Київський національний торговельно-економічний університет

Кафедра публічного управління і адміністрування

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Державна політика у сфері інформаційної безпеки

Студента 4 курсу, 12 групи,
спеціальність 074 «Публічне управління та адміністрування» спеціалізації «Публічне управління та адміністрування»

_____ Писаревський Артем Петрович
(підпис студента)

Науковий керівник
Кандидат економічних наук, доцент

_____ Сонько Юлія Анатоліївна
(підпис керівника)

Гарант освітньої програми
кандидат економічних наук, доцент

_____ Головня Юлія Ігорівна
(підпис гаранта)

Київ 2020

Київський національний торговельно-економічний університет

Факультет економіки, менеджменту та психології
Кафедра публічного управління та адміністрування
Освітній ступінь: бакалавр
Спеціальність: публічне управління та адміністрування
Спеціалізація: публічне управління та адміністрування

Затверджую
Зав. кафедри
_____

« 17» червня
2020р.

Завдання
на випускну кваліфікаційну роботу (проект)
студентові
Писаревському Артему Петровичу
(прізвище, ім'я, по батькові)

1.Тема випускної кваліфікаційної роботи (проекту): «**ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»**

Затверджена наказом ректора від «27» лютого 2020 р. № 757

1. Строк здачі студентом закінченого роботи (проекту): 15.05.2020

2. Цільова установка та вихідні дані до роботи (проекту)

Мета роботи (проекту): Теоретичне обґрунтування і опрацювання та встановлення рекомендацій на фоні досліджень, методів, загроз в інформаційній безпеці України, щодо покращення державної політики у цій сфері.

Зазначена мета вимагає вирішити наступні **завдання**:

- Проаналізувати теоретичні засади дослідження інформаційної безпеки в Україні;
- Проаналізувати органи державної влади в системі забезпечення інформаційної безпеки;

– Дослідити ключові загрози інформаційній безпеці в сучасних умовах;
– Проаналізувати напрями ефективної співпраці держав в контексті забезпечення безпеки глобального інформаційного простору
– Дослідити заходи щодо посилення інформаційної безпеки в Україні

Об'єкт дослідження виступає процес реалізації державної політики у сфері інформаційної безпеки.

Предмет дослідження: є теоретико-методичні та прикладні засади державного управління у сфері інформаційної політики.

4. Зміст випускної кваліфікаційної роботи (проекту) (перелік питань за кожним розділом):

5. Календарний план виконання роботи (проекту)

№ пор.	Назва етапів випускної кваліфікаційної роботи (проекту)	Строк виконання етапів роботи	
		за планом	фактично
1	2	3	4
1	Визначення напряму дослідження та затвердження теми випускної кваліфікаційної роботи	До 27.02.2020	27.02.2020
2	Складання плану та підготовка індивідуального завдання для виконання випускної кваліфікаційної роботи	До 10.03.2020	10.03.2020
3	Представлення на рецензування науковому керівнику рукопису першого розділу випускної кваліфікаційної роботи	До 01.04.2020	01-05.04. 2020
4	Представлення на рецензування науковому керівнику рукопису другого розділу випускної кваліфікаційної роботи	До 15.04.2020	20.04.2020
5	Представлення закінченої випускної кваліфікаційної роботи на кафедру	До 15.05.2020	15-20. 05.2020
6	Підготовка письмового відгуку на випускну кваліфікаційну роботу	До 25.05.2020	25.05.2020
7	Зовнішнє рецензування ВКР	До 01.06.2020	01-05. 06.2020
8	Проведення попереднього захисту випускних кваліфікаційних робіт	05-10. 06.2020	05-10. 06.2020
9	Вирішення питання про допуск випускної кваліфікаційної роботи до захисту	До 15.06.2020	До 15.06.2020
10	Направлення випускної кваліфікаційної роботи із зовнішньою рецензією у ЕК для захисту	За графіком	За графіком

6. Дата видачі завдання « 02 » березня 2020 р.
7. Науковий керівник випускної кваліфікаційної роботи (проекту)
Сонько Юлія Анатоліївна
(прізвище, ініціали, підпис)
8. Керівник проектної групи (гарант освітньої програми) Головня Ю.І.
(прізвище, ініціали, підпис)

9. Завдання прийняв до виконання студент Писаревський Артем Петрович
(прізвище, ініціали, підпис)

10.Відгук наукового керівника випускної кваліфікаційної роботи (проекту):

Тема випускної кваліфікаційної роботи «Державна політика у сфері інформаційної безпеки». Актуальність обраної теми визначається тим, що в умовах швидкого збільшення інформаційної сфери та переходу від індустріального суспільства до інформаційного, що свідчить початок формування інформаційного суверенітету і як наслідок — появи нових загроз котрі можуть впливати на економічне, політичне, етнічне, конфесійне, геополітичне становище та ін. які безпосередньо певним чином впливатимуть на особистість, суспільство так і державу, то стає актуальним питання щодо вдосконалення державної політики та державного управління стосовно інформаційної безпеки України, оскільки забезпечення інформаційної безпеки належить до пріоритетних цілей сучасного державотворення і є одним із основних чинників сталого розвитку країн першого світу. На сьогодні інформаційна безпека України є основною частиною національної безпеки. Без реалізації належного інформаційного забезпечення - ні один з видів безпеки не може бути здійснено, оскільки інформація це універсальний засіб. Як показує історія саме інформаційні ресурси та процеси є причиною конфліктів та криз, що актуалізує питання визначення ключових загроз та обрання ефективного протистояння і боротьби проти агресора.

Об’єктом дослідження виступає державна політика у сфері інформаційної безпеки. Предметом дослідження є процес реалізації державного управління у сфері інформаційної політики. Метою цієї роботи є теоретичне обґрунтування і опрацювання та встановлення рекомендацій на фоні досліджень, методів, загроз в інформаційній безпеці України, щодо покращення державної політики у цій сфері.

Серед позитивних аспектів роботи: в роботі було проаналізовано теоретичні засади дослідження інформаційної безпеки України; розглянуто органи державної влади в системі забезпечення інформаційної безпеки, та визначено їх основні завдання. Безперечною перевагою роботи є те, що автором було досліджено ключові загрози інформаційній безпеці в сучасних

умовах. Розглянуто напрями ефективної співпраці держав в контексті забезпечення безпеки глобального інформаційного простору. Практична цінність роботи визначається тим, що студентом було запропоновано заходи для збільшення ефективності інформаційної безпеки в глобальному просторі, а також досліджено заходи щодо посилення інформаційної безпеки в Україні.

До недоліків можна віднести: описово наведені напрями ефективної співпраці держав в контексті забезпечення безпеки глобального інформаційного простору, рис.1.2. не описано відповідним чином, пункт 2.2. носить незавершений характер. Перераховані роботи не применшують її практичну значимість і загалом не впливають на загальне позитивне враження від роботи.

Робота виконана відповідно до вимог. Оброблено достатню кількість наукової літератури. Відповідно до довідки, наданої студентом, робота має достатній рівень унікальності. Загалом випускна кваліфікаційна робота Писаревського А.П. відповідає встановленим вимогам та може бути допущена до захисту.

Науковий керівник випускної кваліфікаційної роботи (проекту) :
Сонько Юлія Анатоліївна
_____
(підпис, дата)

Відмітка про попередній захист: Головня Юлія Ігорівна
(ПІБ, підпис, дата)

11.Висновок про випускну кваліфікаційну роботу (проект):
Випускна кваліфікаційна робота (проект) студента Писаревського Артема Петровича може бути допущена до захисту екзаменаційній комісії.

Керівник проектної групи (гарант освітньої програми):Головня Юлія Ігорівна
(прізвище, ініціали, підпис)

Завідувач кафедри Новікова Наталія Леонідівна
(підпис, прізвище, ініціали)

« 17» червня 2020 р.

ЗМІСТ

ВСТУП

Актуальність теми. В умовах швидкого збільшення інформаційної сфери та переходу від індустріального суспільства до інформаційного, що свідчить початок формування інформаційного суверенітету і як наслідок — появи нових загроз котрі можуть впливати на економічне, політичне, етнічне, конфесійне, геополітичне становище та ін. які безпосередньо певним чином впливатимуть на особистість, суспільство так і державу, то стає актуальним питання щодо вдосконалення державної політики та державного управління стосовно інформаційної безпеки України, оскільки забезпечення інформаційної безпеки належить до пріоритетних цілей сучасного державотворення і є одним із основних чинників сталого розвитку країн першого світу.

На сьогодні інформаційна безпека України є основною частиною національної безпеки. Без реалізації належного інформаційного забезпечення - ні один з видів безпеки не може бути здійснено, оскільки інформація це універсальний засіб. Як показує історія саме інформаційні ресурси та процеси є причиною конфліктів та криз, що актуалізує питання визначення ключових загроз та обрання ефективного протистояння і боротьби проти агресора.

