

111
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Факультет психології, політології та соціології

Кафедра політичних теорій

Бакалаврська робота

на тему:

«Кібербезпека в сучасному політичному світі: проблеми та перспективи»

Виконала: здобувачка 4 курсу
Галузь знань 05 «Соціальні та поведінкові
науки»

спеціальність 052 «Політологія»

Куліков Даниїл Володимирович

Керівник:

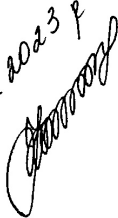
доктор політичних наук, професор

Мамонтова Елла Вікторівна

Рецензент:

Кандидат історичних наук, доцент

Сушко Анатолій Іванович

Закінчено
на «дог»
05.06.2023 р.


Одеса – 2023

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. КІБЕРБЕЗПЕКА ЯК СИСТЕМА. МЕТОДОЛОГІЧНИЙ АСПЕКТ	5
РОЗДІЛ 2. АНАЛІЗ КІБЕРБЕЗПЕКИ У ПОЛІТИЧНОМУ ПРОСТОРІ	27
РОЗДІЛ 3. КІБЕРБЕЗПЕКА В ПОЛІТИЧНОМУ РОЗВИТКУ УКРАЇНИ	32
ВИСНОВКИ.....	40
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	43

ВСТУП

Актуальність теми кваліфікаційної роботи обумовлена суттєвими зрушеннями у інформаційному просторі на глобальному рівні. Розвиток мережі інтернет утворив ситуацію, коли майже вся інформація про індивіда, а тим більше, політичних та громадських діячів, знаходиться в мережі. Ба більше, публічна інформація стає об'єктом кібератак. Органи публічної влади (державної влади та місцевого самоврядування) у глобальному вимірі постійно потерпають від хакерських атак, які здатні паралізувати систему управління на глобальному, національному та регіональному рівнях.

В Україні проблема забезпечення кібербезпеки набуває особливої актуальності у зв'язку із широкомасштабною збройною агресією росії проти нашої держави. Задля перемоги необхідно особливу увагу приділити питанням кібербезпеки. В умовах війни це складне завдання, яке потребує міждисциплінарного синтезу – урахування здобутків природничих та соціальних наук. З точки зору політичної науки питання національної безпеки неможливо забезпечити без урахування такої важливої складової як кібербезпека.

Усе вищезазначене свідчить про особливу актуальність обраної теми кваліфікаційної роботи.

До проблеми кібербезпеки, як складової інформаційної безпеки у глобальному контексті та на національному рівні, з точки зору права, теорії соціальних мереж, соціології, політичної науки звертались багато науковців. Особливо слід відзначити праці таких вчених, як Баранов О.А., Беззубов Д.О., Войcich Н.М., Голобуцький, О. Дзьобань О.П., Завгородня Ю.В., Ставицька О.В., Ліпкан В.А., Медвідь Ф.М., Димарчук О.Л., Б. Кормич, Курчина Т.О., Остапишин П.П., Петрик В. Р., Калюжний В., Гавловський В., Цимбалюк М., В.П. Андрущенко, Почепцов Г.Г., Ю.С. Шемшученко, І.С. Чиж, Романюк Б.В., Тащишин І., Тимченко Л.Д., Третьякова В.Г., Цимбалюк В.С., Шатрава С.О. та ін.

Мета і завдання кваліфікаційної бакалаврської роботи. Метою роботи є дослідження кібербезпеки у сучасному політичному світі, визначення її проблем та перспектив. Поставлена мета обумовила наступні завдання дослідження:

- Визначити кібербезпеку як систему;
- Проаналізувати кібербезпеку у політичному просторі, її різних аспектів (соціального, психологічного тощо);
- Дослідити кібербезпеку в політичному розвитку України.

Об'єктом кваліфікаційної роботи є кібербезпека як складова інформаційної безпеки. Предметом роботи виступає кібербезпека у сучасному політичному світі, її проблеми та перспективи.

Методи дослідження. Для розуміння проблеми кібербезпеки важливим є застосування методів політичної науки. Усі методи, що використовує політична наука задля дослідження кібербезпеки можна поділити на три групи: загальні методи дослідження кібербезпеки, загально-логічні методи, методи емпіричних досліджень дослідження кібербезпеки. Серед загальних методів, які використовувались у дослідженні проблем та перспектив кібербезпеки слід відзначити соціологічний метод, системний метод, культурологічний метод (визначається залежність процесу забезпечення кібербезпеки від рівня політичної культури користувачів), нормативно-ціннісний (з'ясовано значення забезпечення кібербезпеки для суспільства та особистості), структурно-функціональний (для визначення зв'язку між рівнем економічного розвитку та кібербезпеки у різних країнах, та функцій різних органів влади щодо забезпечення кібербезпеки). До спеціальних методів політичної науки, які використовувались у кваліфікаційній роботі належить інституційний метод.

Структура роботи. Кваліфікаційна робота складається із вступу, трьох розділів основної частини, висновків та списку використаних джерел.

РОЗДІЛ 1. КІБЕРБЕЗПЕКА ЯК СИСТЕМА. МЕТОДОЛОГІЧНИЙ АСПЕКТ

У сучасному світі інформації кібербезпека займає важливе місце в наукових дослідженнях, які стають все активнішими з кожним роком. Останнім часом багато уваги приділяється кібербезпеці та її різним аспектам з боку дослідників. Однак, проблема осмислення цього явища залишається відкритою, що є логічним і необхідним, враховуючи швидкий розвиток суспільних відносин у цифровій сфері. Це пояснюється зростанням можливостей інформаційного впливу на суспільство, що створює нові загрози громадській безпеці та потребу у поліпшенні системи захисту. Крім того, саме поняття кібербезпеки потребує глибокого переосмислення через швидкі зміни в сутності інформації та домінуючі тенденції у світовому співтоваристві, яке все більше набуває "інформаційний" характер. У зв'язку з цим, масштабні зміни в інформаційній сфері породжують ряд теоретичних і практичних проблем, які потребують уточнення поняття кібербезпеки. Слід розпочати з розуміння ключових понять. Для визначення особливостей розуміння терміна "забезпечення кібербезпеки" корисно зосередитися на самому понятті "забезпечення". У багатьох словниках слово "забезпечення" має подвійне семантичне роз'яснення:

- 1) задовольняти кого, будь-що у якихось потребах, постачаючи щось у достатній кількості;
- 2) гарантувати щось; створювати надійні умови для здійснення будь-чого;
- 3) захищати будь-що від небезпеки, охороняти будь-кого [1, с. 17].

Поряд з цим, А.О. Стрельцов у своїх працях стосовно терміну «забезпечення»: «Забезпечення є сукупністю діяльності по забезпеченню, засобів забезпечення та суб'єктів забезпечення. Діяльність по забезпеченню полягає у наданні допомоги суб'єктам для досягнення поставлених цілей. Засоби забезпечення утворюють сукупність матеріальних, духовних,

фінансових, правових, організаційних і технічних засобів, необхідних для здійснення діяльності по забезпеченню. Суб'єктами забезпечення є індивіди, організації та органи держави, що здійснюють діяльність по забезпеченню» [38, с. 44]. С.І. Ожегов словом «забезпечити» розуміє «зробити щось цілком можливим, дійсним, реально здійсненим» [39, с. 49]. Слід зазначити, що термін "забезпечення" включає в собі всі необхідні компоненти та структурні елементи як сукупну матрицю з її компонентами. В науковій літературі не існує єдиного усталеного розуміння поняття "кібербезпека". Тому є необхідність уточнення цього поняття, що сприятиме осмисленню перспективних змін у сфері кібербезпеки і дозволить більш повно розкрити його зміст, а також надати йому більш широкий та системний характер, що є належним.

Деякі дослідники, зокрема В. Ліпкань, пропонують своє власне трактування поняття «кібербезпеки» як стану захищеності індивіда, держави та суспільства, при якому реалізується інформаційний розвиток у технічному, інтелектуальному, соціально-політичному та морально-етичному аспектах, і при цьому сторонні інформаційні впливи не завдають їм суттєвої шкоди. [17, с. 443]. Варто зауважити, що таке визначення присутнє не тільки в пасивному сенсі «ступінь захищеності», але й активному сенсі «інформаційний розвиток» (морально-етичний, технічний, соціально-політичний, інтелектуальний). Вчені даного напрямку, а саме: Р. Калюжний, В. Гавловський, В. Цимбалюк, М. Гуцалюк з аспекту кібербезпеки трактують захищеність інфраструктури та інформації, яка її захищає від випадкових чи навмисних споглядань природного чи штучного характеру, котрі здатні завдати неприйнятних наслідків суб'єктам інформаційних відносин, насамперед самим власникам та користувачам інформації та підтримуючої інфраструктури [27]. В свою чергу В.М. Петрик роз'яснює кібербезпеку як становище захищеності об'єктів (інформаційно-технічної інфраструктури особистого, держави, суспільства), за допомогою якого досягається нормальне функціонування незважаючи на наявності внутрішніх чи зовнішніх

впливів на інформацію [26, с. 160–161]. Окрім того, О.А. Баранов формує власне визначення кібербезпеки під яким розуміє «стан захищеності життєво важливих інтересів особистості, суспільства й держави, за якого зводиться до мінімуму заподіяння збитків через неповноту, несвоєчасність і недостовірність інформації, через негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації» [1, с. 134]. Системний характер кібербезпеки дозволяє визначити її забезпечення як складний, комплексний вид діяльності.

