існуючих державних стандартів.

Необхідно також виділити поняття інформаційної безпеки і не через ступінь захищеності національних інтересів у інформаційній сфері, а через можливість та здатність суб'єктів правовідносин забезпечувати, розвивати та захищати інформаційну сферу.

Різноманітність наукових підходів до визначення поняття інформаційна безпека: від вузького - «діяльність щодо захисту властивостей інформації» до широкого - «ступінь захищеності національних інтересів у інформаційній сфері від зовнішніх і внутрішніх загроз» (який включає в себе велику кількість напрямків діяльності: від захисту персональних даних окремих громадян до протиборства у інформаційних війнах) - та відсутність його закріплення у нормативно-правових актах ускладнюють наукове осмислення таких надважливих складових компонентів інформаційної безпеки як система та її структура.

Очевидною є і необхідність розмежування таких понять як безпека інформаційної сфери , інформаційна безпека України, захист інформації й інформаційної структури.

В сучасному світі можна виокремити декілька підходів, відмінних один від одного, до забезпечення інформаційної безпеки держави. Пріоритетним напрямком у першому підході є забезпечення інформаційної відкритості держави, а другого - дозування інформації та забезпечення контролю над доступом до неї.

Раніше у нашій країні проблеми нормативно-правового забезпечення інформаційної безпеки держави не тільки не висувалися, а й фактично повністю ігнорувалися. У даний час зростає значення та роль інформаційної безпеки у межах забезпечення національної безпеки України із таких підстав.

Перше, однією з головних причиною необхідності підтримки на високому рівні інформаційної безпеки є розвиток інформатизації суспільства. Дослідження показують, що розвиток навколишнього інформаційного середовища робить значний вплив на суспільний прогрес і розвиток кожної людини. Тому, інформаційне середовище потребує надійного захисту, в тому числі правової.

Друге, в умовах глобалізації роль інформації зростає. Вона цілком обгрунтовано може вважатися об'єктом і продуктом праці, одним з основних багатств країни, а також стратегічним національним ресурсом.

Третє, в політичній сфері все більшого значення набувають не тільки силові, скільки інформаційні фактори. Наприклад, можливості експлуатувати інтелектуальний потенціал інших країн, поширювати і впроваджувати свої духовні, ідейні цінності, свою культуру, мову, можливості гальмувати духовно-культурний розвиток інших країн, трансформувати і навіть підривати їх духовно-моральні підвалини.

Також слід зважати на той факт, що між науково-технічним прогресом і інформаційною безпекою особистості, суспільства і держави простежується прямо пропорційний зв'язок. У міру розвитку науки і техніки зростає роль і значення інформаційної безпеки.

Варто зазначити, що інформація і інформаційна інфраструктура для розвинених країн стали критичними компонентами, вплив на які здатне викликати великомасштабні аварії, дезорганізувати державне і військове керівництво, фінансову систему, наукові центри, викликати військові конфлікти і поразки в них.

Багато сфери життєдіяльності людини, суспільства і держави важко уявити без останніх досягнень науково-технічного прогресу, які за останні роки проникли в них настільки, що зробили їх залежними. Зросла роль інформації в XXI ст., Який називають століттям інформаційних, як ніколи актуалізує питання про забезпечення інформаційної безпеки. Крім

організаційно-технічної складової забезпечення інформаційної безпеки значну роль в цьому механізмі має виконувати і право.

1.3. Основні функції нормативної бази інформаційної безпеки держави

В сучасних умовах розвитку інформаційного суспільства активно розвивається інформаційна сфера, яка поєднує в собі інформацію, інформаційну інфраструктуру, зокрема інформаційні мережі, інформаційні відносини між суб'єктами цієї сфери, що складаються у процесі збирання, формування, розповсюдження і використання інформації.

Інформаційні відносини займають чільне місце у формуванні інформаційної політики держави, в житті сучасного суспільства, а також в діловому та в особистому житті кожної людини. Це, в свою чергу, обумовлює необхідність розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності.

Зрозуміло, що в демократичній правовій державі такі відносини мають базуватися на сучасній нормативно-правовій базі, що регулює діяльність в інформаційній сфері.

Починаючи з 90-х років ХХ ст. Україна поступово долає складний шлях до високорозвиненого правового суспільства, яке базується на принципах демократії та відкритості інформації.

З моменту набуття незалежності в нашій державі сформоване нове національне законодавство, що регулює суспільні відносини у в інформаційній сфері, зокрема забезпечення інформаційної безпеки держави. Законодавчі норми у цій сфері істотно впливають на нормативно-правове регулювання відносин між суспільством, його членами та державою, між фізичними та юридичними особами тощо. Тобто на сучасному етапі інформаційні відносини виступають, з одного боку, зовнішнім проявом будь-

яких відносин у житті країни, суспільства та громадян, з іншого - тими підвалинами, на яких формується законодавство в інших сферах їх існування.

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 [26, с. 25].

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 розглядаються норми Конституції України, які закріплюють концептуальні положення національної безпеки України в усіх сферах її існування.

Ці документи враховують основні положення міжнародних договорів і угод, ратифікованих Україною, які стосуються її національної безпеки.

На Другому рівні розглядаються закони конститутивного напрямку, де визначаються важливі положення щодо забезпечення національної безпеки в інформаційній сфері.

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.

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.

Висновки до першого розділу

Виявлено, що в українському інформаційному просторі існує безліч дестабілізуючих факторів, які згубно впливають на людину, суспільство та саму державу в цілому. Значний відсоток загроз, які існують на даний момент в Україні, викликані з боку Російської Федерації. РФ проводить інформаційну експансію, інформаційно-психологічний вплив на суспільство, пропаганду сепаратизму і т.д. Росія вдало проводить свою політику відносно інформаційного простору України по причині того, що ІІ є незахищений від зовнішніх негативних впливів, мала кількість українського продукту на медіа ринку, через що Україна не може спростувати або поширити актуальну і правдиву інформацію, вітчизняні ЗМІ погано працюють.

Проаналізовано Закони України “Про основи національної безпеки” та Доктрину інформаційної безпеки України.

Зроблено висновок, що однією з головних загроз ІБ є відсутність правдивої, невикривленої та неупередженої інформації в українському ЗМІ, медіа та інтернеті.

Також потрібно відмітити, що в сучасних умов поширеним є кібервійна та кібертероризм. Вони є серйозною загрозою для національного ІІ та суверенітету держави.

Проаналізовано західну практику та аргументовано необхідність створення якісної нормативно-правовій базі;

- модернізації системи інформаційної безпеки в цілому;
- розвитку національного продукту, послуг і комунікації різних органів влади під час роботи над державної політикою в сфері інформаційної безпеки.