За обраним напрямком проводили дослідження такі вчені як: Б. Кормич, А. Марущак, Г. Сащук, О. Дзьобань, В. Ліпкан, Ю. Максименко, Є. Кравець, Г. Почепцов, В. Гурковський, П. Шпига, О. Косогов, В. Хімей, В. Домарев та інші.

Мета і завдання дослідження. Теоретичне обґрунтування і опрацювання та встановлення рекомендацій на фоні досліджень, методів, загроз в інформаційній безпеці України, щодо покращення державної політики у цій сфері.

Об’єктом дослідження виступає процес реалізації державної політики у сфері інформаційної безпеки.

Предметом дослідження є теоретико-методичні та прикладні засади державного управління у сфері інформаційної політики.

Зазначена мета вимагає вирішити наступні **завдання**:

– Проаналізувати теоретичні засади дослідження інформаційної безпеки в

Україні;

– Проаналізувати органи державної влади в системі забезпечення інформаційної безпеки;

– Дослідити ключові загрози інформаційній безпеці в сучасних умовах;

– Проаналізувати напрями ефективної співпраці держав в контексті забезпечення безпеки глобального інформаційного простору

– Дослідити заходи щодо посилення інформаційної безпеки в Україні

Методи дослідження. Повнота дослідження забезпечуються системним підходом. Для теоретичного бачення різних позицій проблеми використовується аналіз і синтез, моделювання й узагальнення. Інформаційну базу курсової роботи склали нормативно-правові акти, пов'язані з державною політикою інформаційної безпеки в Україні, а також наукові роботи учених в означеній сфері.

У першому розділі розглянуто підходи до поняття «інформаційна безпека» визначено основну характеристику інформаційної безпеки України, визначено органи державної влади які мають пряме відношення до інформаційної безпеки України.

У другому розділі розглянуто можливі загрози для інформаційної безпеки України, наведено ефективні напрямки співпраці у сфері інформаційної безпеки, досліджено заходи та методи щодо забезпечення інформаційної безпеки та їх реалізація у даній сфері.

Інформаційною базою дослідження стали: Закони України, офіційні матеріали Державного комітету статистики України, оперативна інформація міністерств та відомств, періодичні видання, праці вітчизняних й закордонних науковців з проблеми дослідження, а також інформаційні ресурси інформаційної мережі Internet.

Випускна кваліфікаційна робота складається зі вступу, 2-х розділів, висновків і пропозицій списку використаних джерел і додатків. Основний текст роботи становить 27 сторінок, в т.ч. 1 таблицю, 4 рисунка. Список використаних джерел містить 42 найменування, викладене на 4 сторінках.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

1.1 Інформаційна безпека як основа національної безпеки

В сучасному світі, не виключно і в Україні, інформаційна безпека є основним фактором для забезпечення національної безпеки без якої не відбуватиметься розвиток держави, оскільки вона взаємопов'язує загальну діяльність та грає роль в усіх сферах життєдіяльності людини та державній службі. Вдале планування національно – інформаційної стратегії надалі допомогло б вирішити важливі завдання для України.

Перш за все слід почати з розгляду сутнісного набору нормативно-правових актів які певним чином належать до інформаційної сфери та регулюють її.

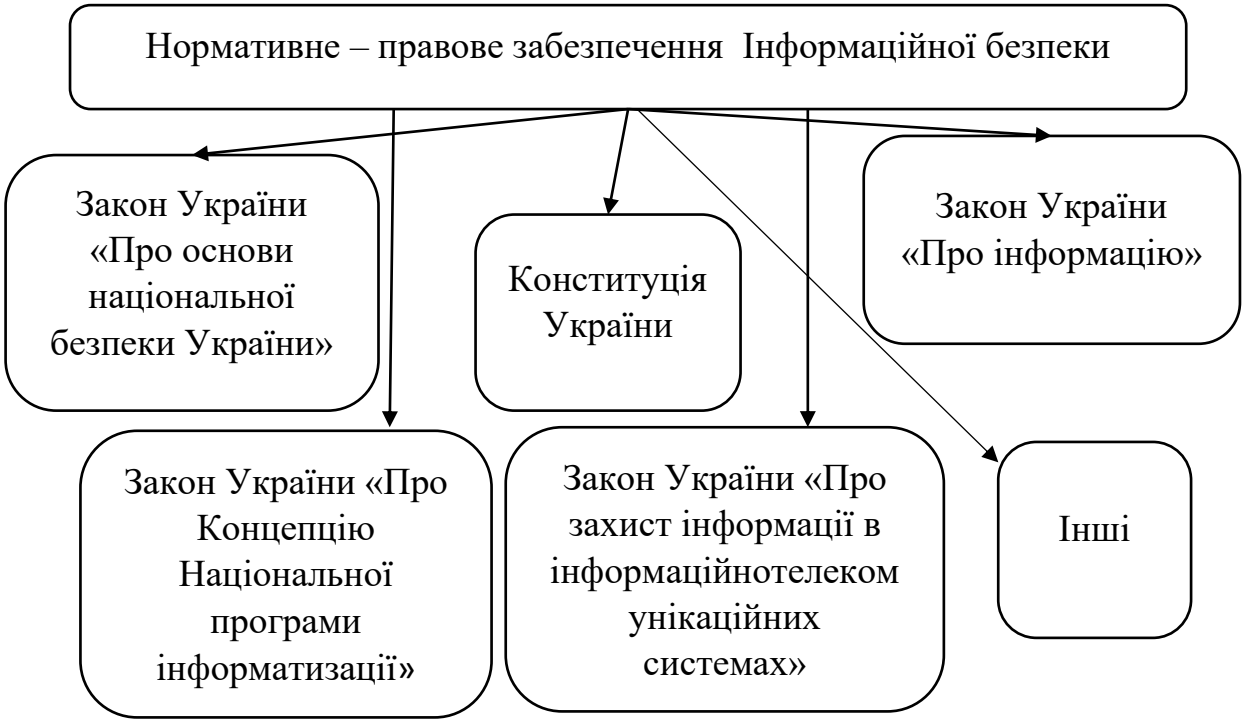

Рис. 1.1 - Нормативно-правові регулятори системи забезпечення інформаційної безпеки

*Розроблено автором на основі даних [3]

Звертаючись до законодавства України, інформаційна безпека, в першу чергу захист якої, згідно зі ст. 17 Конституції України, окрім суверенітету, територіальної цілісності та економічної безпеки, є важливою функцією держави котра здобувається шляхом впровадження сучасних інформаційних технологій, розробки нових актів регулювання, структуризацією функціональної національної інформаційної інфраструктури, створенням та розвитком інформаційних відносин [1].

В Україні науковці поділяють інформаційну безпеку на дві класифікації, першою є інформаційна безпека особистості, а другий це інформаційна безпека держави [2, 3]. Як відомо, безпека особистості перш за все характеризується як захист людини або певних соціальних груп, об'єднань, від негативних явищ, ефектів через прямий або непрямий вплив змінювати їх психологічні стани, та обмежувати свободу вибору [4]. Стосовно Інформаційної безпеки держави — то це в першу чергу стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [5].

Виходячи з того що інформаційну безпеку можна розуміти як комплексне поняття, то більш широко це визначення розкриває В. Ліпкан: «це складова національної безпеки, процес управління загрозами та небезпеками, державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України, вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну, активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України, неухильне дотримання конституційного права громадян на свободу слова доступу до інформації, вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України» [6].

В Законі України «Про Концепцію Національної програми інформатизації» вказано — невіддільною частиною політичної, економічної, оборонної та інших складових національної безпеки є інформаційна безпека [7]. Зазначимо що у багатьох вітчизняних, та закордонних дослідників які вивчають інформаційну безпеку, то вона розглядається як невід'ємна складова національної безпеки. Крім того, інформаційна безпека в такому ракурсі розглядається не просто як окремий елемент національної, але як її інтегральна, якісна характеристика та показник захисту всіх громадян, суспільства і держави [8].

Також у Законі України «Про основи національної безпеки України» достатньо зрозуміло визначено основні напрямки з забезпечення державної політики з питань стосовно національної безпеки в інформаційній сфері, відносять до реалізації наступні дії:

1. Усестороннє забезпечення інформаційного суверенітету на території України;
2. Покращення та вдосконалення повного державного регулювання та розвитку інформаційної сфери шляхом комплексної взаємодії: створення нормативно-правового та економічного середовища для загального розвитку інфраструктури та ресурсів у національній інформаційній сфері, впровадження новітніх сучасних для сьогодення технологій у даній галузі, наповнення й збільшення внутрішньо регіонального та світового інформаційного простору перевіреною, правдивою, неупередженою інформацією про Україну;
3. Активні дії щодо використання та привернення уваги засобів масової інформації до боротьби з такими явищами як корупція, зловживання службовим становищем з боку державних службовців та іншими фактами, які загрожують національній безпеці України;
4. Встановлення неухильного дотримання конституційного права громадян України до доступу до інформації, свободу слова, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації на території України, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;
5. Використання спеціальних комплексних заходів направлених на захист

національного інформаційного простору та протидії монополізації інформаційної сфери на території України.