Згідно з Ліпканем В.А., Максименком Ю.Є. та Желіховським В.М., система забезпечення кібербезпеки включає такі складові:

1. Інформаційно-аналітичні заходи: це включає збір, аналіз та обробку інформації про загрози та вразливості, розробку прогнозів та сценаріїв розвитку кіберзагроз, визначення та оцінку ризиків.
2. Теоретико-методологічні заходи: розробка концептуальних підходів, методологій, стандартів та моделей управління кібербезпекою, а також визначення стратегій та політики безпеки.
3. Адміністративно-правові заходи: встановлення нормативно-правового регулювання в галузі кібербезпеки, визначення обов'язків та відповідальності суб'єктів, забезпечення координації та контролю за діяльністю в цій сфері.
4. Організаційно-управлінські заходи: розробка структури та механізмів управління кібербезпекою, визначення ролей та відповідальності організаційних одиниць, впровадження систем управління ризиками та контролю.
5. Спеціальні заходи: це включає застосування технічних засобів захисту інформації, розробку криптографічних методів та алгоритмів, проведення тестування та аудиту систем безпеки.

Всі ці заходи спрямовані на забезпечення стійкого розвитку об'єктів кібербезпеки, включаючи інформаційну інфраструктуру, яка її підтримує [17, с. 444].

Отже, автор пропонує розуміти в понятті «адміністративно-правове забезпечення кібербезпеки» комплекс попереджувальних дій політичного, юридичного, технологічного, економічного, виявлення і ліквідацію загроз інтересам особи, організаційного характеру, спрямованих на попередження, держави та суспільства в електронній сфері. У інформаційному суспільстві сучасна система забезпечення кібербезпеки України формується та розвивається у відповідності Конституції України та нормативно-правових актів, котрі регламентують суспільні відносини електронної сфери.

Підґрунтя даної системи складають органи, сили і засоби реалізації кібербезпеки, котрі формують комплекс адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, та інших дій, які спрямовані на забезпечення ефективного функціонування системи управління державою. Відповідно до ст. 2 Закону України «Про основи національної безпеки України» основу у напрямку національного захисту України формує Конституція, інші закони України, міжнародні договори, погодженість яких надана Верховною Радою України, а також видана на формування законів інші нормативно-правові акти.

Окремо варто виділити Закони України: «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про доступ до публічної інформації»; Указ Президента України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері кібербезпеки України»; Проект Закону України «Про Концепцію національної інформаційної політики». Згідно ст. 2 Закону України «Про основи національної безпеки України», Стратегія національної безпеки України і

Воєнна доктрина України є документами, обов'язковими для виконання, і основою для розробки конкретних програм за складовими державної політики національної безпеки [34].

Аналізуючи проблеми, пов'язані з кібербезпекою, необхідно враховувати, що кібербезпека є складовою частиною інформаційних технологій. Справді, розвиток і поширення нових інформаційних та телекомунікаційних технологій мають значний вплив на різні сфери функціонування держави. Інформаційні технології стають важливим фактором у формуванні правової науки і політики національної безпеки. Вони можуть сприяти досягненню позитивних результатів у соціальних відносинах, але водночас виникають проблеми, пов'язані з негативним використанням інформаційних технологій.

Деякі з негативних аспектів включають порушення авторських прав, несанкціонований доступ до приватної та секретної інформації, а також кібертероризм, коли обчислювальні машини атакуються зловмисниками з метою завдання шкоди. Ці проблеми ставлять виклик перед національною безпекою, адміністративно-правовим регулюванням інформаційних відносин та кібербезпекою.

Для вирішення цих питань потрібні нові підходи, які базуються на науковому аналізі і призводять до практичних рекомендацій щодо захисту інформаційного простору. Це включає розробку відповідних політик, нормативно-правового регулювання, технічних засобів захисту і впровадження ефективних стратегій кібербезпеки.

В Україні, як і в інших країнах, це є актуальним завданням, оскільки збільшення залежності суспільства від інформаційних технологій вимагає посилення заходів для забезпечення безпеки в цифровому просторі та захисту від кіберзагроз.

У сучасній політико-правовій науці специфіку формування та розвитку інформаційного напрямку суспільної безпеки України в аспекті адміністративного регулювання зі сторони держави досліджують такі відомі

вчені-адміністративісти, як В.А. Ліпкан, В.О. Заросило, О.М. Бандурка, І.С. Братков, О.Г. Мурашин, В.П. Столбовий, В.О. Шамрай, О.В. Копан, та ін. Розгляд питання кібербезпеки України з адміністративно-правового підходу є важливим аспектом. Адміністративно-правове регулювання кібербезпеки включає комплекс заходів законодавчого й адміністративного характеру, спрямованих на забезпечення законності та порядку у сфері інформаційних відносин і захист прав усіх учасників суспільства в цій сфері.

Законодавчий блок складається з ряду законодавчих актів, які гарантують права всіх суб'єктів права на вільний доступ до інформації та визначають права і свободи громадян та інших суб'єктів права в електронній сфері. Ці акти встановлюють норми, що регулюють використання інформації, захист персональних даних, авторських прав і інші аспекти, пов'язані з кібербезпекою.

Адміністративний блок передбачає застосування адміністративних заходів для забезпечення кібербезпеки. Це можуть бути дії органів державної влади щодо моніторингу, контролю та реагування на порушення кібербезпеки, встановлення правил і стандартів безпеки, організація кваліфікованого персоналу та спеціалізованих структур, розробка і впровадження заходів технічного захисту та реагування на кібератаки.

Метою адміністративно-правового регулювання кібербезпеки є забезпечення належного рівня захисту інформаційного простору, прав та свобод усіх учасників суспільства в електронній сфері. Важливо, щоб ці заходи були системними, узгодженими та ефективними, а також враховували міжнародні стандарти та передові практики у галузі кібербезпеки.

До цих нормативних актів слід віднести Конституцію України, Закони України «Про інформацію», «Про основи національної безпеки» та «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [33]. Адміністративний блок визначається наявністю компетенції у відповідних органів державної виконавчої влади, завданням яких є підтримання стану інформаційного захисту суспільства від протиправних і

злочинних посягань. До цих органів виконавчої влади належать загальні органи виконавчої влади, а саме Кабінет Міністрів України, Міністерства та відомства спеціальної компетенції (Міністерство економіки, Міністерство оборони України, Міністерство інформаційної політики тощо) і спеціальні органи виконавчої влади, завданням яких є охорона правопорядку в Україні (Міністерство внутрішніх справ, Служба безпеки України, Державна прикордонна служба України). Окремим блоком у системі розгляду проблеми кібербезпеки в адміністративному аспекті, є науковий блок, який необхідно виокремити, оскільки ця проблематика розглянута в сучасній правовій науці неповно і фрагментарно. Саме відсутність чіткого взаємозв'язку між розв'язанням проблеми кібербезпеки на теоретичному рівні та впровадженням результатів досліджень у життя стає окремою загрозою суспільним відносинам у цій сфері. Адміністративно-правова діяльність України в сфері забезпечення кібербезпеки є активною категорією правового життя, завдання якої — забезпечення наявності відносин в електронній сфері, тобто самого об'єкта охорони. Основний комплекс загроз і небезпек електронній сфері — це наявність суб'єктів та їх вольових дій з метою створення перешкод для функціонування інформаційних і телекомунікаційних мереж у державі. Головною ланкою, яка пов'язує ці компоненти, є наукові розробки в галузі адміністративного захисту інформаційної сфери та вироблення прикладних засад протидії протиправним проявам у цій сфері життєдіяльності держави. Прикладним аспектом розгляду питання кібербезпеки є вироблення методологічних засад забезпечення безпеки інформаційних відносин у системі адміністративної діяльності держави [5]. В галузі кібербезпеки важливо розробити механізми генерації нових рішень, що дозволять адекватно реагувати на погрози кібербезпеки або передбачати нові погрози та вміти їм протистояти. Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання,

поширення та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів [5].

Так, кібербезпека дійсно охоплює захист життєво важливих інтересів людини, суспільства і держави. Це досягається шляхом запобігання шкоді, яка може бути спричинена через різні чинники:

1. Неповнота, невчасність та невірогідність інформації: Кібербезпека включає заходи для забезпечення достовірності, точності та актуальності інформації, що використовується. Це може включати перевірку джерел інформації, використання захисних механізмів для уникнення поширення неправдивої або недостовірної інформації.

2. Негативний інформаційний вплив: Кібербезпека також охоплює заходи для захисту від негативного впливу інформації, яка може шкодити людям, суспільству або державі. Це можуть бути дії спрямовані на запобігання дезінформації, маніпуляцій, кібершантажу, онлайн-шахрайства та інших форм негативного впливу.

3. Негативні наслідки застосування інформаційних технологій: Розвиток інформаційних технологій дозволяє здійснювати широкий спектр дій, але водночас створює нові загрози. Кібербезпека включає заходи для захисту від негативних наслідків використання інформаційних технологій, таких як кібератаки, вразливості програмного забезпечення, крадіжка ідентифікаційних даних та інші.

4. Несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації: Кібербезпека забезпечує захист інформації від несанкціонованого доступу, розповсюдження та використання. Це включає захист конфіденційної інформації, збереження її цілісності та доступність лише авторизованим користувачам.

Усі ці аспекти кібербезпеки важливі для забезпечення безпеки та захисту від потенційних загроз у сфері інформаційних технологій та

інформаційного простору. [5]. У цьому змісті кібербезпека має кілька напрямків:

1. Система заходів, спрямованих на недопущення несанкціонованого доступу до інформації, несанкціонованої її модифікації або порушення цілісності. Цей напрямок часто називають «InformationalSecurity».

2. Захист політичних, державних і громадських інтересів країни, захист загальних моральних цінностей, недопущення закликів до порушення територіальної цілісності, заборона інформації, яка включає ідеї війни, насилля, дискримінації і посягання на права людини.