Аналізуючи місце нормативно-правової бази в інформаційній безпеці, то можна сказати, що вона необхідна для підвищення інформатизації суспільства.

Також в умовах глобалізації інформація є продуктом, об'єктом праці, а також національним ресурсом. Вона існує в усіх сферах нашого життя, тому нормативно-правове забезпечення є актуальним питанням на даний момент і в умовах сучасних інформаційних війн є важливо, щоб нормативно-правова база, як швидше оновлювалась, аби вміло захищати свої та державні інформаційні інтереси.

На сьогоднішній день Україна зробила великий крок в створені нормативної бази, яка змогла б підтримувати інформаційну безпеку.

Дане дослідження можна використовувати з метою покращення нормативної бази України та виявлення її позитивних і негативних сторін.

Розділ 2

ОСНОВНІ НОРМАТИВНО-ПРАВОВІ АКТИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Положення Закону України “Про інформацію”

Закон України “Про інформацію” [33] установлює загальні правові засади одержання, використання, поширення й зберігання інформації, закріплює права особи на інформацію у всіх сферах державного та суспільного життя України, а також всю систему інформації та її джерела, визначає статус свіх учасників інформаційних відносин, врегульовує доступ до інформації, забезпечуючи її охорону, захищає громадян та суспільство від неправдивої інформації.

Даний Закон визначає поняття інформації як документованих або публічно оголошених відомостей щодо явищ та подій, що відбуваються в державі, суспільстві та навколишньому середовищі.

Об’єктами інформаційних відносин відповідно є документована або публічно оголошена інформація щодо явищ та подій у галузі політики, економіки, охорони здоров’я, культури, а також в екологічній, соціальній, міжнародній та інших сферах суспільства.

Всі громадяни України, державні органи та юридичні особи мають право на інформацію. Однак реалізація прав на інформацію громадянами, державою та юридичними особами не повинна порушувати політичні, економічні, екологічні, громадські, соціальні, духовні та інші права, законні інтереси і свободи інших громадян, інтереси та права юридичних осіб.

У відповідності із Законом інформаційна діяльність трактується як сукупність дій, що спрямовані на задоволення інформаційних потреб держави, громадян та юридичних осіб.

Важливе місце у Законі займає опис механізму функціонування інформаційних потоків в суспільстві. Так, держава в особі органів влади здійснює контроль над режимом доступу до інформації.

Її завдання при цьому полягає в забезпеченні дотримання вимог діючого законодавства щодо інформації всіма органами державної влади, установами та організаціями, підприємствами, недопущенні необґрунтованого віднесення відомостей в категорію інформації з обмеженим доступом.

Такий державний контроль над дотриманням встановленого режиму здійснюється спеціальними органами, що визначаються Верховною Радою України та Кабінетом Міністрів України. Обмеження прав на отримання відкритої інформації забороняється законодавством.

Закон визначає також порядок доступу до інформації, а саме: дає визначення інформаційного запиту та порядку його розгляду відповідними державними органами, встановлює перелік документів й інформації, які не підлягають наданню для ознайомлення відповідно до запитів, а також визначає порядок відшкодування витрат, які пов'язані з задоволенням запиту.

Інформація виступає об'єктом права власності держави, організацій (юридичних осіб) і громадян. Інформація може бути також об'єктом права власності і в повному обсязі, і об'єктом лише розпорядження, користування чи володіння.

Власник інформації має право також здійснювати будь-які законні дії щодо об'єктів своєї власності. Підставами появи права власності на інформацію являються: створення інформації за свій рахунок і своїми силами; договір, що містить умови передачі права власності на інформацію іншій особі; договір на створення інформації.

Суб'єктами інформаційних відносин згідно з Законом України «Про інформацію» також можуть бути іноземні держави, їхні громадяни, особи без громадянства, юридичні особи та міжнародні організації.

Об'єктами інформаційних відносин виступає задокументована чи публічно оголошена інформація про явища та події у галузі економіки, політики, охорони здоров'я, культури, а також в екологічній, соціальній, міжнародній і інших сферах.

Державні органи, юридичні особи та всі громадяни України мають право на інформацію, яке передбачає можливість вільно одержувати, використовувати, зберігати та поширювати відомості, які є необхідними для них, щоб здійснювати свої завдання, функцій та реалізовувати свої права, свободи й законні інтереси.

Реалізація прав на інформацію з боку держави, юридичних осіб та громадян не повинна порушувати політичні, економічні, соціальні, громадські, екологічні, духовні та інші права, законні інтереси і свободи інших громадян, інтереси і права юридичних осіб. Кожному громадянину гарантується вільний доступ до інформації, що стосується особисто його, крім випадків, які передбачені Законами України [33].

Права на інформацію забезпечуються через:

- формування в державних органах спеціальних інформаційних систем або служб, які будуть забезпечувати доступ до інформації у встановленому порядку;
- обов'язок державних органів (органів державної влади, органів регіонального і місцевого самоврядування) інформувати громадян про прийняті рішення та свою діяльність загалом;
- вільний доступ суб'єктів інформаційних відносин до архівних, музейних і бібліотечних фондів та статистичних даних (обмеження такого доступу зумовлюється тільки специфікою інформації та особливостями умов їх охоронності, які визначаються законодавчо;
- створення механізму реалізації права на інформацію;
- здійснення державного контролю над дотриманням законодавства щодо інформації;

- встановлення відповідальності за порушення діючого законодавства щодо інформації.

2.2. Вимоги Національної програми інформатизації

Інформатизація є сукупністю взаємопов'язаних правових, політичних, організаційних, соціально-економічних, виробничих та науково-технічних процесів, які спрямовані на формування умов задля задоволення інформаційних потреб та реалізації прав суспільства в цілому і громадян зокрема на основі створення, розвитку та використання інформаційних мереж, систем, інформаційних технологій і ресурсів, що створені на основі використання сучасної телекомунікаційної та обчислювальної техніки.

Телекомунікаційна та обчислювальна техніка, телекомунікаційні мережі, банки та бази даних і знань, інформаційні технології, система інформаційно-аналітичних центрів різноманітних рівнів, створення технічних засобів інформатизації, формування системи науково-дослідних установ й підготовка висококваліфікованих фахівців є сьогодні складовими компонентами інформаційної національної інфраструктури та основними чинниками, які забезпечують економічне піднесення.

Інформатизація, як демонструє досвід інших країн, сприяє забезпеченню та реалізації національних інтересів, покращенню керованості національною економікою, розвитку високих технологій та наукоємких виробництв, удосконаленню соціально-економічних відносин, зростанню продуктивності праці, духовному збагаченню життя і подальшій демократизації суспільства.