Свій вклад у дослідження зробив Є. А. Кравець, який проаналізував та сформував характеристику Інформаційної безпеки [9].

Характеристика Інформаційної безпеки

- Законодавче формуванням державної інформаційної політики
- Гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України
- Всебічний розвиток інформаційної структури
- підтримка розвитку національних інформаційних ресурсів країни, враховуючи досягнення науки і техніки та особливості духовного й культурного життя народу
- Створення згідно з законами України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, об'єднаннями громадян, громадянами, а також іншими суб'єктами права в Україні;
- Охорона державної таємниці, інформації з обмеженим доступом, яка є об'єктом володіння, розпорядження, користування лише державою або об'єктом права власності;
- Створення та впровадження безпечних інформаційних технологій;
- Створення загальної системи охорони інформації, зокрема інформації з обмеженим доступом та державної таємниці;
- Захист національного інформаційного простору від поширення забороненої законодавством для поширення інформації;
- Законодавче визначення порядку поширення інформації зарубіжного виробництва на території держави.

Рис. 1.2 - Характеристика інформаційної безпеки

*Розроблено автором на основі даних [9]

Можна зробити проміжний висновок, що інформаційна безпека представляє із себе одне із важливих факторів у різноманітних сферах людського життя та діяльності, а також має багатоманітне значення в залежності від підходів та змісту у сфері інформаційної безпеки.

1.2 Органи державної влади в системі забезпечення інформаційної безпеки України

Важливим завданням залишається хто саме буде здійснювати забезпечення інформаційної безпеки. Встановлення та обрання ефективного регулювання інформаційною безпекою як координаційного та командного методу для логічного розподілу зобов'язань між органами влади.

Реалізація політики інформаційної безпеки забезпечується системою інститутів публічної влади, інститутами громадянського суспільства, їх компетенція це розв'язання питань щодо створення безпечних умов функціонування і розвитку інформаційної сфери [10].

Об'єктами інформаційної безпеки слід вважати: події та явища в галузі політики, економіки, культури, охорони здоров'я, а також у соціальній, екологічній, міжнародній та інших сферах, свідомість, психіку людей; інформаційно-технічні системи різного масштабу і призначення. Якщо ж вести мову про соціальні об'єкти інформаційної безпеки, то до них можна віднести особистість, людину, колектив, суспільство, державу, світова спільнота.

Склад чинного механізму встановлено ст. 4 Закону України «Про основи національної безпеки України», а саме: Верховна Рада України, Президент України, Кабінет Міністрів України, Рада національної безпеки і оборони України, міністерства та інші центральні органи виконавчої влади, Національний банк України, суди загальної юрисдикції, прокуратура України, місцеві державні адміністрації та органи місцевого самоврядування: Збройні Сили України, Служба безпеки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України. [11].

На сьогодні в Україні створені такі центральні органи котрі напряму займаються питанням інформаційної безпеки: Національна рада з питань телебачення та радіомовлення, Державний комітет інформаційної політики, телебачення і радіомовлення України, Державний комітет зв'язку та інформатизації України, Рада національної безпеки та оборони України.

Згідно зі ст. 107 Конституції України, РНБО – це «координаційний орган з питань національної безпеки і оборони при Президентові України» [12].

Державний комітет інформаційної політики, телебачення і радіомовлення України, координується Кабінетом Міністрів України. У своїй діяльності керується Конституцією України, законами України, актами Кабінету Міністрів України, актами Президента України. Робить внесок до застосування і розробки законодавства що належать до його компетенції, вносить їх на розгляд Кабінету Міністрів України та Президентові України.

До основних завдань відносять:

1. Аналіз та прогнозування тенденцій розвитку інформаційного простору України;

2. Формування та реалізація державної політики в інформаційних та видавничій сфері;

3. Розроблення заходів, які спрямовані на розвиток видавничої справи, виробників інформаційної продукції;

4. Координація діяльності державних медіаресурсів з метою поширення найважливішої інформації яка відбувається на території держави;

Не менш важливою є роль Державного комітету зв'язку та інформатизації України, який підпорядковується Кабінету Міністрів України, виконує важливі функції Адміністрації зв'язку України, забезпечує та відповідає за державну політику в галузі зв'язку, розподіл та використання радіочастотного ресурсу в діяльності забезпечення інформатизації, відповідає за їх розвиток. Керується Конституцією України, законами України, актами Кабінету Міністрів України, актами Президента України. Розробляє пропозиції законодавства у цій сфері, та виносить їх на розгляд.

До завдань Держкомзв'язку відносять:

1. Регулювання діяльності яка спрямована на потреби споживачів у послугах зв'язку, та діяльності що пов'язана з радіочастотами ресурсами;

2. Формування та реалізація державної політики щодо зв'язку, використанню, розподілу радіочастотного ресурсу;

3. Розвиток підприємництва на основі конкурсних засад в галузі послуг зв'язку;

4. Реалізація заходів щодо розробки та вдосконаленню національної системи зв’язку, підтримка її стабільного функціонування;

Вагового внеску для радіомовлення і телебачення, а також підвищення рівня надання передач і програм є Національно рада України з питань телебачення і радіомовлення, яка підзвітна Президентові України та Верховній Раді України.

Згідно з Конституцією України та Закону «Про телебачення і радіомовлення» покладено такі завдання:

1. Дотримання законодавства України с сфері телебачення і радіомовлення;
2. Забезпечення свободи слова;
3. Захист прав та інтересів радіослухачів та телеглядачів, виробників телерадіопрограм на законній підставі;
4. Раціональне використання радіочастотного ресурсу;
5. Здійснення та розробка ліцензування телерадіоорганізацій;

Значну діяльність в інформаційній сфері безпосередньо виконує Служба безпеки України, яка згідно з нормами ст. 1 Закону «Про службу безпеки України» визначається як «державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України» [13]. Контролюється: Президентом України, Верховною Радою та Кабінетом міністрів України.

Органи державної влади, у компетенцію яких входить регулювання соціально-політичних відносин в інформаційній сфері, а також недержавні суб'єкти даної діяльності, які залучаються для вирішення завдань державного управління, виступають у якості суб'єктів державної інформаційної політики та забезпечують рух її правового й організаційного механізмів. [14]

Після теоретичного аналізу діяльності державних органів можливо окреслити сукупні дії, що мають здійснюватися ними у сфері забезпечення інформаційної безпеки:

1. забезпечення та охорона прав громадян в інформаційній сфері, що закріплені в Конституції, державних та міжнародних правових актах;
2. розробка і реалізація державної інформаційної політики;
3. розвиток та узгодження нормативно-правової бази у сфері інформаційної

безпеки;

4. формування і розвиток закладів та інституцій, сферою відповідальності яких є інформаційно-психологічна безпека;

5. забезпечення інформаційного суверенітету України;

6. захист державних таємниць.

7. сприяння розвитку національного інформаційного простору [15,16,17].

На цьому можна завершити аналіз теоретичних засад інформаційної безпеки України і зробити проміжний висновок, що законодавча база з питань інформаційної безпеки прописана у Законі України та інших правових актах, питанням інформаційної безпеки займається велика кількість науковців, також визначено декілька органів влади які забезпечують інформаційну безпеку та встановлено їх завдання.

РОЗДІЛ 2
ПРІОРИТЕТНІ НАПРЯМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В СУЧАСНИХ УМОВАХ

2.1 Ключові загрози інформаційній безпеці в сучасних умовах

Як і всі об’єкти інформаційна безпека не виняток і теж має певні загрози які треба вчасно виявити та звести до мінімуму. Як вказано в Законі України "Про основи національної безпеки України" під загрозами розуміються наявні, та потенційно можливі явища і чинники, які створюють небезпеку важливим національним інтересам [19].