3. Запобігання розповсюдженню відомостей, що становлять державну таємницю, а також відомостей з обмеженим доступом до інформації закритого типу, що переміщуються через державний кордон [14].

Сьогодні в Україні сформовано певну законодавчу базу функціонування інформаційного простору України. З огляду інформаційного законодавства розуміється комплекс законів, міжнародних договорів і нормативних актів, що регламентують правовідносини в галузі збирання, опрацювання, збереження і використання інформації. Базовим законом у даній сфері відносин є Закон України «Про інформацію» від 2 жовтня 1992 р. У цьому Законі закріплені основні принципи інформаційних відносин. Такими принципами є:

- гарантованість права на інформацію — «Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір» (ст. 34 Конституції України);

- відкритість, доступність інформації, свобода обміну інформацією — «Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе... » (ст. 32 Конституції України), «Закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, мають бути доведені до відома населення...» (ст. 57 Конституції України);

- захищеність особи від втручання в її особисте та сімейне життя — «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України» (ст. 32 Конституції України);

- достовірність і повнота інформації — «Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації» (ст. 32 Конституції України);

- свобода вираження поглядів і переконань — «Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань» (ст. 34 Конституції України);

- правомірність одержання, використання, поширення, зберігання та захисту інформації — «Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір» (ст. 34 Конституції України).

Створення відкритого інформаційного простору в Україні та реалізація конституційного права на свободу одержання інформації вимагають налагодження механізму, який забезпечує доступ до інформації та встановлює прозорі правила і процедури. Цей процес вимагає розвитку відповідного законодавства та практичної реалізації на рівні органів державної влади і місцевого самоврядування.

Нижче наведено деякі ключові аспекти, які можуть бути враховані у правовій основі механізму реалізації конституційного права на свободу одержання інформації:

1. Законодавче закріплення правил та умов доступу: Важливо мати законодавчі норми, які чітко визначають правила, умови та порядок отримання інформації з боку громадян і інституційних структур суспільства. Це може включати механізми запиту на інформацію, процедури розгляду запитів, терміни надання відповідей тощо.

2. Прозорість діяльності державних органів: Державні органи повинні мати зобов'язання надавати інформацію про свою діяльність, прийняті рішення, публікувати офіційні документи та звіти. Це забезпечує прозорість та публічний контроль за діяльністю державних органів.

3. Доступ до державних та недержавних інформаційних ресурсів: Механізм має передбачати прямий доступ до державних і недержавних інформаційних ресурсів, таких як веб-сайти, бази даних, електронні архіви тощо. Це дозволяє громадянам і структурам суспільства отримувати необхідну інформацію безпосередньо.

4. Захист персональних даних та конфіденційності: Правова основа механізму повинна враховувати захист персональних даних громадян і забезпечувати конфіденційність інформації, яка може бути обмежена з певних причин.

5. Механізми оскарження інформаційних відмов: Важливо передбачити процедури оскарження неприйняття рішень щодо доступу до інформації або відмови у наданні інформації. Це дозволяє громадянам та іншим суб'єктам права вести справедливу та ефективну боротьбу за свої права.

Ці аспекти можуть бути включені до законодавчих актів та нормативних документів, що регулюють питання доступу до інформації. При їх практичній реалізації слід забезпечити ефективні механізми контролю та нагляду за дотриманням цих правил усіма суб'єктами, що мають обов'язки надання інформації [2].

Відповідна державна політика проводиться і щодо підтримки розвитку саме інформаційної сфери — сфери засобів масової інформації, сфери науково-технічної інформації, видавничої справи та реклами, сфери статистики, сфери бібліотечної та архівної справи, сфери інформатики та обчислювальної техніки тощо. У такому вигляді ця політика легалізована та легітимізована у законах України: «Про Національну програму інформатизації» [32], «Про Концепцію Національної програми

інформатизації», «Про інформацію» тощо. В Конституції України (ст. 17) чітко закріплено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та кібербезпеки є найважливішими функціями держави, справою всього Українського народу. Сучасне суспільство значним чином здобуває риси інформаційного суспільства, і як результат зростаюча роль інформації в суспільному житті обумовлює необхідність зосередження уваги на проблемах забезпечення кібербезпеки. Дослідження проблеми кібербезпеки, як правило, починається з виявлення кола її суб'єктів. До суб'єктів забезпечення кібербезпеки належать:

- держава, що здійснює свої функції через відповідні органи: – Президент України; – Верховна Рада України; – Кабінет Міністрів України; – Рада національної безпеки і оборони України; – міністерства та інші центральні органи виконавчої влади (Міністерство освіти і науки України, Національний інститут стратегічних досліджень, Міністерство інформаційної політики, Національна Рада України з питань телебачення і радіомовлення; Державний комітет телебачення і радіомовлення, Державне агентство з питань науки, інновацій та інформатизації; – суди загальної юрисдикції; – прокуратура України;

- місцеві державні адміністрації та органи місцевого самоврядування; – Служба безпеки України, Міністерство внутрішніх справ України, Міністерство оборони України, Збройні сили України, а також інші правоохоронні органи та військові формування, утворені відповідно до Законів України;

- громадяни, громадські або інші організації та об'єднання, які мають повноваження щодо забезпечення кібербезпеки відповідно до законодавства (ЗМІ, політичні партії, професійні спілки). Таким чином, система суб'єктів забезпечення кібербезпеки України включає в себе систему суб'єктів, які забезпечують реалізацію державної політики в електронній сфері.

Інтегруючим чинником для діяльності цих суб'єктів має бути спільна мета — забезпечення інформаційного суверенітету України.

Забезпечення кібербезпеки передбачає проведення урівноваженої та збалансованої державної політики в електронній сфері. Ця політика є комплексним явищем, яке включає внутрішньо- та зовнішньополітичні, економічні, технологічні, військові та інші аспекти, і потребує комплексного підходу на основі норм адміністративного права для формування кібербезпеки. З урахуванням загроз, що посилюються, соціально-економічної й суспільно-політичної кризи в Україні, забезпечення кібербезпеки стає особливо актуальним.

Україна переживає трансформацію, яка охоплює гуманітарну сферу і є важливим фактором у відтворенні нації. В таких умовах особливу увагу слід приділити формуванню державної інформаційної політики на основі наукових досліджень у сфері інформації. Кібербезпека є одним з провідних елементів цього процесу. Дослідження виконуються з використанням різних методологічних підходів, включаючи системний, логіко-функціональний, індуктивний, системний аналіз та синтез.

Для оптимізації інформаційного розвитку України та її інтеграції у світовий інформаційний простір, важливим є виокремлення та деталізація складових політики, які забезпечують кібербезпеку. Однак, загальна структура забезпечення кібербезпеки ще потребує більш детального розгляду, що негативно впливає на формування державної інформаційної політики. Покращення правових механізмів забезпечення кібербезпеки повинно стати пріоритетом державної політики України.

З огляду на міждисциплінарний характер кібербезпеки, який охоплює технічні, правові, економічні та психологічні аспекти, системні зв'язки в забезпеченні кібербезпеки є дуже складними та багаторівневими.

Осмислення і врахування особливостей кожної з цих складових сприятиме досягненню комплексного підходу до забезпечення кібербезпеки. Це включає формування тактичних і стратегічних напрямків діяльності в

сфері кібербезпеки, гармонізацію національного законодавства з питань інформації. Все це створює міцні основи для ефективної державної інформаційної політики [37]. Варто відмітити, що в чинному законодавстві недостатньо регулюється механізм управління сферою безпеки, і відсутня чітка регламентація понять і категорій. Закон не визначає статус екологічної, економічної, інформаційної та державної безпеки, а також не встановлює їх співвідношення з поняттям "національна безпека". При аналізі категорії "національна безпека" використовуються два підходи: перший зосереджений на "національних інтересах", а другий пов'язує національну безпеку з системою базових національних цінностей на структурному та функціональному рівнях [29, с. 88–92]. Науковці з галузі адміністративного права визначають національну безпеку через діяльність спеціальних органів, що забезпечують її. Встановлення проблем забезпечення національної безпеки, їх пріоритетів, послідовності та системної реалізації регулюється Стратегією національної безпеки України. Зазначена Стратегія ставить перед собою завдання відновлення територіальної цілісності України та демократичних інститутів на всій її території, а також реінтеграції тимчасово окупованих територій після їх звільнення. Основними цілями Стратегії є:

- мінімізація загроз державному суверенітету та створення умов для відновлення територіальної цілісності України в рамках міжнародно визнаного державного кордону, забезпечення мирного майбутнього України як суверенної, незалежної, демократичної, соціальної та правової держави;
- захист прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального та гуманітарного розвитку, інтеграція України до Європейського Союзу та створення умов для вступу до НАТО є важливими складовими Національної стратегії у сфері прав людини [35].

Україна потребує розробки цілісної, гнучкої та динамічної державної політики кібербезпеки, що враховуватиме багатоаспектність цього явища. Важливо врахувати перспективні тенденції змін у інформаційному просторі, особливості геополітичного становища та економічного стану країни. Ця

політика повинна знайти відображення у суспільній свідомості, а також мати підґрунтя на правовому та концептуально-доктринальному рівнях. Важливим елементом є розробка ефективного інформаційного законодавства, яке має систематизований характер. З наукової точки зору, розуміння кібербезпеки як складного соціально-технічного явища сучасного глобального аналізу передбачає виокремлення дисциплінарних аспектів, таких як політичний, правовий, соціологічний, ідеологічний, психологічний, технічний тощо, всередині широкого підходу до цієї проблематики.