Інформаційна національна інфраструктура, яка сформована із врахуванням світових досягнень, тенденцій і закономірностей, сприятиме рівноправній інтеграції України в міжнародне співтовариство загалом.

Концепція Національної програми інформатизації [34] включає в себе характеристику сучасного стану інформатизації, основні принципи та стратегічні цілі інформатизації, очікувані наслідки від її реалізації.

В Україні загальна ситуація в галузі інформатизації сьогодні не може бути визначена задовільною і не лише через кризові явища в соціально-економічній системі. Рівень інформатизації українського суспільства складає лише 2-2,5 % порівняно із розвинутими країнами Заходу.

Через технологічне відставання та загальну кризу потрапили в скрутне становище галузі, що займаються створенням й використанням засобів інформатизації і відповідної предметно-елементної бази.

Сьогодні має місце технічне відставання мереж передачі даних та телекомунікаційних систем, що відзначаються надійністю зв'язку та недостатньою пропускнуою здатністю, незначним обсягом послуг та низькою якістю. Переважна більшість установ для передачі даних користується комутованими каналами загального використання.

Національна програма інформатизації формує стратегію розв'язання проблем інформаційної підтримки та забезпечення інформаційних потреб соціально-економічної, науково-технічної, оборонної, екологічної, національно-культурної та інших видів життєдіяльності в сферах загальнодержавного значення.

Складовою частиною національної інформаційної інфраструктури та стратегічних інформаційних ресурсів країни є державні інформаційні ресурси.

Формування Національної програми інформатизації охоплює розробку, узгодження і затвердження завдань (далі - завдань на три роки) Національної програми інформатизації на три наступні роки та завдань (проектів) (далі - завдання (проекти) на один рік) Національної програми інформатизації на поточний бюджетний період, їхніх обсягів фінансування та державних замовників.

Невизначеність фінансово-економічних та правових основ діяльності різноманітних суб'єктів в інформаційній сфері призводить як правило до інформаційної монополізації управлінських та комерційних структур щодо відкритих інформаційних ресурсів загального використання, обмеження прав на користування інформаційними ресурсами держави для більшості громадян, а також знецінення вартості (товарної) інформаційних ресурсів держави.

Здебільшого загальна інформація знаходиться в неформалізованому вигляді та в різних фізичних формах (від друкованих видань до електронних зведень). Все це спричинюється, зокрема, досить повільним освоєнням перспективних інформаційних технологій, які до того ж ускладнені через неповноту та недостатність системи, негармонізованість з міжнародними стандартами в сфері інформатизації, і через що відбувається різке зменшення конкурентоспроможності вітчизняних програмних та технічних продуктів на світових ринках.

В Україні здійснювалася низка певних заходів щодо комплексної, комп'ютеризації, електронізації та автоматизації у невиробничих та виробничих сферах: розвивалися мережі підприємств електронної промисловості і приладобудування (вони є практично у всіх великих промислових центрах країни), значна кількість організацій та підприємств займаються розробленням програмних послуг і продуктів, функціонують спеціалізовані проектно-конструкторські бюро і науково-дослідні інститути.

Діє в Україні і система сервісних підприємств, що є складовою інформаційної національної інфраструктури, але можливості її обмежені. Україна володіє значним науково-технічним потенціалом та фундаментальними досягненнями в галузі інформатики. Відомі в світі здобутки українських вчених у галузі створення нетрадиційних архітектур обчислювальних машин та в моделюванні, системному аналізі, створенні

штучного інтелекту, оптимізації процесів. Україна досягла певного рівня централізації та концентрації наукоємних виробництв.

Більш ніж 70 % стратегічних матеріалів для роботи електронної промисловості в Європі вироблено було саме на українських підприємствах, що дає позитивні можливості в справі інформатизації країни.

Проекти національної інформатизації розроблялися у багатьох територіальних ланках і галузях за прикладними та фундаментальними програмами.

Усі ці програми діяли розрізнено, в умовах обмеженості фінансових ресурсів, без дотримання єдиної державної координації та науково-технічної політики, належним чином незалучених до функціональних завдань необхідних органів управління, зокрема регіональних, що призвело до вагомих моральних, соціально-економічних та інших збитків.

Тому немаловажливою умовою подолання відставання України у галузі інформатизації повинні бути державна політика інформатизації країни, Національна програма інформатизації (Програма) і відповідний ефективний механізм її реалізації.

Щодо державної політики інформатизації країни, то вона формується як складова компонента соціально-економічної політики держави в загальному і спрямовується на раціональне й ефективне використання науково-технічного і промислового потенціалів, фінансових і матеріально-технічних ресурсів для формування сучасної інформаційної національної інфраструктури в інтересах та з метою вирішення комплексу перспективних та поточних завдань розвитку України у напрямку демократичної незалежної держави з ринковою економічною системою.

Для пришвидчення процесу інформатизації в країні, що потребує концентрації відповідних ресурсів, за основу державної політики повинно братися покладене на державу регулювання інформатизаційних процесів на основі поєднання принципів децентралізації і централізації, саморозвитку,

самоокупності ті самофінансування, державної підтримки через систему прямого бюджетного фінансування, кредитів, пільг.

Бюджетні кошти насамперед повинні бути спрямовані на формування та реалізацію проектів інформатизації загальнодержавного значення: створення національної телекомунікаційно- інформаційної системи; розвиток системи інформаційних національних ресурсів; інформатизація стратегічних напрямів щодо розвитку економіки, соціальної сфери, безпеки та оборони, держави.

Державне регулювання покликане забезпечити комплексність, системність та узгодженість напрямку розвитку інформатизації країни із використанням при цьому нетрадиційних та традиційних форм і методів контролю та супроводження.

Важливе значення для розвитку національної інформатизації має здійснення виваженої політики в сфері реформування власності в Україні.

Держава повинна сконцентрувати потрібну кількість державних систем і об'єктів інфраструктури інформатизації для того, аби мати необхідні важелі формування та реалізації державної політики.

Для підтримки конкурентного середовища необхідно здійснювати політику підтримки середніх та малих підприємств в сфері інформатизації.

В період становлення України в якості самостійної незалежної держави в кризових умовах економіки та обмеженості всіх видів ресурсів здійснення процесу національної інформатизації можливе тільки шляхом визначення пріоритетних напрямів і сфер із концентрацією на них трудових, фінансових й матеріальних ресурсів.

Пріоритети не повинні бути постійними, а визначатися на певний конкретний період та коригуватися залежно від ситуації, яка складається.