Види загроз дуже різні та мають низку класифікацій:

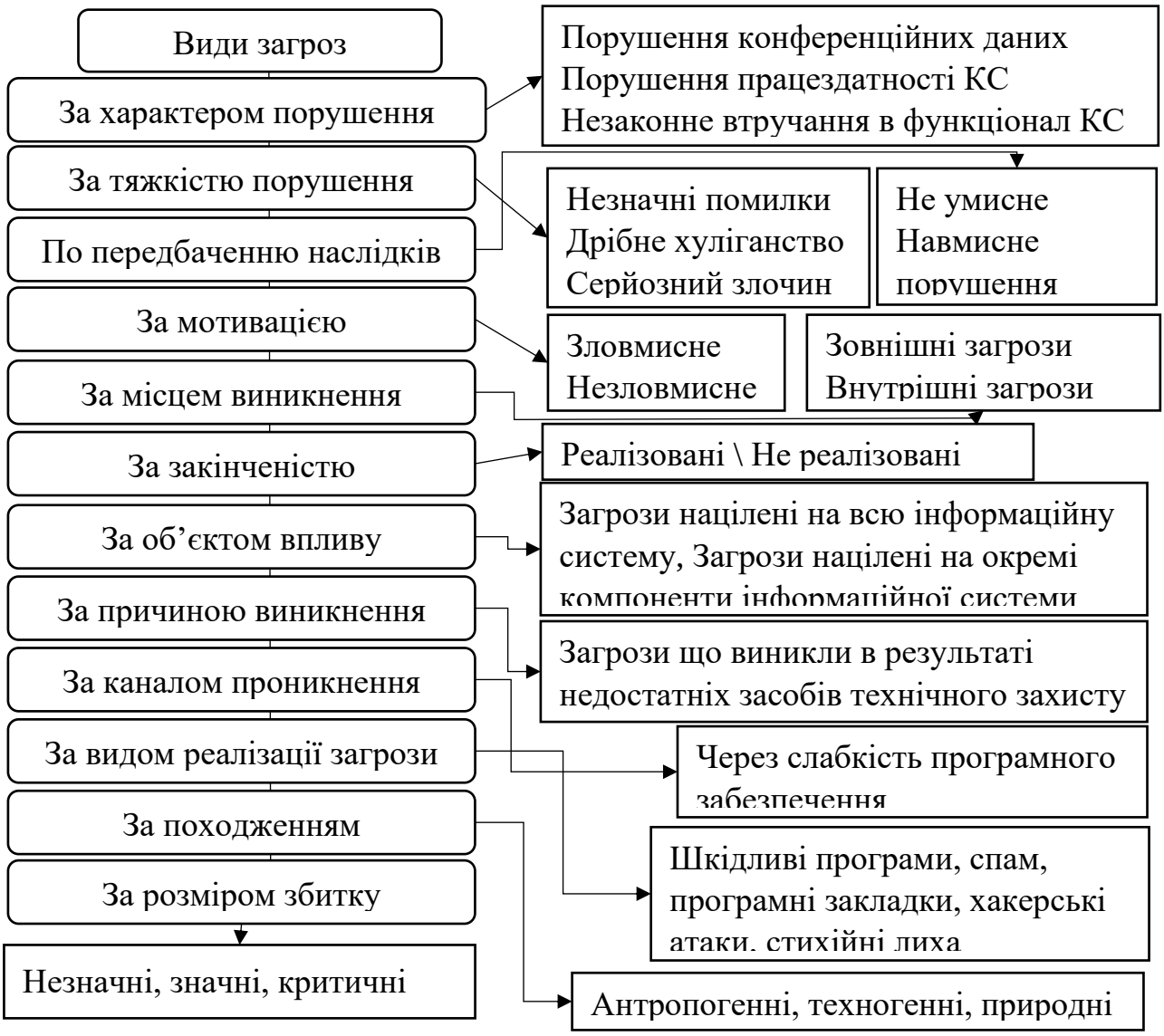

Рис. 2.1 - Види та класифікація загроз
*Розроблено автором на основі даних [18]

В офіційних документах, а саме закон «Про основи національної безпеки України» виділено п’ять основних загроз у сфері інформаційної безпеки: [19]

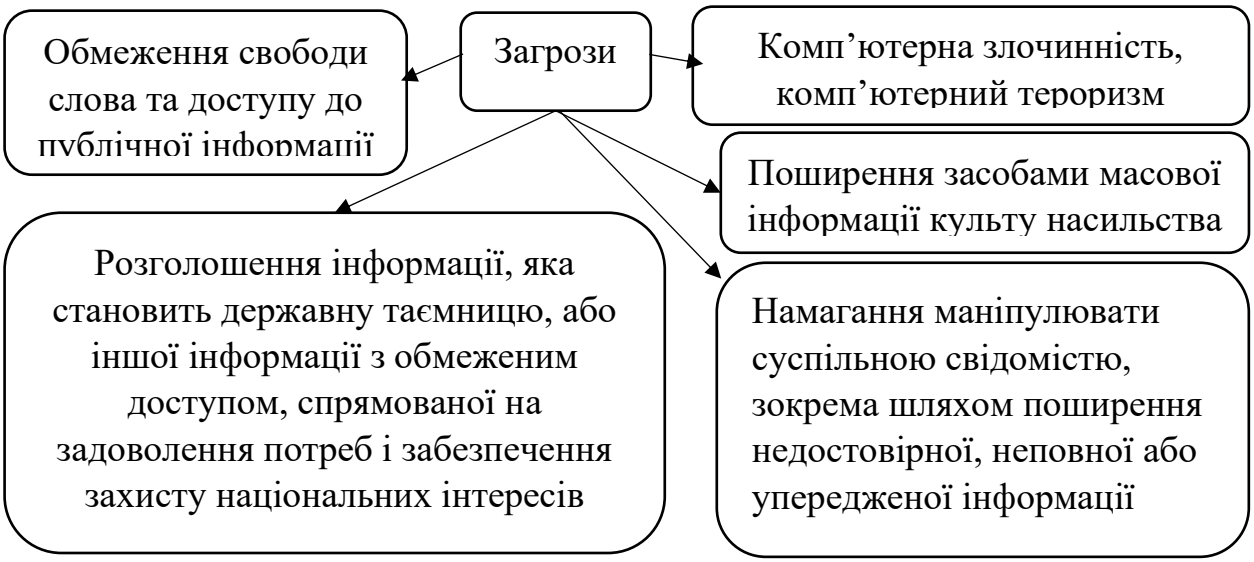

Рис. 2.2 - Основні загрози національній безпеці у сфері інформаційної безпеки
*Розроблено автором на основі даних [20]

Якщо брати до уваги сучасний стан України, а саме умови гібридної війни проти нашої держави, то до загроз слід віднести — інформаційну зброю яка використовується проти України. Деякі дослідники надають таке тлумачення інформаційній зброї — це інформація (дані), які є засобом ведення інформаційних воєн і призначення яких полягає в зміні системних якостей об’єкта інформаційного впливу за допомогою прихованих установок на здійснення задуманих користувачем інформаційної зброї дій.

До прикладів інформаційної зброї відносять:

1. Дезінформацію у будь-якому вигляді;
2. Впровадження агентів інших держав у засоби масової інформації для дестабілізації стану суспільства;
3. Пропагандистські акції у сфері політики та культури;
4. Порушення чи модифікація інформаційного середовища та ресурсів;
5. Здійснення певного впливу на політичну еліту;
6. Несанкціоноване проникнення в систему управління баз даних, зараження

вірусами комп'ютерні системи;

7. Підтримка опозиційних рухів [21].

В цьому зв'язку О. М Косогов проаналізував що через застосування інформаційної зброї яку використовують іноземні держави проти України з'явилися реальні загрози для нашої держави, про це свідчать такі дії:

1. Дискредитація України як конкурента у сфері міжнародного військово-технічного співробітництва;

2. Необ'єктивна критика вищого державного керівництва України;

3. Зростання для України загроз кібер-атак, що обумовлено появою нових, більш досконалих зразків кібернетичної зброї

4. Збільшення інформаційних заходів для перешкоджання реалізації Україною зовнішньополітичного курсу та спонукання її до участі в проектах, які в сучасних умовах не вигідні нашій державі;

5. Посилення і реалізація деякими іноземними державами певних дій для створення несприятливого до України міжнародного іміджу;

6. Здійснення інформаційного тиску на Україну на меті якого є спонукання українського керівництва до прийняття вигідних для іноземних країн рішень у внутрішній та зовнішній політиці [22].

Спираючись на дослідження О. Дзьобаня можливо виділити декілька груп загроз інформаційній безпеці. Перша це та котра пов'язана з інформаційною зброєю вплив якої відбувається на психіку та свідомість людей, армію, технічно-інформаційну інфраструктуру суспільства. Друга – це інформаційно-технічні загрози які впливають на особистість її свідомість та підсвідомість, суспільство, державу, злочини з використанням сучасних технологій, махінації з електронними грошима, тощо. Третя група – інформаційно технічні загрози – введення електронного контролю за життям людей та політичними організаціями, їх настоями, планами. Четверта група – це використання інформаційних технологій у політичних цілях [23, 24].

Слід зазначити що загрози також посилюються через певну кількість проблем пов'язаних з функціонуванням нашого інформаційного простору. До головних чинників негативних посилень відносять:

1. Технічне відставання інформаційної інфраструктури та пряму залежність від іноземної техніки та спецзасобів, це наслідки від занепаду телекомунікаційної промисловості;

2. Інвестування за «залишковим принципом» інформаційних структур;

3. Недостатній кваліфікаційний рівень підготовки працівників інформаційної сфери;

4. Збільшення закордонних виробників інформаційної продукції на «українських полицях» [25].