Дослідники Дзьобань та Ставицька встановили, що політика забезпечення кібербезпеки України є невід'ємною складовою національної безпеки країни. Вона включає в себе систему поглядів та практичну діяльність органів державної влади і управління, спрямовану на забезпечення стану кібербезпеки, при якому будь-яка інформаційна загроза не знижує рівня безпеки суб'єктів нижче припустимого, небезпечного рівня високої ймовірності негативного впливу [10, с. 70].

Також важливим аспектом державної політики кібербезпеки є формування національної самосвідомості та національного світогляду на основі національної ідеї. В сучасному етапі розвитку держави, особливо в умовах жорсткого інформаційно-психологічного протистояння між розвинутими країнами, формування національної самосвідомості є надзвичайно важливим. Вплив на свідомість, підсвідомість, ціннісні орієнтації та емоційно-вольову сферу громадян стає об'єктом цього протистояння. Однак, беззаперечним фактом є необхідність виховання українських громадян на основі національної ідеї [10, с. 72].

Захист кібербезпеки має здійснюватися, насамперед, шляхом проведення виваженої та збалансованої політики держави в електронній сфері, яка має три основні вектори: захист інформаційних прав і свобод людини, захист державної безпеки в електронній сфері та захист національного інформаційного ринку, економічних інтересів держави в електронній сфері, національних виробників інформаційної продукції [16].

Основними цілями інформаційної політики України, згідно з дослідниками Дзьобань та Ставицька, є:

1. Захист інформаційного суверенітету держави, зокрема захист національного інформаційного простору та систем формування масової свідомості, в умовах глобалізації та інтернаціоналізації електронних процесів.

2. Забезпечення інформаційної достатності для прийняття рішень державними органами, підприємствами та громадянами.

3. Реалізація конституційних прав і свобод громадян, суспільства та держави щодо доступу до інформації.

Політика кібербезпеки має багатовекторний характер і включає такі складові (вектори):

- Регулювання інформаційних відносин з метою забезпечення національної безпеки, територіальної цілісності та громадського порядку, підтримання законності.

- Регулювання інформаційних відносин з метою забезпечення прав і свобод громадян, здоров'я і моральності.

- Регулювання інформаційних відносин у сфері комерційної інформації.

Законодавець пропонує кілька основних напрямків державної політики з питань національної безпеки в електронній сфері, зокрема:

- Забезпечення інформаційного суверенітету України.

- Удосконалення державного регулювання розвитку інформаційної сфери, створення передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій, що допоможуть заповнити внутрішній та світовий інформаційний простір достовірною інформацією про Україну.

- Активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем та іншими явищами, що загрожують національній безпеці.

- Забезпечення дотримання конституційного права громадян на свободу слова та доступ до інформації, запобігання неправомірного втручання органів влади, дискримінації в електронній сфері та переслідування журналістів за політичні позиції.

- Застосування комплексних заходів для захисту національного інформаційного простору та протидії монополізації інформаційної сфери в Україні.

Правові механізми можуть грати важливу роль у забезпеченні єдності і взаємозв'язку напрямів державної політики з кібербезпеки. Деякі з таких правових механізмів, які можуть бути визначені на законодавчому рівні, включають:

- Чітко сформульовані цілі і завдання державної політики з кібербезпеки. Це дозволяє визначити напрямки дій і конкретні цілі, що слід досягти у цій сфері.

- Забезпечення взаємодії між державними і громадськими інститутами для реалізації міжвідомчих напрямів державної політики з кібербезпеки. Це включає співпрацю, координацію та обмін інформацією між різними суб'єктами, що займаються забезпеченням кібербезпеки.

- Організація системи інформування суб'єктів, які працюють у сфері кібербезпеки, про актуальні проблеми, загрози і небезпеки, а також заходи для їх попередження, нейтралізації та ліквідації наслідків. Це сприяє своєчасному реагуванню та ефективній роботі в цій сфері.

- Забезпечення узгоджених і спрямованих дій суб'єктів, що діють у різних сферах суспільства і держави, для адекватного реагування на виявлені потенційні і реальні загрози і небезпеки. Це означає спільну спрямовану діяльність і координацію зусиль для захисту кіберпростору.

- Забезпечення загальнодержавного керівництва, координації та контролю у сфері кібербезпеки. Це включає узгоджену стратегію, ефективне

керівництво та механізми контролю для забезпечення ефективності та виконання політики з кібербезпеки на рівні держави.

Ці правові механізми можуть допомогти створити систему, що забезпечує єдність і взаємозв'язок напрямів державної політики з кібербезпеки в Україні [18].

Зазначається, що Указом Президента України «Про Міжвідомчу комісію з питань інформаційної політики та кібербезпеки при Раді національної безпеки і оборони України» від 8 лютого 2002 року була створена Міжвідомча комісія з питань інформаційної політики та кібербезпеки при Раді національної безпеки і оборони України. Ця комісія є консультативно-дорадчим органом з такими завданнями:

1. Аналіз стану і можливих загроз національній безпеці України в електронній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики.

2. Аналіз здійснення галузевих програм і виконання заходів, пов'язаних з реалізацією державної політики в електронній сфері з боку міністерств та інших центральних органів виконавчої влади.

3. Розроблення та внесення пропозицій Президентів України та Раді національної безпеки і оборони України щодо:

- Визначення національних інтересів України в електронній сфері, концептуальних підходів до формування державної інформаційної політики та забезпечення кібербезпеки України.

- Здійснення системних заходів, спрямованих на вдосконалення інформаційної політики України, реалізацію державної стратегії розвитку і захисту національного інформаційного простору та входження України у світовий інформаційний простір.

- Удосконалення системи правового та наукового забезпечення кібербезпеки України.

- Розвиток інформаційної інфраструктури держави, модернізація її матеріально-технічної бази та належне фінансове забезпечення.

- Організація та порядок міжвідомчої взаємодії міністерств, інших центральних органів виконавчої влади у сфері забезпечення кібербезпеки.

- Удосконалення системи оперативного інформаційно-аналітичного забезпечення Президента України (включаючи альтернативну інформацію) в сфері національної безпеки і оборони.

Дослідження завдань цього органу дає підстави зробити висновок, що співробітництво в сфері кібербезпеки України забезпечується переважно органами виконавчої влади. Однак, для ефективного координації потрібна така організація, яка б могла об'єднати не лише представників державного апарату, а й недержавні суб'єкти, які забезпечують інформаційну складову національної безпеки. Взаємодія між державним та громадським управлінням є однією з найважливіших умов соціально-економічного розвитку, будівництва держави та забезпечення кібербезпеки особистості, суспільства і держави. Ще одним важливим аспектом, пов'язаним з формуванням і забезпеченням реалізації державної політики кібербезпеки, є визнання забезпечення кібербезпеки як однієї з найважливіших функцій держави [14]. Це передбачає розробку відповідною державними органами політики і правових механізмів для її реалізації у сфері кібербезпеки.

Державні органи відіграють важливу роль у забезпеченні реалізації державної політики кібербезпеки, згідно з їх повноваженнями у відповідних сферах відповідальності. Вони здійснюють організаційне, нормативно-правове, методичне, науково-технологічне, матеріально-технічне та фінансове забезпечення реалізації державної політики кібербезпеки.

З урахуванням сучасного стану кібербезпеки України, важливим стає координація діяльності всіх суб'єктів, які виконують певні функції у цій сфері. Також актуальним є застосування загальнодержавних засобів і заходів державного впливу для ефективного та якісного виконання законів та нормативно-правових актів з питань кібербезпеки.

Відповідно до конституційної правової норми, "Забезпечення кібербезпеки як справи всього українського народу", держава повинна

реалізовувати політичну волю народу, що виражаєся в права народу бути носієм суверенітету та єдиним джерелом влади. Для досягнення цієї мети держава створює необхідну правову основу та організаційну структуру суб'єктів, які виконують відповідні функції. Наприклад, Міністерство інформаційної політики України було створено з метою забезпечення формування та реалізації державної політики кібербезпеки.

Зазначені завдання, які пропонуються для Міністерства інформаційної політики, відображають певні пріоритети і вагомості до його діяльності у сфері кібербезпеки. Наведу краткий опис кожного з цих завдань:

1. Розробка та реалізація єдиної програми кібербезпеки, включно з забезпеченням достовірної інформації для населення: Міністерство повинно мати відповідальність за розробку та впровадження цілісної програми з кібербезпеки, а також забезпечувати доступ до достовірної інформації для населення.

2. Просування України в світі та формування іміджних інструментів: Міністерство має сприяти впровадженню заходів для покращення іміджу України у світі і формування позитивного сприйняття її інформаційного простору.

3. Активне протистояння інформаційній агресії Росії: Міністерство повинно виконувати заходи для протидії дезінформації та інформаційній агресії з боку Росії, зоконичаючи інформаційний простір України.

4. Запобігання зовнішнього впливу на внутрішній інформаційний простір України: Міністерство повинно здійснювати заходи для захисту внутрішнього інформаційного простору від негативного зовнішнього впливу.

5. залучення інвестицій для створення національного інформаційного продукту: Міністерство має сприяти привертанню інвестицій для розвитку національного інформаційного сектору та створення конкурентоспроможного інформаційного продукту.

6. Надання повної та якісної інформації для ухвалення ефективних рішень щодо безпеки країн: Міністерство повинно забезпечувати Раду

реалізовувати політичну волю народу, що впливає з права народу бути носієм суверенітету та єдиним джерелом влади. Для досягнення цієї мети держава створює необхідну правову основу та організаційну структуру суб'єктів, які виконують відповідні функції. Наприклад, Міністерство інформаційної політики України було створено з метою забезпечення формування та реалізації державної політики кібербезпеки.