Входження України в інформаційне середовище світу на паритетній правовій основі на першому (початковому) етапі можливе шляхом придбання

в провідних виробників світу інформаційних послуг та продуктів державою ліцензій з подальшим їх упровадженням у вітчизняне виробництво.

Інвестиційна політика держави в сфері інформатизації повинна полягати у такому: цільові бюджетні інвестиції отримують лише ті національні виробники, що можуть забезпечити зростання обсягу виробництва за рахунок кінцевих послуги або продукту, чистого експорту або створення продукції, яка замінює імпорту.

Важливим принципом державної політики також повинно стати впровадження необхідних антимонопольних заходів як під час реалізації Національної програми інформатизації, так і на стадії її коригування.

Державна політика інформатизації також повинна бути спрямована на всебічну демократизацію процесів виробництва і споживання інформації, захист прав громадян від інформаційного вторгнення, загальнодоступність інформаційних послуг і ресурсів тощо.

За основу оцінки ефективності інформатизації потрібно взяти комплексний підхід, що ґрунтується на урахуванні не лише ресурсних показників, але й впливу інформаційних процесів на усі сфери життєдіяльності суспільства у цілому, в тому числі на збільшення обсягів виробництва валового внутрішнього продукту в країні.

Державне регулювання в сфері інформатизації також повинно базуватися на програмно-цільових методах та системному підході, які реалізуються шляхом формування, виконання та моніторингу Програми.

Національна програма інформатизації є комплексом взаємопов'язаних окремих завдань (або проектів) інформатизації, що спрямовані на реалізацію державної політики і пріоритетні напрями формування сучасної інформаційної національної інфраструктури за рахунок концентрації і раціонального використання матеріальних, технічних, фінансових та інших ресурсів, науково-технічного та виробничого потенціалу держави, а й також координації діяльності державних органів (органів державної влади й органів

регіонального та місцевого самоврядування), установ, організацій, підприємств усіх форм власності та громадян в сфері інформатизації країни.

Головна мета Національної програми інформатизації - це забезпечення суспільства і громадян своєчасною, повною та достовірною інформацією за допомогою широкого використання інформаційних технологій, забезпечуючи при цьому інформаційну безпеку держави.

Національна програма інформатизації як правило формується, враховуючи довгострокові пріоритети економічного, соціального, національно-культурного, науково-технічного розвитку країни; світові досягнення науки; тенденції та закономірності в сфері інформатизації та направлена на розв'язання загальносуспільних найважливіших проблем, а саме: здоров'я людей та охорона довкілля, розвиток системи науки і освіти, економічне реформування, демократизація суспільства, створення умов для інтеграції України в міжнародний інформаційний простір у відповідності до сучасних тенденцій інформаційної геополітики, забезпечення державної безпеки та обороноздатності країни.

Реалізація Національної програми інформатизації повинна здійснюватися із дотриманням основних принципів, а саме:

1. узгодженість основних пріоритетів інформатизації країни із основними напрямами Програми діяльності Уряду України, Державної програми соціального та економічного розвитку України, державних цільових програм;
2. розроблення, реалізація і координація державних, відомчих, міжгалузевих програм інформатизації щодо етапів, ресурсів, цілей та об'єктів робіт;
3. випереджувальний розвиток нормативно-правової основи регулювання відносин учасників (суб'єктів) створення, використання, й розповсюдження інформаційних послуг та продуктів, а також єдиної національної системи зв'язку в країні;

4. підтримка вітчизняного виробника;
5. системність формування та виконання Національної програми інформатизації [34].

Основними напрямками інформатизації є:

1. Розроблення політики та організаційно-правове забезпечення інформатизації. Організаційно-правове забезпечення процесу інформатизації передбачає розроблення пакета нормативно-правових актів з питань організації та правового регулювання відносин у сфері інформатизації, зокрема:
 - захисту авторського права і прав та свобод громадян у питаннях інтенсивної інформаційної взаємодії держави та громадянина відповідно до Конституції України;
 - економічного стимулювання створення національного інформаційного ресурсу;
 - доступу фізичних та юридичних осіб до міжнародних інформаційних ресурсів;
 - розроблення системи державних стандартів у галузі інформатизації;
 - сертифікації технічного і програмного забезпечення; локалізації програмного забезпечення;
 - розроблення нормативних актів про діяльність та взаємодію державних та комерційних структур щодо виконання Національної програми інформатизації, залучення різних джерел фінансування, митне регулювання та інше.
2. Формування національної інфраструктури інформатизації. Національна інфраструктура інформатизації включає:
 - міжнародні та міжміські телекомунікаційні і 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;
- системи підготовки висококваліфікованих фахівців у сфері інформатизації [34].

Сучасною основою розвитку телекомунікаційних мереж є будівництво магістральних волоконно-оптичних каналів зв'язку, завершення формування мережі міжнародного та міжміського телефонного зв'язку з переходом на цифрові системи як найбільш ефективні та прибуткові, розроблення системи лазерного зв'язку, національної системи комп'ютерного телемовлення, наземних і космічних каналів зв'язку, створення інформаційно-телекомунікаційної мережі для освіти та науки тощо.

Виконання проектів зазначеного розділу Національної програми інформатизації сприятиме підвищенню рівня самозабезпечення засобами інформатизації і перетворенню України в рівноправного партнера у міжнародному поділі праці з виробництва та використання засобів інформатизації.

Індустрія програмних засобів повинна стати базою для створення нових сучасних інформаційних технологій та систем, автоматизованих систем керування різноманітного призначення.

Передбачається створення інструментально-технологічних комплексів підтримки розроблення високоякісного і конкурентоспроможного програмного забезпечення, відповідної державної системи оцінки якості, сертифікації програмної продукції. Виробництво програмних продуктів повинно стати самоокупною галуззю економіки, здатною експортувати свою продукцію.

Науково-дослідні установи повинні створити та впровадити інтегровані інформаційні технології побудови розподілених баз знань та експертних систем, заснованих на автоматичному формуванні знань для вирішення завдань, що важко формалізуються, з різних предметних галузей, розробити

базові засоби інтелектуалізації інформаційних технологій, системи електронного документообігу, засоби мовно-зорового діалогу, системи розуміння текстів тощо. Інформатизація стратегічних напрямів розвитку державності, безпеки та оборони. Досягається шляхом створення і розвитку інформаційно-аналітичних, обчислювальних та автоматизованих систем, центрів і мереж, які забезпечують роботу органів державної влади та органів місцевого самоврядування.