Що стосується інформаційної безпеки суспільства то до них також відносять таку загрозу як незаконне приховування відкритої інформації, модифікація такого виду інформації або знищення, наслідком таких дій може спричинити посилення корупції та інших економічних злочинів, маніпуляція свідомістю людей [26].

Також до важливих об’єктів інформаційних загроз слід виділити вплив на духовну сферу суспільства, складовими якої є соціально – психологічний стан людей, суспільна думка та суспільна свідомість. Одним з найрозповсюдженіших видів інформаційних загроз є так звані патогенні тексти. Патогенними текстами вважаються ті котрі мають на меті повідомлення стосовно суперечливості ідеологічній системі яка використовується на сьогоднішній день. Зокрема, у різних системах цінностей патогенними вважаються тексти, що:

1. Спрямовані на підрив віри у Бога;

2. На підрив національних та державних інтересів; загрожують суспільній моралі;

3. Загрожують глобальній безпеці;

4. Мають шкідливий психологічний вплив;

5. Призводять до нехтування основними правами та свободами.

Іноді в патогенних текстах можуть буди приписані державні та інші види таємниць, деякі з таких текстів навіть втручаються у особисте життя людини як особистості [27].

2.2 Напрями ефективної співпраці держав в контексті забезпечення безпеки глобального інформаційного простору

В наш час коли в Україні відбуваються процеси які наближують Євроінтеграцію, особливо важливим для держави залишається правильне та ефективне забезпечення рівноважного розвитку інформаційної безпеки в Україні, котра виявляється у міжнародній співпраці з іншими країнами та організаціями. Як відомо Україна, ЄС та НАТО історично опинилися в певному взаємозалежності, в сучасний час Україна на жаль не може ефективно здійснювати протистояння поточним загрозам з боку Росії без вагомої міжнародної підтримки, а ЄС і НАТО – в першу чергу зацікавлені в демографічній та економічній стабільності в Україні, що гарантуватиме їх власну безпеку в просторі. Як результат це створило основу для тристороннього партнерства на меті якого було зміцнення стабільності у Європі в контексті гарантування безпеки та навколо України з довгостроковою метою забезпечення регіональної стабільності, миру та процвітання [30].

Відділи інформаційної безпеки обов’язково входять до структури державних та приватних підприємств, установ, організацій, де для роботи використовуються інформаційні ресурси, несанкціонований доступ до яких може завдати шкоди. Технічні засоби, що надають безпеку інформації, створюються спеціальними організаціями, такими як ДП «Українські спеціальні системи», до якого у січні 2020 року увійшло ДП «Державний центр інформаційної безпеки», ТОВ "Український центр інформаційної безпеки» та ін. Контроль за дотриманням інформаційної безпеки в Україні здійснюється на вищому державному рівні. Так при РНБО діє спеціальна міжвідомча комісія.

Україна є учасником програми «Наука заради миру та безпеки», що запроваджена НАТО та має на меті реалізацію заходів, направлених на підвищення безпеки інформації. Згідно цієї програми, задля досягнення поставлених завдань використовуються такі засоби:

1. Видача грантів на реалізацію проектів;
2. Консультації експертів;

3. Обмін технологіями;

4. Встановлення нових та підтримка існуючих зв’язків;

Спільна діяльність України та НАТО у відповідності до програми «Партнерство заради миру» заснована на принципах інформаційної безпеки в умовах вільного обміну важливими даними. Це потрібно для збільшення прозорості планування оборонних бюджетів держав, відкритості даних про стан збройних сил, планування змін у військовій сфері задля збереження миру. Зважаючи на важливість цієї стратегічної інформації та великі ризики при несанкціонованому доступі, кожна з країн-учасниць «Партнерства заради миру» повинна бути впевненою, що інша сторона має технічну можливість забезпечити збереження секретних даних, які передаються.[28,29].

Міжнародне співробітництво у сфері інформаційної безпеки має наступні напрямки:

1. Недопущення відкритого доступу до секретної інформації, яка стосується забезпечення міжнародної торгівлі, фінансових операцій, правоохоронної діяльності в тому числі боротьби з тероризмом, поширенням наркотичних речовин, організованими злочинними групами.

2. Запобігання створенню та введенню в дію інструментів інформаційної війни.

3. Створення безпечних умов для вільного обміну інформацією між країнами із застосуванням державних каналів зв’язку та телекомунікації.

4. Спільна діяльність правоохоронців країн-учасниць світової спільноти для запобігання кіберзлочинності.

Беручи за зразок країни Європейського Союзу та зокрема НАТО, Україна розбудовує власну структуру забезпечення інформаційної безпеки як таку, що постійно захищає комп’ютерні мережі від можливих кібератак, а також ефективно протидіє кіберзлочинності. Такий підхід є доцільним, адже завдяки йому за 2018 рік було попереджено понад чотириста атак на комп’ютерні мережі стратегічного значення [31].

У 2016 році в Україні була затверджена державна Стратегія кібербезпеки. Відтак, цей документ є першочерговим джерелом для планування будь-яких заходів з

дотримання інформаційної безпеки. Зокрема Стратегією передбачено поетапний перехід до стандартів кібербезпеки Європейського Союзу та блоку НАТО, а також постійне співробітництво з ними у цьому напрямку. Стосовно військового сектору, Україна повністю переймає досвід НАТО у дотриманні правил кібербезпеки, а також використовує інформаційний простір у якості сфери здійснення операцій [30,32].

На законодавчому рівні, зокрема у Законі України «Про основні засади забезпечення кібербезпеки України», використовується термінологія аналогічна тій, що зустрічається у правовій базі НАТО та Європейського Союзу. Це дає можливість більш тісної співпраці, а також забезпечення відповідальності сторін. В цьому документі простежуються характерні для країн Європи засади, а саме прозорість, доступність, стійкість, захист інформаційного простору. Також увага приділена точкам дотику державного та приватного інформаційного простору з метою забезпечення кібербезпеки [30,33].

Впродовж 2017-2018 років Європейський Союз надав значну технічну підтримку Україні в рамках програми Technical Assisstance and Information Exchange, направлену на реалізацію трьох основних напрямків кібербезпеки. А саме: розробку нормативної бази, запровадження громадсько-приватного партнерства та популяризацію діяльності державних структур, які забезпечують кібербезпеку, а також підвищення кваліфікації співробітників відповідальних за інформаційну безпеку структур в Україні [30].

Також значимою є консультаційна допомога Європейського Союзу – EU Advisory Mission to Ukraine, яка направлена на захист від загроз порушення інформаційної безпеки. Бюджет місії – 2,5 мільйонів євро. Вона спрямована на покращення технічного забезпечення вітчизняної кіберполіції, проведення просвітницької роботи: консультацій, тренінгів, дискусій в яких беруть участь члени Європолу та інші спеціалісти [30].

У 2014 році в Україні стартував проект, що мав на меті утворення структур, які б реагували на загрози порушення інформаційної безпеки, здійснювали постійний моніторинг. Також на меті було обладнання технічних лабораторій для вивчення несанкціонованої діяльності в інформаційному просторі та усунення негативних

наслідків. Необхідне обладнання було отримано влітку 2017 року, а на початку 2018-го року організовано роботу Ситуаційного відділу, який відповідає за інформаційну безпеку СБУ. Цей проект був профінансований Альянсом НАТО, його бюджет склав понад 1 мільярд доларів США. Слід зазначити, що фінансування з боку НАТО мають також профільні урядові структури, зокрема Міністерство внутрішніх справ [30].

Впродовж 2015 року для фахівців з України Естонією було організовано навчальну програму з метою отримання інформації про загрози у кіберпросторі, отримання досвіду реагування на дії зловмисників. В Естонії працює Центр передового досвіду, одним з напрямків діяльності якого є вивчення ситуації з забезпеченням кібербезпеки в Україні та надання консультативної допомоги [30].

Фахівці з України у 2018 році долучилися до програми НАТО «Вдосконалення військової освіти». Її мета – це розгляд та практичне застосування інформаційних операцій, направлених на підтримку військових місій [30].

2.3 Заходи щодо посилення інформаційної безпеки в Україні

В Україні головні напрямки діяльності для забезпечення інформаційної безпеки держави це великий перелік комплексних заходів, до яких відносяться: розвиток науково-практичних основ, розвиток нормативно правової та законодавчої бази інформаційної безпеки, розробка нормативно-правових документів, розвиток та вдосконалення концепції інформаційної безпеки, формування правового статусу суб'єктів системи, відновлення порушеного права та ресурсів, реалізація компенсаційних мір, вдосконалення організаційних форм та методів запобігання і нейтралізації загроз інформаційній безпеці та розвиток сучасних методів [34].