Зазначені завдання, які пропонуються для Міністерства інформаційної політики, відображають певні пріоритети і вимоги до його діяльності у сфері кібербезпеки. Наведу короткий опис кожного з цих завдань:

1. Розробка та реалізація єдиної програми кібербезпеки, включно з забезпеченням достовірної інформації для населення: Міністерство повинно мати відповідальність за розробку та впровадження цілісної програми з кібербезпеки, а також забезпечувати доступ до достовірної інформації для населення.

2. Просування України в світі та формування іміджевих інструментів: Міністерство має сприяти впровадженню заходів для покращення іміджу України у світі і формування позитивного сприйняття її інформаційного простору.

3. Активне протистояння інформаційній агресії Росії: Міністерство повинно вживати заходів для протидії дезінформації та інформаційній агресії з боку Росії, захищаючи інформаційний простір України.

4. Запобігання зовнішнього впливу на внутрішній інформаційний простір України: Міністерство повинно здійснювати заходи для захисту внутрішнього інформаційного простору від негативного зовнішнього впливу.

5. Залучення інвестицій для створення національного інформаційного продукту: Міністерство має сприяти привертанню інвестицій для розвитку національного інформаційного сектору та створення конкурентоспроможного інформаційного продукту.

6. Надання повної та якісної інформації для ухвалення ефективних рішень щодо безпеки країни: Міністерство повинно забезпечувати Раду

національної безпеки і оборони України, Президента та Кабінет Міністрів якісною інформацією для прийняття ефективних рішень щодо кібербезпеки країни.

7. Формування кадрового резерву для розвитку сфери комунікацій та імплементації міжнародних рішень і стандартів: Міністерство повинно займатися формуванням та розвитком кадрового резерву в галузі комунікацій та забезпечувати впровадження міжнародних рішень і стандартів в цій сфері.

Ці завдання вказують на необхідність активного впливу Міністерства інформаційної політики на формування та розвиток кібербезпеки в Україні, а також на захист національного інформаційного простору від загроз.

Згідно Положення про Міністерство інформаційної політики України, міністерство є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України. Міністерство інформаційної політики України входить до системи органів виконавчої влади і є головним органом у системі центральних органів виконавчої влади із формування стратегії інформаційної політики держави та забезпечення її дотримання у сферах просвітницької діяльності, створення інформаційної продукції, сприяння розвитку засобів масової комунікації, формування і використання національних інформаційних ресурсів, створення умов для розвитку інформаційного суспільства, а також у сфері здійснення державного нагляду (контролю) за діяльністю засобів масової комунікації та поширенням суспільно важливої інформації, незалежно від їх форми власності, в тому числі в питаннях, що стосуються національної безпеки. Основними завданнями Міністерства інформаційної політики України є: забезпечення формування державної політики щодо діяльності засобів масової комунікації, формування стратегії інформаційної політики держави та забезпечення її дотримання, реалізація державної політики у сферах поширення інформації, просвітницької діяльності і використання національних інформаційних ресурсів, створення умов для розвитку інформаційного суспільства, а також у

сфері здійснення державного нагляду (контролю) за діяльністю засобів масової комунікації незалежно від їх підпорядкування і форми власності.

Отже, кібербезпека є однією з основних складових національної безпеки країни. Її забезпечення з використанням якісно сформульованої національної інформаційної політики значно сприяло б досягненню успіху у виконанні завдань в політичній, воєнно-політичній, військовій, економічній, соціальній та інших сферах державної діяльності. Зокрема, впровадження вдалої інформаційної політики може істотно впливати на зниження соціальної напруги та розв'язання зовнішньополітичних й військових конфліктів.

РОЗДІЛ 2. АНАЛІЗ КІБЕРБЕЗПЕКИ У ПОЛІТИЧНОМУ ПРОСТОРІ

Одним з основних пріоритетів в Україні є створення безпечного інформаційного суспільства, орієнтованого на потреби та інтереси людей. Мета цього суспільства полягає в створенні, накопиченні та поширенні інформації і знань, забезпеченні вільного доступу до них і обміну ними. Сучасний розвиток суспільства характеризується все більшою роллю інформаційної сфери, що призводить до залежності національної безпеки від кібербезпеки. Розвиток інформаційних систем та технологій є важливим фактором для економічного зростання, а сфери, які використовують сучасні інформаційні технології, стають все більш прибутковими.

Закон України "Про рекламу" встановлює основні принципи рекламної діяльності в Україні і регулює відносини, пов'язані з виробництвом, поширенням та споживанням реклами. Згідно з законодавством, реклама представляє собою інформацію про особу чи товар, що поширюється в будь-якій формі та способом з метою стимулювання усвідомлення споживачів щодо цієї особи чи товару.

З цього визначення можна зробити висновок, що реклама є одним із видів інформації, яка передає відомості про осіб, предмети, факти, події та явища. Рекламна діяльність і сама реклама в рамках інформаційних правовідносин потребують надійного забезпечення кібербезпеки.

Сьогоднішня реальність полягає в тому, що кожна особа стикається з небаченим раніше обсягом інформації, що впливає на неї за допомогою різних каналів маніпуляції. Ці канали включають ідеологію, іміджмейкінг, передвиборні кампанії, паблікрейшнз (публічні відносини), рекламу, соціокультурне проектування, які є інструментами свідомої маніпуляції [25, с. 368]. У контексті правових відносин, що стосуються безпеки інформації в галузі реклами, важливо забезпечити нормальне (безпечне) функціонування рекламної діяльності та її учасників (рекламодавців, виробників реклами, поширювачів реклами, споживачів реклами) [25, с. 369]. Слід визнати, що

інформаційні відносини в галузі реклами мають свою специфіку як об'єкта безпеки. Наприклад, стаття 41 Конституції України гарантує кожній особі право володіти, користуватися і розпоряджатися своєю власністю, а також результатами своєї інтелектуальної і творчої діяльності. Стаття 54 Конституції України надає громадянам свободу літературної, художньої, наукової і технічної творчості, а також захист інтелектуальної власності, авторських прав, моральних і матеріальних інтересів, пов'язаних з різними формами інтелектуальної діяльності. Зазначені права відносяться до інформаційної сфери за своїм об'єктом, але мають економічний або соціальний характер за своїм змістом.

З розвитком ринкових відносин в Україні збільшилася важлива роль реклами та рекламної діяльності, які займають значно більше місця у повсякденному житті людей. В наш час реклама є головним джерелом інформації про товари і послуги, і, відповідно, вона може бути корисною або може завдати шкоди правам і законним інтересам споживачів і виробників. У сучасних умовах, сфера створення і поширення реклами нерозривно пов'язана з використанням об'єктів авторського права і суміжних прав. Часто авторами реклами виступають не тільки учасники рекламної діяльності, такі як рекламодавці, виробники і розповсюджувачі реклами, але й самі творці реклами. Наразі закон України "Про рекламу" не розглядає виробника реклами як автора і не регулює відносини, що виникають у сфері використання об'єктів авторського права в рекламній діяльності. Таким чином, участь автора відносин, пов'язаних з рекламою, регулюється законодавством про авторське право і суміжні права [39, с. 87]. За останні роки розвиток сучасних технологій сприяє широкому поширенню і використанню об'єктів авторського права. Наприклад, фотографію можна швидко перетворити на комп'ютерний файл за допомогою сканера і використовувати її для створення рекламного плаката для білбордів або публікації у журналах. Проте для законного використання таких матеріалів необхідно мати дозвіл власника авторських прав на фотографію або інший

твір. Крім того, якщо в процесі створення реклами був створений самостійний об'єкт авторського права, автором цього об'єкта буде виробник реклами [39].

Індивідуально-психологічна складова відображає психологію окремої особистості в ролі громадянина, її готовність до здійснення суспільно корисної діяльності, ставлення до влади, співвідношення між власними і суспільними інтересами, а також психологічне здоров'я особи. Інформаційно-психологічна складова відображає вплив інформації на індивідуальну психіку кожного громадянина і соціальну психіку громадських груп, виражаючи те, що будь-яка інформація є психічним явищем, яке може позитивно, нейтрально або негативно впливати на індивідуальну психіку окремих осіб і соціальну психіку суспільства в цілому. Соціально-психологічна складова проявляється у характері спілкування і взаємодії різних соціальних груп, а також у таких явищах, як зайнятість чи безробіття, справедливість чи несправедливість і т. д. Морально-психологічна складова включає моральні принципи функціонування суспільства як мотивацію для поведінки та діяльності його членів, різних соціальних груп, включаючи політичні партії і блоки. У сучасний час думка суспільства стала одним із суттєвих чинників, що впливають на процеси прийняття рішень на різних рівнях соціального та державного управління [18, с. 15].

В контексті інформаційної боротьби об'єктами впливу можуть бути різні суб'єкти і системи. По-перше, це психіка людей, яка є уразливою до інформаційного впливу. По-друге, це інформаційно-технічні системи різних масштабів і призначень, які можуть бути об'єктом атак і зловживань. Також до об'єктів впливу відносять систему формування, поширення і використання інформаційних ресурсів, систему формування суспільної свідомості через пропаганду та засоби масової інформації, систему формування і функціонування громадської думки та систему прийняття рішень.

Умовно об'єкти впливу можна поділити на технічні та соціальні. Технічні об'єкти включають системи управління, зв'язку, фінансово-

економічної діяльності держави тощо. Соціальні об'єкти включають окремих індивідів, групи, суспільство, державу, світове співтовариство. Основними соціальними елементами суспільства є групи і окремі індивіди. Об'єктами небезпечного інформаційного впливу, а отже, кібербезпеки, можуть бути свідомість, підсвідомість, психіка людей, інформаційно-технічні системи різного масштабу та призначення.