Особливістю завдань цього напрямку є їх складність, пов'язана з необхідністю оброблення великого обсягу різноманітної інформації, що надходить із значної кількості джерел, а також з високими вимогами до швидкості і форми її надання, достовірності, актуальності, безпеки інформації.

Програмою передбачається створити комплекс інформаційних технологій та засобів інформатизації для збору, зберігання, аналізу і обробки великих обсягів інформації про стан соціально-економічних процесів в Україні з метою забезпечення інформаційно-аналітичної підтримки прийняття рішень органами державної влади, інформаційно-аналітичну систему Верховної Ради України, інструментально-технологічний комплекс підтримки прийняття рішень у штатних і нештатних ситуаціях в умовах інформаційної протидії, Урядову інформаційно-аналітичну систему з питань надзвичайних ситуацій тощо.

Планується розробити типову структуру інформаційно-аналітичних центрів органів державної влади і місцевого самоврядування. Формування інформаційно-аналітичної та програмно-технічної бази дасть можливість органам державної влади і місцевого самоврядування повно і оперативно аналізувати та оцінювати ситуацію в усіх сферах і галузях діяльності суспільства.

З цією метою необхідно здійснити інтеграцію існуючих інформаційних систем органів державної влади і органів місцевого самоврядування та

інформаційних ресурсів, тобто створити єдину інформаційно-телекомунікаційну систему збору, обробки та передачі даних, необхідних для прийняття стратегічно важливих рішень у сфері економіки, внутрішньої та зовнішньої політики.

2.3. Особливості Доктрини інформаційної безпеки України

Загальні положення технології гібридної війни проти України зробили інформаційну сферу ключовою ареною протиборства.

Проти України сьогодні застосовуються найпрогресивніші інформаційно-психологічні методи й засоби впливу на свідомість людей, що спрямовані на пропаганду агресивної війни, розпалювання релігійної і національної ворожнечі, зміну конституційного ладу насильницькими шляхами, порушення суверенітету, незалежності й територіальної цілісності України.

Комплексність характеру актуальних загроз національній безпеці України у інформаційній сфері потребує використання інноваційних підходів до формування систем розвитку та захисту інформаційного простору держави в умовах вільного обігу інформації та глобалізації.

Пріоритети, напрями та принципи забезпечення кібербезпеки України визначаються у Стратегії кібербезпеки України (затверджена Указом Президента України № 96 від 15 березня 2016 р. (Рішення Ради національної безпеки й оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»).

Національні інтереси України у інформаційній сфері, загрози їхньої реалізації, пріоритети і напрями державної політики у інформаційній сфері визначає Доктрина інформаційної безпеки України [10].

Правову основу Доктрини складають Закони України, Конституція України, Укази Президента України (наприклад, Стратегія національної безпеки України).

Метою Доктрини виступає уточнення основних засад формування та реалізації інформаційної політики держави, насамперед, стосовно протистояння руйнівному інформаційно-психологічному впливу агресора в умовах розв'язаної ним гібридної війни [10].

Принципами, на яких базується Доктрина, є дотримання свобод й прав людей та громадян, захисту їхніх законних інтересів, поваги до гідності людини, а також законних інтересів держави та суспільства, забезпечення територіальної цілісності і суверенітету України.

У інформаційній сфері національними інтересами України є:

1. Життєво важливі інтереси держави та суспільства, зокрема захист українських громадян від агресивного руйнівного впливу деструктивної пропаганди, перш за все з боку агресора.
2. Життєво важливі інтереси людини, зокрема забезпечення конституційних свобод й прав людей на збирання, зберігання, поширення й використання інформації, а також захист від деструктивного інформаційно-психологічного впливу та забезпечення конституційних прав людей на захист свого приватного життя.
3. Захист українського суспільства від руйнівних агресивних інформаційних впливів агресора, що спрямовані на пропаганду війни, зміну конституційного ладу насильницькими шляхами, розпалювання релігійної й національної ворожнечі, порушення територіальної цілісності та суверенітету України.
4. Всестороннє задоволення потреб громадян, установ, організацій і підприємств всіх форм власності щодо доступу до об'єктивної та достовірної інформації.

5. Захист та розвиток інформаційної національної інфраструктури, примноження й збереження духовних, моральних і культурних цінностей народу України.
6. Забезпечення вільного обігу та обміну інформацією, крім випадків, які передбачені законодавчо;
7. Забезпечення всестороннього функціонування і розвитку української мови на всій території України й у всіх сферах суспільного життя.
8. Вільне використання, захист й розвиток мов національних меншин, зміцнення й розвиток інформаційних зв'язків із українською діаспорою, допомога у збереженні її етнокультурної ідентичності, а також сприяння вивченню іноземних мов (мов міжнародного спілкування).
9. Розвиток соціально відповідальної медіа-культури та медіа-середовища суспільства, формування ефективної юридичної системи захисту держави, суспільства й особи від деструктивних руйнівних інформаційно-пропагандистських впливів.
10. Формування системи та конкретних механізмів захисту від зовнішньою негативного інформаційно-психологічного впливу, насамперед пропаганди (з урахуванням норм міжнародного права); розвиток інформаційного суспільства в Україні, зокрема і його технологічної інфраструктури.
11. Безпечні розвиток і функціонування інформаційного простору України та його інтеграція у світову й європейську інформаційну систему.
12. Розвиток систем стратегічних комунікацій України.
13. Раціональна та ефективна взаємодія державних органів влади й інститутів громадянського суспільства у процесі формування й реалізації державної політики у інформаційній сфері.
14. Сприяння розвитку інформаційних ресурсів України й інформаційно-комунікаційних технологій.

15. Захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом.
16. Формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти.
17. Розбудова системи іномовлення України та забезпечення наявності іномовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України [10].

Актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

- Здійснення спеціальних інформаційних операцій, спрямованих на підриє обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні.
- Проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі.
- Інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах.
- Інформаційне домінування держави-агресора на тимчасово окупованих територіях.
- Недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України.

- Неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства.
- Поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [10].

Висновки до другого розділу

Розглянуто Закон України “Про інформацію”. Він являється базовим в інформаційній сфері. Також в розділі наведено основні поняття і визначення, що стосуються інформації та інформаційної безпеки в цілому, а саме інформація, захист інформації, поширення інформації і т.д. Закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації.

Описано основні аспекти Національної програми інформатизації, а саме її мета, головні положення, необхідні умови функціонування та завдання. Дана програма дозволяє Україні долати відставання в галузі інформатизації.

Наведено опис Доктрини інформаційної безпеки України, що базується на принципах додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України.