Функціонування та посилення окремих взаємозалежних зв'язків в інформаційній безпеці досягається шляхом здійснення різноманітних процесів, заходів, засобів, прийомів та способів, котрі в загальному розумінні складають методи. Метод передбачає послідовність дій за конкретним планом. Усі методи які існують у сфері можуть змінюватися від типу діяльності в котрій вони використовуються [35, 36].

Поширеними методами стану інформаційної безпеки є методи дослідження причинних зв'язків. За використанням даних методів визначаються причинні зв'язки між небезпеками, загрозами, ризиками та викликами; реалізується пошук причин, які стали першочерговим джерелом та викликали актуальність питань різноманітних факторів небезпеки, також опрацьовуються та вдосконалюються заходи щодо їх протистояння та усунення. До числа методів причинних зв'язків належать: метод змін, метод відмінності, метод сполучення схожості й відмінності, метод схожості, що супроводжують, метод залишків.

Методами аналізу стану інформаційної безпеки є методи опису та класифікації. Щоб ефективно здійснити захист інформаційного середовища України, слід, по-перше описати, потім класифікувати різноманітні види загроз та небезпек і правильно сформувати систему заходів для управління ними.

Визначення використовування певного методу аналізу стану забезпечення інформаційної безпеки залежить від рівня та сфери організації захисту. Відповідно до загрози стає доступним завдання для диференціації різноманітних рівнів загроз та

різноманітних рівнів захисту та протидії. В інформаційній безпеці виокремлюють: Процедурний, мережевий, рівень користувача, технологічний, управлінський, програмно-технічний, фізичний рівні.

Таблиця 3.1

Рівні захисту інформаційної безпеки

РІВНІ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
Фізичний рівень	Організація та фізичний захист інформаційних ресурсів, інформаційних технологій котрі використовуються;
Програмно-технічний рівень	Перевірка та ідентифікація користувачів КС, протоколювання, управління доступом до КС, аудит, екранування, забезпечення доступу;
Управлінський рівень	управління, контроль, координація організаційних, технологічних та технічних заходів на всіх рівнях системи забезпечення ІБ
Технологічний рівень	Реалізація політики інформаційної безпеки шляхом використовування набору сучасних автоматичних інформаційних технологій;
Рівень користувача	Зменшення впливу на об’єкти інформаційної безпеки, унеможливлення інформаційного впливу з людського боку;
Мережевий рівень	Координація дій у системі управління, які мають спільну мету;
Процедурний рівень	Реалізовані безпосередньо людьми. До нього відносять такі процедурні заходи: планування робіт з ремонту, реагування на порушення, управління персоналом, фізичний захист, підтримка працездатності.

Джерело: [37]

Серед методів, які застосовуються у заходах з дотримання безпеки інформації, можна виокремити наступні:

1. Методи одного рівня – ті що використовують тільки один з принципів керування

безпекою інформації.

2. Методи з багатьма рівнями – ті, які розроблені з урахуванням мінімум двох принципів керування безпекою інформації. Особливість цих методів у тому, що кожен з принципів відповідає за певну задачу, вони зазвичай працюють окремо.

3. Методи комплексної взаємодії – ті, у яких технології мають декілька рівнів, тісно пов'язані між собою в єдине ціле з метою всебічного управління безпекою інформації.

4. Поєднані високотехнологічні методи – це технології з багатьма рівнями та компонентами, у яких для управління безпекою інформації використовуються новітні технологічні засоби в тому числі штучний інтелект [38].

Методи роботи у сфері інформаційної безпеки можна розглянути також як юридичні(правові), економічні та технічно-організаційні.

Серед **юридичних** методів можна назвати: створення нормативної бази, згідно якої має відбуватися регулювання стосунків у в інформаційній галузі, а також розробку юридичних документів, направлених на дотримання безпеки інформації в нашій державі. Основні напрямки правових методів наступні:

1. Оновлення законодавчої бази, яка стосується сфери забезпечення інформаційної безпеки шляхом внесення поправок, доповнень до існуючих законів та підзаконних актів. Мета цього напрямку – приведення законодавчої бази України до міжнародних стандартів, наприклад, ЄС, НАТО та ін., посилення вимог до забезпечення інформаційної безпеки на загальнодержавному рівні, в порядкування юридичних норм, за якими встановлюється відповідальність за порушення у галузі безпеки інформації.

2. Запровадження в дію нормативно-правової бази, яка визначає ступінь відповідальності фізичних та юридичних осіб за незаконне використання інформації. В тому числі доступ, копіювання, розповсюдження без відповідного дозволу, а також

зумисне викладення в різних джерелах неправдивої інформації, розголос конфіденційних даних, використання інформації у злочинній діяльності.

3. Встановлення на загальнодержавному рівні пріоритету на розвиток українських комунікаційних мереж, в тому числі випуск та використання власних супутників.

4. Упорядкування повноважень між органами влади стосовно управління галуззю інформаційної безпеки, формулювання мети і задач. Регулювання участі громадських організацій, окремих осіб у заходах, пов'язаних з інформаційною безпекою.

5. Врегулювання діяльності компаній, які є постачальниками послуг Інтернет на території України, юридичний нагляд та контроль над їхніми діями.

6. Розробка нормативної бази, яка б дозволила створити в Україні середовище інформаційної безпеки, а також формування структури управління цією сферою на рівні державних установ [39].

До **економічних** методів, які дозволяють забезпечувати інформаційну безпеку в нашій держав, можна віднести:

1. Створення спеціальних програм, які дозволять удосконалити роботу в цій галузі, та, відповідно, пошук джерел їх фінансування.

2. Перегляд та усунення недоліків існуючої схеми фінансування діяльності, направленої на реалізацію юридичних, технічних та організаційних методів захисту даних. Удосконалення страхової системи, в контексті додавання ризиків втрати інформації юридичними та фізичними особами [40].

Щодо **технічно-організаційних** методів у галузі безпеки інформації, які працюють в нашій державі, варто назвати такі:

1. Розробка ефективної системи, яка б на належному рівні забезпечувала інформаційну безпеку по всій території Україні. Активна робота виконавчої влади всіх рівнів, з використанням відповідних юридичних норм, направлена на подолання злочинності та правопорушень в інформаційній галузі.

2. Вдосконалення старих та створення нових засобів контролю за дотриманням норм інформаційної безпеки. Забезпечення захисту систем зв'язку, підвищення надійності захисних програм.

3. Впровадження в дію технічних засобів , які попереджають несанкціонований

доступ до інформаційних систем сторонніх осіб, які мають на меті викрадення, видалення, спотворенні даних, вивід з ладу засобів комунікації.

4. Знаходження та знешкодження спеціального обладнання та програмного забезпечення, які несуть шкоду системам зв'язку, можуть перехоплювати дані. Використання спеціальних шифрів для передавання важливої стратегічної інформації.

5. Видача ліцензій, сертифікатів, дозволів на діяльність у галузі забезпечення інформаційної безпеки.

6. Вироблення єдиних вимого до сертифікованих засобів обробки даних, з урахуванням законодавства про забезпечення інформаційної безпеки.

7. Підвищення кваліфікації кадрів, які працюють з важливою інформацією, посилення вимог щодо дотримання інформаційної безпеки, контроль дій працівників цієї сфери.

8. Розробка комплексної системи нагляду за станом дотримання інформаційної безпеки в Україні, особливо у стратегічно важливих галузях [41, 42].

Згадані вище останні три методи, постійно використовуються на кожному з етапів забезпечення інформаційної безпеки, або подолання наслідків порушень, що сталися.

Рішенням проблем можуть стати наступні етапи:

1. Обрання сфери діяльності, де існують ризики порушення принципів інформаційної безпеки.

2. Розробка єдиної багаторівневої стратегії, алгоритму дій в політичній, соціальній, економічній, публічній та інших галузях.

3. Сприяння розумінню надважливого значення забезпечення захисту даних в органах державної безпеки.

4. Формування єдиної політики інформаційної безпеки в Україні з урахуванням ключових ресурсів, а саме: політичних, адміністративних, соціальних та ін.

ВИСНОВКИ

1. В роботі було проаналізовано теоретичні засади дослідження інформаційної безпеки України. Аналізуючи проблеми інформаційної безпеки України, доцільно вказати на невизначеність та розбіжність думок між науковцями що до визначення інформаційної безпеки як основи національної безпеки, вирішенням цієї проблеми може стати проведення конференції між співтовариством науковців та державою для надання нового сучасного для нашого часу значення інформаційної безпеки.

2. Нами було проаналізовано органи державної влади в системі забезпечення інформаційної безпеки, та визначено їх основні завдання, якщо казати загально то основна проблема органів державної влади це відсутність загальної та узгодженої системи суб'єктів забезпечення інформаційної безпеки, органів наділених відповідними завданнями та функціями й засобами для виконання певних завдань, це може ставити під загрозу інформаційний суверенітет держави. Вирішенням цього питання може стати реформування законодавства з питань інформаційної безпеки та певних суб'єктів на прикладі країн Європи.