Суб'єктами кібербезпеки вважаються органи і структури, що займаються забезпеченням безпеки в цифровому просторі.

Сучасні цифрові технології, такі як теле-, радіо-, відео-, аудіо-, продукція, можуть бути потужним інструментом для прихованого інформаційного впливу на великі маси людей. Такий вплив може призвести до зниження соціальної активності людей і маніпуляції їхньою свідомістю. Крім того, інформаційні впливи можуть спричинити розвиток фізіологічних і органічних порушень у функціонуванні організму, а також призвести до загострення чи появи психосоматичних захворювань [29].

Засоби масової комунікації, такі як преса, телебачення, радіо, Інтернет та інші, можуть використовуватися для пропагандистсько-психологічного впливу, спрямованого на свідомість і підсвідомість людей. Цей вплив має на меті нав'язати бажану систему цінностей, поглядів, інтересів та рішень у важливих сферах життя особистості, суспільства і держави.

Важливою особливістю інформаційно-психологічного впливу на індивідуальну свідомість є те, що людина може не помічати його і не усвідомлювати як загрозу. Мозок (свідомість, мислення) керує поведінкою особи, тому все, що має вплинути на її дії, повинно спочатку пройти через її мислення. Таким чином, інформаційно-психологічний вплив, спрямований на зміну поведінки особистості, має прагнути до відповідних змін у свідомості.

Реклама і розважальна індустрія також впливають на свідомість людей, створюючи і нав'язуючи уявний стиль життя, який може мати негативні наслідки для суспільства. Ще однією загрозою інформаційній безпеці

України є маніпулювання суспільною свідомістю шляхом поширення недостовірної, неповної або неупередженої інформації.

Узагальнено, маніпуляція може мати такі наслідки для руйнування людської свідомості:

1. Безкритичне сприйняття інформації та подій.
2. Некоректне розуміння ситуації.
3. Байдуже ставлення до подій.
4. Спотворення уявлень про події.
5. Інтенсивне споживання інформації.
6. Страх перед інформацією (інфофобія) та інше.

Застосування різноманітних методів маніпулятивного інформаційно-психологічного впливу значно збільшує небезпеку інформаційних загроз, особливо з урахуванням їхнього впливу на суспільну та індивідуальну свідомість.

Негативні технології маніпуляції суспільною свідомістю охоплюють деформації системи масового інформування та поширення дезінформації. Ці явища призводять до потенційних порушень суспільної стабільності, завдають шкоди здоров'ю та життю громадян через пропаганду або агітацію, що спонукають до соціальної, расової, національної або релігійної ненависті і ворожнечі. Ці впливи, будь то свідомі або неусвідомлені, як підтверджує життя, можуть призводити до серйозних порушень психічного та фізичного здоров'я громадян, порушення природних і культурних норм поведінки та зростання ризикових соціальних та особистісних ситуацій.

РОЗДІЛ 3. КІБЕРБЕЗПЕКА В ПОЛІТИЧНОМУ РОЗВИТКУ УКРАЇНИ

У сучасному світі, який характеризується мобільним розвитком глобального інформаційного суспільства та широким застосуванням інформаційно-комунікаційних технологій у всіх сферах життя, особливу вагу набуває проблема кібербезпеки. Ефективне забезпечення кібербезпеки вимагає тісної співпраці з впливовими структурами безпеки на регіональному, трансрегіональному та глобальному рівнях. Держави або групи держав повинні приділяти особливу увагу будівництву ефективних механізмів стабільності для забезпечення власної національної безпеки. Кібербезпека має особливу актуальність для України, оскільки вона приєдналася до глобальної кіберцивілізації, де рівень розвитку інформаційного суспільства визначається науково-технічним прогресом і освоєнням комп'ютерних інформаційних технологій як засобів глобальної телекомунікації.

У контексті розвитку глобального інформаційного суспільства та втілення України в світовий інформаційний простір, велике значення має покращення ефективності адміністративно-правового регулювання кібербезпеки. Особливо це стає актуальним, оскільки в Україні людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються найвищими соціальними цінностями. На науковому рівні основні принципи правових відносин у міжнародній інформаційній діяльності щодо кібербезпеки ще перебувають у стадії формування, включаючи вітчизняну науку. Протягом останнього десятиліття, з метою прискорення інтеграції України в Європейський союз і серед розвинених країн, вітчизняні вчені неодноразово зверталися до проблематики кібербезпеки.

В даний час правовідносини у сфері кібербезпеки досліджують такі вчені, як В. Копилов, І. Бачило, І. Арістова, В. Цимбалюк та ін.

Для досягнення кібербезпеки необхідно збалансувати інформаційні права та свободи різних суб'єктів права з захистом національного

інформаційного суверенітету. Питання кібербезпеки, як і загальна національна безпека, вимагають знаходження балансу між правами і інтересами людини та компетенцією і інтересами державної влади. Цей баланс може бути досягнутий лише шляхом встановлення відповідних правових норм. Врахування міжнародних правових норм є важливим аспектом у визначенні принципів формування та забезпечення функціонування системи кібербезпеки. Основна мета забезпечення кібербезпеки полягає у розумінні цього поняття як важливої складової національної безпеки та системоутворюючого фактору у всіх сферах життєдіяльності людини, суспільства, держави та інших секторів.

Головним принципом державної зовнішньої політики в галузі кібербезпеки повинно бути дотримання Конституції України, яка визначає Україну як суверенну, незалежну, демократичну, соціальну та правову державу. У контексті зовнішньої політики, Україна повинна прагнути захищати свої національні інтереси та безпеку шляхом утримання мирного та взаємовигідного співробітництва з іншими країнами на основі загально визнаних принципів та норм міжнародного права. Участь у міжнародних та регіональних системах кібербезпеки є актуальною необхідністю у сучасному світі.

У контексті інформаційної революції та глобалізаційних інформаційних процесів, захист власної кібербезпеки стає складним завданням для окремої держави. Однак, в умовах війни це стає необхідністю, і на сучасному етапі українська влада успішно забезпечує цей пріоритет. Виклик широкомасштабної збройної агресії вимагає забезпечення кібербезпеки.

Глобалізаційні інформаційні процеси та глобальні комунікаційні системи розширюють межі забезпечення кібербезпеки, вимагаючи участі світових та регіональних спільнот у вирішенні цих проблем. Завдяки відсутності територіальних обмежень у єдиному інформаційному просторі, кібербезпека набуває наднаціонального характеру.

Міжнародна правова регламентація інформаційних відносин має гарантувати баланс інтересів усіх суб'єктів та уникнення домінування однієї світової культури як еталону. Формування глобальної інформаційної системи на основі партнерства і консенсусу щодо загальнолюдських цінностей є важливим аспектом. З іншого боку, відсутність інформаційних кордонів може сприяти розмиванню культур і загальній культурній деградації людства. Тому важливо розуміти нові глобальні інформаційні загрози та відображати їх у збалансованій національній політиці забезпечення кібербезпеки, що дозволить позитивно використовувати потенціал інформаційного суспільства [24].

У даному випадку, кожна держава має відігравати роль у сприянні розвитку інформаційних процесів шляхом створення різних умов у своєму національному інформаційному просторі, таких як економічні, правові, ідеологічні тощо. Останнім часом, українські дослідники з Національного інституту стратегічних досліджень активно працюють над загальнотеоретичними аспектами розвитку інформаційного суспільства в Україні в контексті глобальних інформаційних процесів та формування інформаційної політики. Особлива увага приділяється провідній ролі інформаційних технологій у модернізації суспільства, аналізу процесів становлення та стратегій розвитку інформаційної політики в Україні.

В контексті глобалізації інформаційних систем досліджуються концептуальні засади державної політики України в електронній сфері, висвітлюються поняття "інтереси особистості", "інтереси суспільства" та "інтереси держави" в електронній сфері, аналізується питання кібербезпеки України. Засновуючись на світовому досвіді, описується роль інформаційних технологій як фактора соціальних трансформацій. Враховуючи реалії формування світового інформаційного простору, дослідники приходять до висновку, що електронна сфера поступово стає вирішальним чинником розвитку сучасної країни, особливу вагу приділяючи комп'ютерним мережам, зокрема глобальній мережі "Інтернет".

Вітчизняні дослідники Ф. Медвідь та Р. Буга основним базовим національно-державним інтересом, геополітичним пріоритетом і стратегічним завданням зовнішньополітичного курсу України в умовах глобалізації вбачають її виживання, підвищення життєспроможності та зміцнення як вільної, суверенної, незалежної держави сучасного світу за умов збереження національних цінностей, захисту економічного та політичного суверенітету, власної соціальнокультурної ідентичності, перетворення з об'єкта геополітичних ігор на повноцінний суб'єкт геополітики, тобто на самостійного гравця, який визначає свої цілі і дії на міжнародній арені [21].

У міжнародній практиці національні інформаційні ресурси вважаються суспільним надбанням і культурною спадщиною людства, яку міжнародне співтовариство захищає для задоволення культурних і духовних потреб кожного індивіда. Для забезпечення свого суверенітету держави можуть обмежувати доступ до передачі інформації в інші країни та встановлювати режим обмеженого доступу. Однак, найважливішою ознакою інформаційного суспільства є можливість кожного створювати, отримувати, використовувати та обмінюватися інформацією і знаннями. Основною метою інформаційного суспільства є надання людям можливості реалізувати свій інтелектуальний потенціал, розвивати свої можливості і здібності, сприяючи постійному підвищенню рівня життя. У різних країнах виділяються три основні моделі формування інформаційного суспільства: європейська, американська та азійська [7]. Європейська модель розвитку інформаційного суспільства характеризується активною участю держави та міжнародних інституцій та орієнтацією на соціальні потреби. Органи Європейського Союзу реалізують різноманітні програми, спрямовані на розвиток інформаційного суспільства та створення Єдиного європейського інформаційного простору. Ці програми мають на меті забезпечити права та свободи громадян, розвиток інформаційної інфраструктури, вільний доступ до неї та підвищення рівня інформованості суспільства. Також надаються

пільгові умови для підприємництва в галузі інформаційних технологій. Характерною ознакою європейської моделі інформаційного суспільства є гнучкість політичної спрямованості програм, яка враховує особливості національних контекстів і враховує нову регіональну геополітику, становлення інформаційної (інтелектуальної) економіки держав, інформаційне законодавство та різні можливості постіндустріального розвитку.