Розділ 3

НАПРЯМИ ВДОСКОНАЛЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НОРМАТИВНО- ПРАВОВОЇ БАЗИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

3.1. Механізми протидії загрозам у сфері інформаційної безпеки України

Інформаційна сфера є системоутворюючим фактором життя суспільства і робить значний вплив на стан політичної, економічної, оборонної та інших складових безпеки України. У зв'язку з цим інформаційна безпека в державі поширюється на різні сфери життєдіяльності суспільства і держави: сферу економіки, сферу внутрішньої і зовнішньої політики, сферу оборони, правоохоронну і судову сфери, область науки і техніки, сферу духовного життя та інші.

Кожну з цих сфер можна охарактеризувати особливостями забезпечення інформаційної безпеки, пов'язаними зі специфікою об'єктів забезпечення безпеки, ступенем їх вразливості щодо загроз інформаційної безпеки в Україні.

В даний час інформація та інформаційні технології мають пряме і безпосереднє відношення до політичної сфери. Процеси збору, накопичення, переробки та розповсюдження інформації стають одним з необхідних умов для існування структур політичного управління, здійснення ефективних політичних впливів.

Світовий досвід показав, що в якості джерела політичної загрози може виступати інформація. Тому існує необхідність державно-правового регулювання інформаційних потоків. Засоби масової інформації і глобальна мережа Інтернет придбали величезне значення в політичній сфері.

Пріоритетами державної політики в інформаційній сфері мають бути:

1. Щодо забезпечення інформаційної безпеки:
 - Створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;
 - Удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері;
 - Законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку;
 - Визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ та населення;
 - Заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передачі інформації через комп'ютерні мережі в умовах запровадження правового режиму воєнного стану;

- Створення й розвиток структур, які відповідають за інформаційну (інформаційно-психологічну) безпеку, передусім в Збройних Силах України (із врахуванням практики країн-членів НАТО);
- Оптимізація чинних законодавчих механізмів виконання зобов'язань України у рамках Європейської конвенції щодо транскордонного телебачення по відношенню країн, які не підписали зазначену Конвенцію;
- Захист й розвиток технологічної інфраструктури, що забезпечує інформаційну безпеку в Україні;
- Забезпечення повного покриття всієї території України цифровим телебаченням, передусім тимчасово окупованих територій, а також у прикордонних районах;
- Розвиток цифрового мовлення й унеможливлення впливу на інфраструктуру цього мовлення суб'єктів, які пов'язані із державою-агресором;
- Формування ефективних та дієвих систем стратегічних комунікацій;
- Побудова механізмів взаємодії інститутів громадянського суспільства з державою стосовно протистояння інформаційній агресії в Україні;
- Боротьба з деструктивною пропагандою й руйнівною дезінформацією з боку агресора;
- Посилення можливостей сектору оборони й безпеки стосовно протистояння спеціальним інформаційним операціям, що спрямовані на зміну конституційного ладу насильницьким шляхом, порушення територіальної цілісності й суверенітету, підрив та зниження стану обороноздатності України, деморалізацію особового складу військових формувань (передусім, Збройних Сил України), загострення суспільно-політичного стану в країні;
- Виявлення й притягнення до юридичної відповідальності у відповідності із діючим законодавством суб'єктів інформаційного

- національного простору, які створені та/або використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;
- Унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни, національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення;
 - Проведення розвідувальними органами України акцій сприяння реалізації та захисту національних інтересів України в інформаційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави за межами України;
 - Недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;
2. Щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію: стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів;
- Забезпечення функціонування Суспільного телебачення і радіомовлення України, у тому числі його належного фінансування;
 - Створення системи мовлення територіальних громад, яка сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад;
 - Підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек;

- Розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;
 - Комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності;
 - Підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності;
 - Удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці;
 - Задоволення потреб населення тимчасово окупованих територій в об'єктивній, оперативній і достовірній інформації;
 - Повне покриття території України цифровим та інтернет-мовленням замість аналогового і надання рівних можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет;
 - Формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту;
 - Пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз;
3. Щодо відкритості та прозорості держави перед громадянами: розвиток механізмів електронного урядування;
- Сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних; інформування громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами;
 - Проведення реформи урядових комунікацій;

- Розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень органами державної влади та органами місцевого самоврядування;
- Сприяння формуванню культури суспільної дискусії;
- 4. Щодо формування позитивного міжнародного іміджу України:
 - грунтовне реформування системи представлення інформації про Україну на міжнародній арені;
 - Розвиток публічної дипломатії, у тому числі культурної та цифрової; активізація скоординованої інформаційної роботи закордонних дипломатичних установ України;
 - Сприяння поширенню та розвитку системи іномовлення України;
 - Створення та забезпечення функціонування правового механізму взаємодії державних органів з інститутами громадянського суспільства з метою інформаційної підтримки комерційної, гуманітарної, просвітницької, культурної та іншої діяльності таких інститутів за межами України;
 - Постійний моніторинг пропаганди держави-агресора, розроблення та оперативна реалізація адекватних заходів протидії;
 - Недопущення використання міжнародного інформаційного простору в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;
 - Реформування системи взаємовідносин з українською діаспорою шляхом забезпечення більш тісної співпраці та проведення ефективних заходів, зокрема в рамках комунікацій «від людини до людини»;
 - Участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності;
 - Запровадження міжнародних культурних фестивалів в Україні з метою популяризації української культури та розвитку комунікацій «від людини до людини».

Механізм реалізації Доктрини Рада національної безпеки і оборони України відповідно до Конституції України та у встановленому законом порядку має здійснювати координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері.

Кабінет Міністрів України забезпечуватиме здійснення інформаційної політики держави, фінансування програм, пов'язаних з інформаційною безпекою, спрямовуватиме і координуватиме роботу міністерств, інших органів виконавчої влади у цій сфері.

Зважаючи на особливі умови і ведення проти України агресивної інформаційної війни не лише на її території, але й у світі, забезпечення реалізації Доктрини можливе лише за умови належної координації заходів, здійснюваних усіма державними органами.

Ключові заходи відповідно до положень Доктрини визначатиме Рада національної безпеки і оборони України.

Суб'єкти реалізації державної інформаційної політики у взаємодії з інститутами громадянського суспільства в межах компетенції забезпечують реалізацію Доктрини, а також за необхідності вносять обґрунтовані пропозиції щодо корегування її положень.

3.2. Забезпечення інформаційного суверенітету України

Інформаційний суверенітет України - це право держави на формування і здійснення національної інформаційної політики відповідно до Конституції і законодавства України, міжнародного права в національному інформаційному просторі України.