3. Досліджено ключові загрози інформаційній безпеці в сучасних умовах, визначено що проти України використовується сучасні технології та методи інформаційно-психологічних, та інших впливів, котрі використовуються задля дестабілізації України в її інформаційному просторі. Розв'язати це питання допоможе ефективна взаємодія між органами державної влади, впровадження нових сучасних технологій протистояння інформаційним загрозам в процес державного управління, модернізація та реалізація загальної системи забезпечення національної безпеки та інформаційної політики в Україні.

4. Розглянуто напрями ефективної співпраці держав в контексті забезпечення безпеки глобального інформаційного простору. Зовнішня політика України є складовою інформаційної безпеки та простору, тому для забезпечення глобальної інформаційної безпеки Україна співпрацює з Європейськими країнами які мають спільну мету – забезпечення інформаційної безпеки. Пропонуємо наступні дії для

збільшення ефективності інформаційної безпеки в глобальному просторі , а саме: для початку - поширення грамотності у сфері інформаційної безпеки між громадянами України сучасними методами, та у подальшому співпраця у вигляді громадянин-держава, що допоможе в довготривалій перспективі реагувати на інформаційні небезпеки швидше, та сприятливо відобразиться на міжнародній співпраці у боротьбі з інформаційними загрозами та небезпеками.

5. Досліджено заходи щодо посилення інформаційної безпеки в Україні. Держава використовує зазначені методи та засоби, але ефективне регулювання та реалізація даних методів не закріплена належним чином на законодавчому рівні, тому залишається питання щодо розробки певного документу на державному рівні який буде контролювати виконання перелічених засобів забезпечення інформаційної безпеки для збільшення ефективності за використанням методів.

Підсумовуючи слід зазначити що державна політика у сфері інформаційної безпеки України є одним із головних чинників щодо забезпечення загальної національної безпеки, вона впливає на економічне, політичне, геополітичне, та інші становища в сучасній Україні, які безпосередньо певним чином впливатимуть на особистість, суспільство та державу. Вищенаведене актуалізує необхідність проведення досліджень, спрямованих на вирішення проблем з інформаційними небезпеками та загрозами, а також вдосконаленням правової бази у питанні інформаційної безпеки на рівнях особистості, суспільства та держави для більш ефективного вирішення питань у даній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України від 28.06.1996 // Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141

2. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література, 2003. 472 с.

3. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки // Державна безпека України. 2011. № 21. С. 92- 95.

4. Г. Сащук «Інформаційна безпека в системі забезпечення національної безпеки» [Електронний ресурс]. – Режим доступу : https://web.archive.org/web/20151110042232/http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php

5. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007—2015 роки» від 09.01.2007 № 537-V

6. Ліпкан В. А. Національна безпека України: навч. посібник / В. А. Ліпкан. – К.: Кондор, 2009. – 576 с. с. 21

7. Про Концепцію Національної програми інформатизації: Закон України від 4 лютого1998 р. // Відомості Верховної Ради. – 1998. – No 27-28. – Ст. 182.

8. Інформаційна безпека України в умовах євроінтеграції: навч. посібник / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. – К.: КНТ, 2006. – 280 с. с.46

9. Кравець Є. А. Інформаційна безпека держави / Є. А. Кравець // Юридична енциклопедія [Текст] : в 6 т. — К. : Укр. енцикл., 1992. — С. 744.

10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017 / Верховна Рада України. Законодавство України. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/47/2017

11. Про основи національної безпеки України: Закон України від 19.06.2003. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/964-15

12. Конституція України від 28.06.1996 // Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 14

13. Про службу безпеки України: Закон України від 25.03.1992 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2229-12

14. Почепцов Г. Інформаційна політика : навч. посіб. / Г. Почепцов, С. Чукут. – К. : Вид-во УАДУ, 2002. – 88 с.

15. Гурковський В. Взаємовідносини органів державної влади у сфері забезпечення інформаційної безпеки України: організаційно-правові питання/ Вісн. УАДУ : наук. журн. 2002. № 3. С. 27-31.

16. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017[Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/47/2017

17. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 р[Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/ show/287/2015

18. Черевко О.В. Електронний журнал «Ефективна економіка» Ефективна економіка № 5, 2014 [Електронний ресурс]. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=3304

19. Закон України "Про основи національної безпеки України". — К., 2003. — 1 с.

20. Про основи національної безпеки України : Закон України 09.06.2003 р. № 964–IV / Верховна Рада України. Законодавство України. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/964-15

21. Шпига П.С. Рудник Р. М. Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин. 2014. Вип. 8. С. 326–339.

22. Косогов О.М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору. Збірник наукових праць Харківського університету Повітряних Сил. 2014. Вип. 3. С. 127–130.

23. Шемчук В.В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктрини й законодавчої основи. // Теорія та історія держави і права; історія політичних і правових учень Том 30 (69) № 4 2019 – С. 31-37

24. Дзьобань О. П. До проблеми загроз інформаційній безпеці України: цивілізаційний контекст. Побудова інформаційного суспільства: ресурси і технології: матеріали XVIII Міжнародної науково-практичної конференції (Київ, 19–20 верес. 2019 р.). Київ: УкрІНТЕІ, 2019. С. 173–176.

25. Хімей В. Основні сучасні проблеми інформаційної безпеки України. Теле- та радіожурналістика. 2014. Вип. 13. С. 127–132

26. Архипова Є.О. Механізми управління свідомістю людини в інформаційному суспільстві Мультиверсум. Філософський альманах / Гол. ред. В.В. Лях. Вип. 4(92). 2010. С. 3–13

27. Потятиник Б.В. Патогенний текст у масовій комунікації: ідентифікація, типологія, нейтралізація / Б.В. Потятиник. – Львів, 1996. – 349 с.

28. Дмитрієва К. Україна - НАТО: співробітництво в галузі безпеки інформації [Електронний ресурс]. – Режим доступу: http//www.lntersecurity.jrg/arhivst26.html.

29. Закон України „Про національну програму інформатизації" від 4 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України. - 1998. - № 27-28. - ст. 181.

30. Співробітництво Україна-ЄС-НАТО з протидії гібридним загрозам у кібер-сфері [Електронний ресурс]. – Режим доступу: https://geostrategy.org.ua/ua/analitika/item/1565-cooperation-ukraine-nato

31. Українські спеціалісти з кібербезпеки змогли заблокувати близько 400 кібератак у 2018 році. [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/rubric-technology/2638599-v-ukraini-torik-zablokuvali-majze-cotiri-sotni-kiberatak.html

32. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/96/2016/ed20180509

33. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19

34. Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту. [Електронний ресурс] – Режим доступу: http://domarev.kiev.ua

35. Пєвцов Г.В. Концептуальні підходи щодо забезпечення інформаційної безпеки у воєнній сфері / Г.В. Пєвцов, С.В. Залкін, А.О. Феклістов // Системи обробки інформації. – 2011. – Вип. 2 (92). – С. 57-59.

36. Власюк О.С. Можливості застосування аналітичного планування для обґрунтування та підготовки рішень на вищих рівнях управління. НІСД. – Вип. 47, серія наукові доповіді, 1996. – 71 с

37. Северина С.В. Інформаційна безпека та методи захисту інформації // Вісник Запорізького національного університету №1(29) 2016

38. Семенченко А.І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України: моногр. / А.І. Семенченко. – К.: Вид-во НАДУ, 2008. – 428 с

39. Бачило И. Л. Информационное право [Текст] : учебник / И. Л. Бачило, В. Н. Лопатин, М. А. Федотов, под ред. Б. Н. Топорнина. – СПб. :Юридический Центр Пресе, 2001. – 789с.

40. Гурковський В. Організаційно-правові засади забезпечення інформаційно-психологічної безпеки в контексті дослідження функціонування традиційних і конвергентних медіа // Збірник наукових праць. – 2014. – Вип. 40 “Ефективність державного управління”

41. До проблеми забезпечення інформаційної безпеки України / В. Остроухов, В. Петрик // Політичний менеджмент. — 2008. — № 4(31). — С. 135-141.

42. Северина С.В Інформаційна безпека та методи захисту інформації // Вісник Запорізького національного університету № 1 (29), 2016

Київський національний торговельно-економічний університет
Кафедра публічного управління та адміністрування

РЕФЕРАТ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на тему:

«ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Студента 4 курсу 12 групи спеціальності 074 «Публічне управління та адміністрування», спеціалізації «Публічне управління та адміністрування» _____ Писаревський Артем Петрович

Науковий керівник : кандидат економічних наук, доцент _____ Сонько Юлія Анатоліївна

Гарант освітньої програми: Кандидат економічних наук, доцент _____ Головня Юлія Ігорівна

Київ 2020

РЕФЕРАТ

випускної кваліфікаційної роботи, виконаної на тему:

«Державна політика у сфері інформаційної безпеки»

Структура роботи. Випускна кваліфікаційна робота складається зі вступу, 2-х розділів, висновків і пропозицій списку використаних джерел. Основний текст роботи становить 27 сторінок, в т.ч. 1 таблицю, 4 рисунка. Список використаних джерел містить 42 найменування, викладене на 4 сторінках.