Справді, Україна активно працює над формуванням інформаційного суспільства і має пріоритети, спрямовані на побудову відкритого та розвитку орієнтованого на інтереси людей інформаційного суспільства. В країні вже сформовані правові засади для побудови інформаційного суспільства, такі як Закони України "Про Концепцію Національної програми інформатизації" та "Про Національну програму інформатизації" та інші нормативно-правові акти.

Український ринок інформаційно-комунікаційних технологій також перебуває в активному становленні і може стати основою для розвитку інформаційного суспільства в країні.

У сучасних умовах глобалізації інформаційних процесів особлива увага приділяється міжнародній інформаційній діяльності, оскільки вона стає провідним напрямком у формуванні глобального інформаційного суспільства та глобальної інформаційної цивілізації. Кібербезпека також стає важливим аспектом у сучасному глобалізованому світі, оскільки інформаційні ресурси набувають великого значення для країн, які прагнуть досягти інформаційного домінування та захистити свої національні інтереси.

Таким чином, Україна активно розвивається в напрямку інформаційного суспільства і має відповідні правові засади, а також приділяє увагу міжнародній інформаційній діяльності та кібербезпеці.

Кібербезпека розглядається як міжнародна проблема, пов'язана з захистом інформації, інформаційного простору та інформаційного суверенітету. У кожній державі практичні заходи щодо розв'язання проблем

кібербезпеки та притягнення до відповідальності за порушення або загрозу інформаційній безпеці виконуються відповідно до норм міжнародного права, міждержавних договорів та внутрішнього законодавства. Кібербезпека регулюється нормами міжнародного права, які містяться в документах ООН і ЮНЕСКО, а також в документах європейських міжнародних організацій та національних нормативних актах. Кожна розвинута країна має власні закони, що стосуються захисту інформації в різних сферах. Наприклад, у Франції існує Закон «Про інформацію, інформаційні файли і права людини», у Німеччині, Австрії, Бельгії, Данії та Ірландії — Закон «Про захист інформації», у Фінляндії та Ісландії — Закон «Про захист інформації про особу», у Люксембурзі — Закон «Про використання інформації в процесі роботи з комп'ютером». Межі національного інформаційного простору визначаються інформаційним суверенітетом держави, який означає здатність держави контролювати та регулювати потоки інформації з-за меж держави з метою дотримання національних законів, прав і свобод громадян, а також забезпечення національної і державної кібербезпеки, як частини загальної міжнародної кібербезпеки.

Захист конституційних прав і свобод людини і громадянина, забезпечення цілісності культурних, історичних, інтелектуальних і матеріальних цінностей суспільства, а також політичної, економічної, соціокультурної, науково-технічної, оборонної і державної безпеки, є головною метою державної політики кібербезпеки. У рамках розвитку інформаційного суспільства в Україні на 2007-2015 роки визначаються основні засади, які передбачають реалізацію через різні механізми.

Один з таких механізмів - планування соціально-економічного розвитку України з урахуванням потреб розвитку інформаційного суспільства і розробка державних програм для ефективного забезпечення завдань розвитку інформаційного суспільства.

Також важливим є забезпечення громадської дискусії з питань формування інформаційного суспільства, щоб залучити громадян до процесу прийняття рішень і виконання стратегій розвитку.

Міжнародна співпраця також має важливе значення, включаючи співпрацю з провідними міжнародними організаціями з розвитку інформаційного суспільства, реалізацію спільних проектів та інтеграцію України в глобальний інформаційний простір.

Координація розробки та реалізації загальнодержавних програм і бізнес-проектів, фінансування цільових програм та створення сприятливих умов для розвитку інноваційних структур з інформаційних технологій також є важливими механізмами.

Загалом, ці механізми спрямовані на забезпечення реалізації Основних засад розвитку інформаційного суспільства, сприяють впровадженню універсального підходу до спільних дій і зменшенню цифрової та інформаційної нерівності.

Реалізація Основних засад розвитку інформаційного суспільства в Україні має потенціал привести до позитивних змін в різних сферах життєдіяльності суспільства і людини. Це означає, що можна досягти наступних результатів: зміцнення захисту прав і свобод людини, поліпшення її добробуту, залучення громадян до активної участі в управлінні державою та підтримка розвитку демократії; підвищення конкурентоспроможності України, ефективності державного управління і продуктивності праці у всіх секторах економіки; підвищення рівня кібербезпеки для людей, суспільства та держави, а також розвиток інформаційно-телекомунікаційної інфраструктури, зокрема українського сегменту Інтернету; сприяння переходу до науково-технічного та інноваційного розвитку економіки, збільшення частки наукоємних продуктів, покращення якості та доступності освіти, науки, культури та охорони здоров'я через впровадження ІКТ; забезпечення широкого доступу людей до національних та світових інформаційних електронних ресурсів; створення нових робочих місць,

поліпшення умов праці та життя людей; і продовження розвитку нормативно-правових засад інформаційного суспільства.

ВИСНОВКИ

Таким чином, дослідивши у даній кваліфікаційній роботі проблеми та перспективи кібербезпеки, слід зробити наступні висновки.

В державній політиці необхідно приділяти особливу увагу безпеці цифрової економіки, і це вимагає виділення проблемного поля, пов'язаного з загрозами національній безпеці та розробкою відповідних механізмів для їх протидії. Незважаючи на еволюційний характер державної політики у галузі кібербезпеки, її темпи розвитку не відповідають сучасним вимогам. Тому нагально потрібно досліджувати шляхи покращення ситуації з питань кіберзахисту. У даній роботі визначено поняття "кіберпростір" та "кібербезпека" з політичної науки. Вони розглядаються в контексті їх взаємозв'язку та ролі у цифровому суспільстві, зокрема в політичній сфері. Це дозволяє відобразити модель національної безпеки з погляду кібербезпеки. Високий рівень розвитку кіберпростору та загрози, пов'язані з кібератаками, свідчать про необхідність зміни парадигми стратегії кібербезпеки. Вона повинна ґрунтуватися на прогнозуванні і плануванні заходів протидії майбутнім діям зловмисників у кіберпросторі, а не тільки на реагуванні на події. Для цього необхідно постійно аналізувати сучасні тенденції у сфері кіберзагроз. У цій роботі виокремлені найактуальніші з них на сьогоднішній день. Підкреслюється, що для успішного протистояння наведеним викликам Україні потрібна нова кіберстратегія. Важливо, щоб шлях, яким Україна розвиває свою кібербезпеку, зазнав належних і термінових змін, і сам процес розвитку був достатньо швидким. У роботі також визначено заходи, які мають бути пріоритетними у цьому напрямку. Результати дослідження свідчать про важливість врахування серйозних проблем, пов'язаних з забезпеченням кібербезпеки, і необхідність розробки та впровадження більш ефективних механізмів для функціонування та забезпечення безпеки кіберпростору в умовах воєнного стану, підвищення надійності основних компонентів глобальної інтернет-мережі та інших ІКТ-

пристроїв, урахування людського фактору та комплексного системного підходу до формування державної політики з кібербезпеки.

Також важливою складовою кібербезпеки, як складової системи національної інформаційної безпеки є усвідомлення на індивідуальному рівні загроз та кроків щодо їх недопущення та подолання кожним із громадян України. Адже на рівні індивідуальних користувачів можна подолати більшість проблем та запобігти їх подальшому розповсюдженню. Користувачі мережі Інтернет регулярно стають жертвами хакерів, в результаті чого втрачають свої кошти та стикаються із викраденням персональних даних. У багатьох випадках хакери використовують необачність чи недотримання користувачами елементарних правил особистої безпеки в Інтернеті. Як наслідок, навіть захисне програмне забезпечення не здатне вберегти користувача, якщо він своїми діями привертає увагу кіберзлочинців. Розглянемо детальніше типові помилки користувачів Інтернету, які роблять їх вразливими до кібератак: встановлення елементарних чи слабких паролів, для зламу яких хакерам достатньо перевірити декілька найпоширеніших комбінацій. Наприклад, встановлення паролю, який складається із послідовності чисел або дати народження користувача, є типовою помилкою; нехтування двофакторною автентифікацією; використання неперевірених мереж Wi-Fi у публічних місцях; введення персональних даних на незахищених та неперевірених вебсайтах; відкриття файлів, прикріплених до підозрілих електронних листів чи повідомлень; неуважність при перевірці веб-сайту на справжність; використання єдиного або схожих паролів для усіх облікових записів; збереження паролів у браузері; розголошення користувачами надмірної кількості особистої інформації у соціальних мережах; хибні упередження щодо власної захищеності у мережі тощо.

Кожен користувач Інтернету не може повністю захистити себе від всіх можливих кіберзагроз. Однак, дотримуючись основних правил безпеки в Інтернеті, користувачі можуть суттєво зменшити ризики для своєї безпеки.