Здійснення інформаційного суверенітету України включає: законодавче визначення та забезпечення державою стратегічних напрямів розвитку і захисту національного інформаційного простору, цілісної державної інформаційної політики; визначення норм, засад і меж діяльності зарубіжних

й міжнародних суб'єктів у інформаційному національному просторі України; захист й формування інтересів України у інформаційному світовому просторі та інформаційних міжнародних відносинах; гарантування інформаційної безпеки країни.

Основними потенційними й реальними загрозами національній безпеці країни (у зовнішньополітичній сфері) загалом та стабільності у суспільстві зокрема на сучасному етапі є:

- спроби втручання в внутрішні справи України зі сторони інших держав;
- посягання на територіальну цілісність України й її державний суверенітет України, територіальні претензії зі сторони інших держав.

Посилення й удосконалення законодавчої бази у інформаційно-комунікаційній сфері у першу чергу повинно бути спрямовано на забезпечення захисту інформаційного суверенітету усіх сучасних країн. Дослідник Є. Кирильчук з цього приводу зауважує, що у науковій літературі, коли мова йдеться про захист інформаційного національного простору як такого, то передусім мають на увазі інформаційний державний суверенітет, а саме належне розповсюдження й володіння усією спільнотою в країні відповідними інформаційними національними ресурсами [25].

Варто стверджувати, що на даному сучасному етапі українського державотворення захист інформаційного суверенітету країни, її ефективна стратегія стосовно майбутніх й існуючих інформаційних війн у світі є одним з найголовніших та найважливіших завдань в сфері національної безпеки країни.

Для проведення системних й ефективних безпекових заходів в інформаційній сфері України необхідно постійно удосконалювати нормативно-правову базу з метою збереження балансу між інформаційними правами людей й інтересами держави в сфері інформаційної безпеки.

Реалізація інформаційного суверенітету розглядається у чотирьох напрямках:

- 1) законодавче визначення та забезпечення державою стратегічних напрямів розвитку та захисту національного інформаційного простору, цілісної державної інформаційної .
- 2) визначення норм, засад і меж діяльності зарубіжних та міжнародних суб'єктів в інформаційному просторі України;
- 3) формування та захист інтересів України в світовому інформаційному просторі, міжнародних інформаційних відносинах;
- 4) гарантування інформаційної безпеки України.

Найактуальнішою для теперішньої інформаційної ситуації в Україні є:

- сприяти створенню єдиної державної інформаційної політики, без чого неможливе ефективне обстоювання національних інтересів держави;
- повернути український телерадіоефір у площину українських національних інтересів;
- створити систему ефективної інформаційної безпеки України.

Висновки до третього розділу

Досліджено механізми протидії загрозам у сфері інформаційної безпеки держави. Було визначено головні пріоритети державної політики в сфері інформатизації. Одним з головних органів в сфері ІБ є Міністерство інформаційної політики України. Також було описано вплив інформаційних загроз на економічну безпеку завдяки рівневому підходу.

Визначено поняття інформаційного суверенітету України та способу його здійснення. Описано основні загрози національній безпеці в зовнішньополітичній сфері.

ВИСНОВКИ

Створення нормативно-правової бази держави є одним з основних кроків у формуванні захищеності інформаційного простору України та відіграє важливу роль в процесі забезпечення інформаційної безпеки держави.

Проаналізовано специфіку та основні характеристики ключових нормативних документів України, а саме Доктрина інформаційної безпеки України, Закон України “Про інформацію”, Закон України “Про національну програму інформатизації”.

Проведено аналіз існуючих загроз та засобів протидії їм, що описані в законодавчій базі держави.

Досліджено напрями вдосконалення політики інформаційної безпеки та перспективи розвитку нормативно-правової бази забезпечення інформаційної безпеки в Україні.

На основі аналізу документів, які використовуються при забезпеченні інформаційної безпеки держави, в роботі описано ряд рекомендацій для побудови більш надійного захисту інформаційного простору держави. Дані рекомендації можуть бути використані державними органами влади України в сфері інформатизації при формуванні покращеної нормативно-правової бази.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурич К. Л. Інформаційна безпека України у сучасному кіберпросторі / К. Л. Бурич, І. Н. Єфименко, Б. Д. Коган // Національна безпека і оборона. – 2014. – № 10. – С. 21-27.
2. Галамба М. Інформаційна безпека України: поняття, сутність та загрози / М. Галамба, В. Петрик [Електронний ресурс] – Режим доступу: <http://www.justinian.com.ua>
3. Гиркіна О. О. Сучасні аспекти забезпечення інформаційної безпеки України / О. О. Гиркіна, В. М. Семенов // Юридичні науки. – 2014. – С. 234-239.
4. Гнатцов О. Г. Інформаційні ресурси в системі забезпечення державної безпеки / О. Г. Гнатцов [Електронний ресурс] – Режим доступу: <http://www.niisp.gov.ua/vydanna/panorama>
5. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О. М. Горбатюк // Вісн. Київ. ун-ту ім. Т. Шевченка. Сер.: Міжнар. відносини. – 2009. – Вип. 14. – С. 46-48.
6. Горбулін В. П. Актуальні проблеми системного забезпечення інформаційної безпеки України / В. П. Горбулін, М. М. Биченок, П. М. Копка // Матеріали міжар. наук.-практ. конф. «Форми та методи забезпечення інформаційної безпеки держави». – К.: Нац. акад. СБУ. – 2018. – С. 79-85.
7. Гуровський В. О. Роль органів державної влади у сфері забезпечення інформаційної безпеки України / В. О. Гуровський // Вісник Національної академії державного управління при Президентові України. – К., 2014. – № 3. – С. 21-31.
8. Гуцалюк М. Інформаційна безпека в сучасному суспільстві / М. Гуцалюк // Право України. – 2015. – № 7. – С. 71-74.