Об'єктом дослідження виступає процес реалізації державної політики у сфері інформаційної безпеки.

Предметом дослідження є теоретико-методичні та прикладні засади державного управління у сфері інформаційної політики.

Зазначена мета вимагає вирішити наступні **завдання**:

- проаналізувати теоретичні засади дослідження інформаційної безпеки в Україні;
- Проаналізувати органи державної влади в системі забезпечення інформаційної безпеки;
- Дослідити ключові загрози інформаційній безпеці в сучасних умовах;
- Проаналізувати напрями ефективної співпраці держав в контексті забезпечення безпеки глобального інформаційного простору;
- Дослідити заходи щодо посилення інформаційної безпеки в Україні.

Одержані результати можуть бути використані в практичній діяльності державних органів які реалізують державну політику у сфері інформаційної безпеки.

Рік виконання роботи 2019– 2020 рр.

Рік захисту роботи – 2020

Анотація
випускної кваліфікаційної роботи, виконаної на тему:
«Державна політика у сфері інформаційної безпеки»

Випускна кваліфікаційна робота присвячена дослідженню діяльності органів які реалізують державну політику у сфері інформаційної безпеки. В роботі обґрунтовано практичні рекомендацій щодо вдосконалення державної політики у сфері інформаційної безпеки.

Досліджено напрями підвищення ефективності державної політики у сфері інформаційної безпеки, проблеми забезпечення державного управління у сфері інформаційної безпеки, проаналізовано особливості інформаційної безпеки в сучасних умовах. На цій основі розроблено практичні рекомендації щодо збільшення ефективності державної політики у сфері інформаційної безпеки.

Ключові слова: Державна політика, інформаційна безпека, рекомендації.

Annotation
final qualifying paper performed on the theme:
« State policy in the field of information security »

The final qualifying work is devoted to the study of the activities of state agencies that implement state policy in the field of information security. The paper substantiates practical recommendations for improving state policy in the field of information security.

The directions of increase of efficiency of the state policy in the field of information security, problems of maintenance of the state management in the field of information security are investigated, features of information security in modern conditions are analyzed. On this basis, practical recommendations have been developed to increase the effectiveness of state policy in the field of information security.

Key words: State policy, information security, recommendations.

РЕЦЕНЗІЯ

на випускну кваліфікаційну роботу
студена Писаревського Артема Петровича
4 курсу 12 групи денної форми навчання
спеціальності 281 «Публічне управління та адміністрування»
на тему «Державна політика у сфері інформаційної безпеки»

Випускна кваліфікаційна робота виконана на тему, яка є актуальною для сфери інформаційної безпеки в сучасних умовах розвитку інформаційних технологій, передбачає виявлення основних небезпек, пов'язаних із розвитком інформаційної безпеки в Україні. Виконана робота за змістом відповідає завданню в повному обсязі. Студент продемонстрував достатній рівень володіння теоретичним матеріалом щодо обґрунтування теоретичних та аналітичних даних щодо державної політики у сфері інформаційної безпеки та вміння застосовувати цей матеріал у процесі реального дослідження.

Робота розкриває сучасний стан державної політики у сфері інформаційної безпеки в Україні. В роботі проаналізовано інформаційну безпеку як основу національної безпеки, проаналізовано органи державної влади в системі забезпечення інформаційної безпеки. Досліджено ключові загрози інформаційній безпеці в сучасних умовах, проаналізовано напрями ефективної співпраці держав в контексті забезпечення безпеки глобального інформаційного простору, досліджено та запропоновано заходи щодо посилення інформаційної безпеки Україні.

Якість оформлення випускної кваліфікаційної роботи можна вважати задовільною. Основні вимоги щодо оформлення матеріалу враховані. Слід відзначити деякі несуттєві порушення стилю викладення матеріалу, який в окремих місцях роботи є ненауковим. В цілому матеріал роботи викладено послідовно і логічно.

Випускна кваліфікаційна робота рекомендується до захисту.

Рецензент
Керівник апарату
Дарницької районної в місті Києві
державної адміністрації
Доцент, кандидат економічних наук _____ Микола КАЛАШНИК

ДАРНИЦЬКА РАЙОННА В МІСТІ КИЄВІ ДЕРЖАВНА АДМІНІСТРАЦІЯ
ЄДРПОУ 37388777
УКРАЇНА

Завідувачу кафедри публічного
управління та адміністрування
Новіковій Н.Л.

Заява

Я, Писаревський Артем Петрович (ПІБ), повідомляю, що за результатами проведення самостійної перевірки з використанням програмно-технічних засобів у наданій випускній кваліфікаційній роботі на тему: **« Державна політика у сфері інформаційної безпеки »** не міститься елементів академічного плагіату. У випадках використання прямих запозичень з друкованих та електронних джерел, вказані відповідні посилання.

Робота для перевірки надається у друкованому та електронному варіантах. Електронна версія моєї роботи ідентична з друкованою.

« 8 » червень 2020 року _____ (підпис)

Оригинальность	Заимствования	Цитирования	Самоцитирования
91,81%	8,19%	0%	0%

Полный отчет | Краткий отчет | История отчетов

РАСПЕЧАТАТЬ | ВЫГРУЗИТЬ | СОЗДАТЬ ССЫЛКУ

Свойства документа

Параметры проверки

Статистика по документу

Имя исходного файла	ЗМІСТ.txt	
Авторы документа	Не указано	Не указано
Название документа	ЗМІСТ.txt	
Тип документа	Не указано	

РЕДАКТИРОВАТЬ СВОЙСТВА

AntiPlagiarism.NET

Файл Правка Вид Операции Дополнительно Справка

Etxt.ru - биржа контента

Стандартная Экспресс Глубокая На рерайт Пакетная проверка Проверка сайта SEO проверка Проверка картинок

Проверить уникальность

Игнорировать домены:

Редактор Адрес: http:// Страница

Текст(53770):

;Обмін технологіями
;Встановлення нових та підтримка існуючих зв'язків;Спільна діяльність України та НАТО у відповідності до програми "Партнерство заради миру" заснована на принципах інформаційної безпеки в умовах вільного обміну важливими даними. Це потрібно для збільшення прозорості планування оборонних бюджетів держав, відкритості даних про стан збройних сил, планування змін у військовій сфері задля збереження миру. Зважаючи на важливість цієї стратегічної інформації та великі ризики при несанкціонованому доступі, кожна з країн-учасниць "Партнерства заради миру" повинна бути впевненою, що інша сторона має технічну можливість забезпечити збереження секретних даних, які передаються.[27,28].
Міжнародне співробітництво у сфері інформаційної безпеки має наступні напрямки:
Недопущення відкритого доступу до секретної інформації, яка стосується забезпечення міжнародної торгівлі, фінансових операцій, правоохоронної діяльності в тому числі боротьби з тероризмом, поширенням наркотичних речовин, організованими злочинними групами.
Запобігання створенню та введенню в дію інструментів інформаційної війни.
Створення безпечних умов для вільного обміну інформацією між країнами із застосуванням державних каналів зв'язку та телекомунікації.
Спільна діяльність правоохоронців країн-учасниць світової спільноти для запобігання кіберзлочинності.
Беручи за зразок країни Європейського Союзу та зокрема НАТО, Україна розбудовує власну структуру забезпечення інформаційної безпеки як таку, що постійно захищає комп'ютерні мережі від можливих кібератак, а також ефективно протидіє кіберзлочинності. Такий підхід є доцільним, адже завдяки йому за 2018 рік було попереджено понад чотириста атак на комп'ютерні мережі стратегічного значення [30].У 2016 році в Україні була затверджена державна Стратегія кібербезпеки. Відтак, цей документ є першочерговим джерелом для планування будь-яких заходів з дотримання інформаційної безпеки. Зокрема Стратегією передбачено поетапний перехід до стандартів кібербезпеки Європейського Союзу та блоку НАТО, а також постійне співробітництво з ними у цьому напрямку. Стосовно військового сектору, Україна повністю переймає досвід НАТО у дотриманні правил кібербезпеки, а також використовує інформаційний простір у якості сфери здійснення операцій [29,31].На законодавчому рівні, зокрема у Законі України "Про основні засади забезпечення

Журнал: Автопрокрутка Очистить журнал

[16:30:03] Уникальность текста 88%© (Проигнорировано подстановок: 0%)

Готово