Для кожного облікового запису рекомендується використовувати унікальні та надійні паролі, і не повідомляти їх стороннім особам, а також утримуватись від зберігання їх у браузері. Крім того, навіть надійні паролі слід регулярно змінювати. У випадку потреби використання багатьох паролів, рекомендується встановлювати спеціальні програми для керування паролями.

Взагалі, дотримання користувачами основних правил безпеки в Інтернеті зробить їх менш привабливими цілями для кіберзлочинців. Насправді, хакери діють за принципом найменшого опору, тому виконання користувачами правил безпеки в Інтернеті є передовим кроком у превентивній боротьбі з кіберзлочинцями для забезпечення цифрової безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Баранов О.А. Інформаційне право України : стан, проблеми, перспективи / О.А. Баранов. — К. : ВД «СофтПрес», 2005. — 316 с.
2. Беззубов Д.О. Суспільна безпека (організаційно-правові засади забезпечення): монографія / Д.О. Беззубов. — Київ : «МП Леся», 2013. — 425 с.
3. Бесчастний В. Міжнародний досвід у діяльності міліції України // Віче. Грудень, 2009. — № 24. URL : <http://veche.kiev.ua/joLima/1780/7feed> (дата звернення: 06.03.2018).
5. В Україні найближчим часом з'явиться доктрина кібербезпеки http://na.mil.gov.ua/25677-v-ukra%D1%97ni-najbli_zhchim-chasom-zyavitsya-doktrina-informacijno%D1%97-b_ezpeki.
6. Войцях Н.М. Державна політика в українському інформаційному просторі: стан та проблеми [Електронний ресурс] / Н. Войцях // Режим доступу : http://www.ijimv.knukim.edu.ua/zbirnyk/1_2/2-vojzih.pdf.
7. Голобуцький, О. «Електронний уряд» / О. Голобуцький, О. Шевчук. — [Електронний ресурс] — Режим доступу : <http://golob.narod.ru/egovper.html>.
8. Давидов П. Освіта України в контексті світових цивілізаційних конфліктів. // П. Давидов / Всеукраїнська науково-практична конференція з міжнародною участю 14–15 травня 2015 р. Модернізація соціогуманітарного простору: історичний досвід, виклики та перспективи. Збір матеріалів. — Житомир–Вінниця. — С. 95–99.
10. Дзьобань О.П., Ставицька О.В. Деприваційний стан суспільства і питання національної безпеки // О.П. Дзьобань, О.В. Ставицька / Психологічні аспекти національної безпеки: Тези Другої Міжнародної науково-практичної конференції. — Львів : Львівський державний університет внутрішніх справ, 2008. — С. 70–75.

11. Жуков В. Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение. — 2001. — № 1. — С. 2–9.

12. Калюжний Р.А. Інформаційне забезпечення управлінської діяльності в умовах інформатизації : організаційно-правові питання теорії і практики : підручник для студ. вищ. навч. закл. / Р.А. Калюжний, В.О. Шамрай, М.Я. Швець та ін. ; за ред. Р.А. Калюжного та В.О. Шамрая. — К. : Академія державно-податкової служби України, 2002. — 296 с.

13. Колесник О.С. Поет та відтворення архетипу у міфопоетичному світовідношенні / О.С. Колесник // Актуальні філософські та культурологічні проблеми сучасності : 36. наук. праць. — Київ, 2000. — С. 124.

14. Концепція соціального контролю в сучасній теоретико-правовій науці / В. М. Пальченкова // Юридична наука. — 2015 — № 8 — С. 7–14 — Режим доступу : http://nbuv.gov.ua/UJRN/jnn_2015_8_3j.

15. Корупційні практики в Україні : сприйняття vs реальний досвід громадян [Електронний ресурс]. — Режим доступу : <https://www.vopora.ua/org/novyny/41958-korupts-iini-praktiky-v-ukraini-spryiniattia-vs-reahiyi-dosvid-hromadian>.

16. Корупційні ризики в діяльності державних службовців : роз'яснення міністерства юстиції України від 12.04.2011 р. [Електронний ресурс]. — Режим доступу : <http://zakon5.rada.gov.ua/laws/show/n0026323-11j>.

17. Ліпкан В.А. Кібербезпека як складована національної безпеки України / В.А. Ліпкан // Інформаційні технології в економіці, менеджменті і бізнесі : Проблеми науки, практики і освіти : 36. наук. праць VIII Міжнар. наук.-практ. конф. — Ч. 2. — К. : Вид-во Європ. ун-ту, 2003. — С. 443–453.

18. Лісовський П.М. Феномен маніпуляції свідомістю : сутність, структура, механізм у сучасному суспільстві (соціально-філософський аналіз) [Текст] : дис. ... канд. філос. наук : 09.00.03 / Лісовський Петро Миколайович ; Укр. держ. ун-т фінансів та міжнар. торгівлі. — К., 2009. — 191 с.

19. Логунов А.Б. Региональная и национальная безопасность : Учебное пособие / А.Б. Логунов. - Вузовский учебник, 2009. — 432 с.

21. Медвідь Ф.М., Димарчук О.Л., Курчина Т.О. Глобалізація засобів масової інформації: концептуальні засади // Наукові праці МАУП / Редкол. : А.М. Подоляка (гол. Ред.) [та ін.]. — Вип. 4(31). — Київ : ДП «Видавничий дім «Персонал», 2011. — С. 88–92.

22. Мельник М.І. Корупція: сутність, поняття, заходи протидії : монографія / М.І. Мельник. — К. : Атіка, 2001. — С. 145.].

24. Окинавська хартія глобального інформаційного суспільства (Дата проголошення 22.07.2000) [Електронний ресурс]. — Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=998_163.].

25. Остапишин П.П. Забезпечення кібербезпеки у галузі реклами: методологічні підходи / П.П. Остапишин // Науковий вісник НЛТУ України. — 2003. — Вип. 23.7. — Ст. 368–372.

26. Петрик В. Щодо визначення кібербезпеки та її різновидів / В. Петрик // Форми та методи забезпечення кібербезпеки держави : зб. матер. міжнар. наук.-практ. конф. (м. Київ, 13 березня 2008 р.). — К. : Видавець Захаренко В.О., 2008. — 216 с.

27. Питання концепції реформування інформаційного законодавства України / Р. Каложний, В. Гавловський, В. Цимбалюк, М. Гуцалюк // Збірник «Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні». К. : НТУУ «КПІ», Міністерство освіти і науки України, СБУ. — К. — 2000. — С. 17–21.

28. Політологія : підручник / І.С. Дзюбка, К.М. Левківський, В.П. Андрущенко та інші ; за заг. ред. І.С. Дзюбка, К.М. Левківського. — 2-е вид., випр. і допов. — К. : Вища школа, 2001. — 415 с.

29. Почепцов Г.Г. Национальная безопасность стран переходного периода. — К, 1996. — 136 с.

30. Правове забезпечення інформаційної діяльності в Україні / за заг. ред. Ю.С. Шемшученка, І.С. Чижа. — К. : ТОВ «Юридична думка», 2006. — 384 с.

31. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII // Відом. Верхов. Ради України. — 2015. — № 40–41. — Ст. 379.

32. Про національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98 // Відомості Верховної Ради України. — 1998 / — № 27–28. — Ст. 181.

33. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9 січ. 2007 р. № 537-V // Відом. Верховної Ради України. — 2007. — № 12. — Ст. 102.

34. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про стратегію національної безпеки України» : Указ Президента України від 26 травня 2015 року, № 287/2015. Офіційний вісник України від 09.06.2015. — 2015. — № 43. — Ст. 1353.

35. Проект Національної стратегії у сфері прав людини станом на 25 березня 2019 року (українською мовою) [Електронний ресурс]. — Режим доступу : <http://old.minjust.gov.ua/file/44709>.

36. Пундей Сар Дж. Боротьба з корупцією. Критичний огляд з аналізом міжнародного досвіду // Матеріали українсько-американського семінару «Проблеми економічного зростання: питання доброчесності». — Львів, 1997, С. 17.

37. Романюк Б.В. У боротьбі з організованою злочинністю та корупцією важливі конкретні дії // Боротьба з організованою злочинністю і корупцією (теорія і практика). — К. : 2004. — № 9. — С. 517.

38. Стрельцов А.А. Обеспечение информационной безопасности. Теоретические и методологические основы / А.А. Стрельцов ; [ред. В.А. Садовничий, В.П. Шерстюк]., 2002. — 296 с.

39. Сухарев Е.Е. Авторское право в издательском бизнесе и СМИ. Практическое пособие / М.А. Невская, Е.Е. Сухарев, Е.Н. Тарасова. — Изд-во Дашков и К., 2009. — 300 с.

40. Тацишин І. Адміністративно-правове закріплення безпеки інформаційних відносин у галузі реклами / І. Тацишин // Вісник Львівського університету. Серія юридична / М-во освіти і науки України, Львів. нац. ун-т 266 ім. І. Франка ; [редкол. : В.Т. Нор (відп. ред.) та ін.]. — Л., 2008. — Вип. 46. — С. 88–91.

41. Тимченко Л.Д. Международное право : учебник / Л.Д. Тимченко. — Х. : Консум, 1999. — 528 с. 167.

42. Третьякова В.Г. Правове регулювання біоетичних проблем у контексті застосування міжнародних та європейських стандартів. — К. : Парламентське вид-во, 2007. — 304 с.

43. Цимбалюк В.С. Інформаційне право (основитеорії і практики) / В.С. Цимбалюк. Монографія. — К. : «Освіта України», 2010. — 388 с.

44. Шатрава С.О. Корупційні ризики в діяльності органів внутрішніх справ: сутність та зміст // Науковий вісник Ужгородського національного університету: Серія Право. Вип. 21. Ч. II. Том 2. С. 268–270.