9. Гуцалюк М. Інформаційна безпека України: нові загрози / М. Гуцалюк // Бизнес и безопасность. – 2013. – № 5. – С. 2-3.
10. Доктрина інформаційної безпеки України: Указ Президента України № 47/2017 від 29.12.2016 [Електронний ресурс]. – Режим доступу: <http://zakon.rada.gov.ua>
11. Долженко К. І. Нормативно-правове регулювання інформаційної безпеки регіону / К. І. Долженко // Право і Безпека. – 2014. – № 3. – С. 43-48.
12. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки / Д. Дубов // Політичний менеджмент. – 2010. – № 5. – С. 33-37.
13. Кельман М. О. Загальна теорія держави і права: підруч. / М. О. Кельман, О. Г. Мурашин. – К.: Кондор, 2016. – 477 с.
14. Колобков Д. С. Державна інформаційна політика / Д. С. Колобков [Електронний ресурс]. – Режим доступу: <http://merega.org.ua/law/projects/derzhpolityka>
15. Колпаков В. К. Адміністративне право України: підруч. / В. К. Колпаков. – К.: Юрінком Інтер, 2009. – 736 с.
16. Конституція України від 28.06.1996 р. // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – Ст. 141.
17. Концепція інформаційної безпеки держав-учасників Співдружності Незалежних Держав у військовій сфері [Електронний ресурс] – Режим доступу: <http://www.ngo.dn.ua>
18. Коньков А. І. Стан і проблеми забезпечення інформаційної безпеки / А. І. Коньков [Електронний ресурс]. – Режим доступу: <http://old.niss.gov.ua/book/otch/roz13.htm>
19. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посіб. / Б. А. Кормич. – К.: Кондор, 2014. – 384 с.
20. Косач П. Д. Інформаційна безпека як основа національної безпеки / П. Д. Косач. – К.: ЗАТ Видавничий дім «ДЕМІЩ», 2012. – 144 с.

- 21.Крюков О. І. Інформаційна безпека держави в умовах глобалізації [Електронний ресурс] / О. І. Крюков // Державне будівництво. – 2017. – № 2. – Режим доступу: <http://www.nbu.gov.ua/e-journals/DeBu/2007-2/doc/1/10.pdf>
- 22.Литвиненко О. Інформація і безпека / О. Литвиненко // Нова політика. – 2018. – № 1. – С. 47-49.
- 23.Лужецький В. А. Інформаційна безпека: навч. посіб. / В. А. Лужецький, О. П. Войнович, А. В. Дудатьєв. – Вінниця: УНІВЕРСУМ-Вінниця, 2019. – 240 с.
- 24.Макаренко Е. Інформаційно-психологічний захист як складовий чинник інформаційної безпеки / Е. Макаренко, В. Кирик // Проблеми безпеки української нації на порозі ХХІ ст. – К.: Верес, 2008.
- 25.Морозов О. Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності / О. Л. Морозов [Електронний ресурс]. – Режим доступу: <http://www.viche.info>
- 26.Наливайко Л. Р. Концептуальні основи інформаційної безпеки України / Л. Р. Наливайко // Вісник Запорізького державного університету. – 2013. – № 1. – С. 24-26.
- 27.Національний інститут стратегічних досліджень: офіційний сайт [Електронний ресурс]. – Режим доступу: <http://www.niss.gov.ua/>
- 28.Нашинець-Наумова А. Ю. Правове регулювання інформаційної безпеки корпорацій / А. Ю. Нашинець-Наумова // Правова інформатика. – 2014. – № 4 (44). – С. 95-99.
- 29.Непов А. О. Інформаційна потужність держави як складова національної безпеки / А. О. Непов [Електронний ресурс] – Режим доступу: <http://propolis.com.ua>
- 30.Остроухов В. В. Інформаційна безпека (соціально-правові аспекти): [Підручник] / Остроухов В. В. Петрик В. М., Присяжнюк М. М., за заг. ред. Скулиша Є. Д. – К.: КНТ, 2010. – 776 с.

- 31.Петров С. Інформаційна безпека суспільства і держави. Стратегічні цілі і задачі інформаційної боротьби / С. Петров [Електронний ресурс] – Режим доступу: <http://www.ngo.dn.ua/doc/concept.doc>
- 32.Почепцов Г. Г. Інформаційна політика: навч. посібник / Г. Г. Почепцов – К.: Знання, 2016.
- 33.Про інформацію: Закон України № 2657-XII від 02.10.1992 [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/2657-12>
- 34.Про Концепцію Національної програми інформатизації: Закон України від 4.02.1998 р. № 75/98-ВР // Відомості Верховної Ради. – 1998. – № 27-28. – С. 182.
- 35.Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр.: Закон України від 09.01.2007 [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/537-16>
- 36.Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII [Електронний ресурс]. – Режим доступу: <http://zakon.rada.gov.ua>
- 37.Про службу безпеки України: Закон України від 25.03.1992 [Електронний ресурс]. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/2229-12>
- 38.Систематизація інформаційного законодавства України: монографія / В. А. Ліпкан, В. А. Залізняк / За заг. ред. В. А. Ліпкана. – К.: ФОП О. С. Ліпкан, 2018. – 304 с.
- 39.Сорокін О. Інформаційна безпека та її складові: проблеми визначення концепту / О. Сорокін // Держава та право. – 2014. – №8. – С. 18-22.
- 40.Соснін О. Державне управління інформатизацією як виклик цивілізаційного зростання нації / О. Соснін // Зовнішні справи. – 2017. – № 3. – С. 17-21.

- 41.Степко О. М. Аналіз головних складових інформаційної безпеки держави / О. М. Степко // Наук. вісн. Ін-ту міжнар. відносин НАУ. – Сер.: Економіка, право, політологія, туризм. – К., 2011. – Вип. 1 (3). – С. 90-99.
- 42.Стрельцов А. А. Обеспечение информационной безопасности. Теоретические и методологические основы / А. А. Стрельцов; под ред.: В. А. Садовниченко и В. П. Шерстюка. – М.: МЦНМО, 2012. – 153 с.
- 43.Суббот А. Інформаційна безпека суспільства / А. Суббот // Віче. – 2015. – № 8. – С. 29-31.
- 44.Тополевський Р. Коментарі до проекту Закону України «Про інформаційну безпеку України» (№ 5732 від 22 вересня 2014 р.) / Р. Тополевський, Є. Захаров [Електронний ресурс]. – Режим доступу: <http://khpg.org.ua>
- 45.Уфимцев Ю. С. Методика информационной безопасности / Ю. С. Уфимцев, В. П. Буянов и др. – М.: Экзамен, 2014. – 544 с.
- 46.Шубіна О. В. Державна інформаційна безпека: проблеми визначення концепту / О. В. Шубіна // Держава та права. – 2014. – № 3. – С. 26-31.
- 47.Ярочкин В. И. Информационная безопасность: Учебник для студентов вузов / В. И. Ярочкин. – М.: Фонд «Мир», 2013. – 640 с.
- 48.Charter of the United [Електронний ресурс]. – Режим доступу: <http://www.un.org/en/documents/charter/>
- 49.Resolution adopted by the General Assembly UN [on the report of the First Committee (A/53/576)] «Development in the field of information and telecommunication in the context of information security». – Distr. General A/RES/53/70, 4 January, 1999, N.Y.