**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**ЮРИДИЧНИЙ ФАКУЛЬТЕТ**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_конституційного і трудового права \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(повна назва кафедри)

**Кваліфікаційна робота**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_магістра\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(рівень вищої освіти)

на тему\_\_\_\_\_\_\_\_\_\_\_ Інформаційна безпека як складова національної безпеки України в умовах глобалізаційних правових процесів \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Виконав: студент магістратури, групи\_\_\_\_\_\_

спеціальності

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_081 право \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(шифр і назва спеціальності)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ініціали та прізвище)

Керівник \_\_\_\_\_\_\_\_ Журавльова Г.С.,

професор кафедри конституційного та трудового права, д.ю.н.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Рецензент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Запоріжжя – 2019

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

Факультет\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кафедра\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рівень вищої освіти\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Спеціальність \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(шифр і назва)

**ЗАТВЕРДЖУЮ**

Завідувач кафедри\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_року

**З А В Д А Н Н Я**

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(прізвище, ім’я, по батькові)

1. Тема роботи (проекту) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

керівник роботи \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ЗНУ від «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_20\_\_\_року №\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Строк подання роботи \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Вихідні дані до роботи \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Консультанти розділів роботи

|  |  |  |
| --- | --- | --- |
| Розділ | Прізвище, ініціали та посадаконсультанта | Підпис, дата |
| завданнявидав | завданняприйняв |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Дата видачі завдання\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**КАЛЕНДАРНИЙ ПЛАН**

|  |  |  |  |
| --- | --- | --- | --- |
| №з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (ініціали та прізвище)

Керівник роботи (проекту) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (ініціали та прізвище)

**Нормоконтроль пройдено**

Нормоконтролер \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (ініціали та прізвище)

РЕФЕРАТ

Зайцев Д.С. Інформаційна безпека як складова національної безпеки України в умовах глобалізаційних правових процесів. – Запоріжжя, 2020. – 121 с.

Кваліфікаційна робота складається зі 121 сторінок, перелік посилань містить 98 джерел.

В умовах євроінтеграції України, з урахуванням побудови інформаційного суспільства, все більшої актуальності набувають питання правового забезпечення інформаційної безпеки – запобігання й усунення різноманітними засобами і способами загроз людині, суспільству, державі в інформаційній сфері. Однак у сучасному багатогранному та динамічному світі проблеми інформаційної безпеки набувають принципово нових рис, тепер вони виходять далеко за межі запобігання війн і збройних конфліктів. Сьогодні вони стали їх підґрунтям, першоджерелом, основним ресурсом та головною зброєю.

В українських реаліях ці проблеми стали очевидними. У таких умовах стає пріоритетним осмислення сукупності інформаційних процесів у контексті правового забезпечення безпеки України. З огляду на це цілком природним вбачається пошук основоположних цінностей, цілей, інтересів та надбань в інформаційній сфері, які слугуватимуть орієнтирами європейської перспективи України, майбутнього розвитку українського суспільства, заснованої на інформаційних технологіях, закладуть фундамент подальшого розвитку інформаційного права в Україні.

У цьому контексті закономірно зростає роль правових механізмів у забезпеченні інформаційної безпеки України, потреба ефективного законодавчого врегулювання суспільних відносин, що виникають у досліджуваній сфері, визначення правових засад організації та координації дій суб’єктів забезпечення інформаційної безпеки України, розробці пріоритетних напрямів державної політики у сфері інформаційної безпеки. Дослідження інформаційної безпеки України з правничої точки зору пов’язане з формуванням якісної системи інформаційної безпеки, що відповідатиме сучасним вимогам та нагальним потребам України як повноправного члена й надійного партнера європейської спільноти.

Обравши євроінтеграційний курс та визначивши вступ до НАТО своїм стратегічним пріоритетом, Україна має орієнтуватися передусім на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфері. Для нашої держави імплементація європейських стандартів правового забезпечення інформаційної безпеки держави є пріоритетним засобом інтеграції в європейський правовий простір.

*Об’єктом кваліфікаційної роботи* є суспільні відносини, що виникають у сфері інформаційної безпеки.

*Предметом* дослідження інформаційна безпека як складова національної безпеки України в умовах глобалізацій них правових процесів.

*Мета* роботи полягає у тому, щоб на підставі комплексного аналізу наявних наукових та нормативних джерел визначити зміст інформаційної безпеки як складової національної безпеки України.

ДЕРЖАВНА ПОЛІТИКА, ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, НАЦІОНАЛЬНА БЕЗПЕКА, ПРАВОВІ МЕХАНІЗМИ, СУБ’ЄКТИ

SUMMARY

Zaitsev D.S. Information security as a component of national security of Ukraine in the context of globalization legal processes. - Zaporizhia, 2020. - 121 p.

The qualification consists of 121pages, the list of references contains 98 sources.

In the context of Ukraine's European integration, taking into account the construction of the information society, the issues of legal security of information security - prevention and elimination by various means and methods of threats to the person, society, and the state in the information sphere become more and more urgent. However, in today's multifaceted and dynamic world, information security issues are taking on a whole new set of features, now they go far beyond preventing wars and armed conflict. Today, they have become their foundation, primary source, primary resource and primary weapon.

In Ukrainian realities, these problems have become apparent. In such circumstances, it becomes a priority to understand the set of information processes in the context of legal security of Ukraine. In view of this, it is quite natural to search for the fundamental values, goals, interests and assets in the information sphere, which will serve as a guide for the European perspective of Ukraine, the future development of Ukrainian society based on information technologies, will lay the foundation for the further development of information law in Ukraine.

In this context, the role of legal mechanisms in ensuring information security of Ukraine, the need for effective legislative regulation of public relations arising in the research sphere, the definition of legal principles of organization and coordination of actions of subjects of information security of Ukraine, the development of priority directions of state policy in the field of information security. From a legal point of view, the study of information security of Ukraine is connected with the formation of a high-quality information security system that will meet modern requirements and urgent needs of Ukraine as a full member and reliable partner of the European community.

Having chosen a European integration course and identifying NATO as a strategic priority, Ukraine should focus primarily on the development strategy of the EU and NATO member states in the information field. For our country, the implementation of the European standards of legal support for information security of the state is a priority means of integration into the European legal space.

The subject of the qualification is the public relations that arise in the field of information security.

The subject of research is information security as a component of national security of Ukraine in the context of globalization of legal processes.

The purpose of the work is to determine the content of information security as a component of national security of Ukraine on the basis of a comprehensive analysis of available scientific and regulatory sources.

STATE POLICY, INFORMATION SECURITY, INFORMATION SECURITY, INFORMATION SOCIETY, INFORMATION TECHNOLOGY, NATIONAL SECURITY, LEGAL MECHANISMS, ENTITIES

ЗМІСТ

|  |  |
| --- | --- |
| РОЗДІЛ 1 ПОЯСНЮВАЛЬНА ЗАПИСКА………………………………. | 10 |
| РОЗДІЛ 2 ПРАКТИЧНА ЧАСТИНА…………………….……………….. | 74 |
| 2.1. Інформаційна безпека людини інтегральне явище в системі національної безпеки………………………………….……………………. | 74 |
| 2.2. Поняття, ознаки, правовий режим інформаційної безпеки в системі національної безпеки в Україні …………………………………... | 76 |
| 2.3. Особливості правового забезпечення інформаційної безпеки в умовах загроз національній безпеці………………………………………. | 89 |
| 2.4. Особливості забезпечення інформаційної безпеки людини в умовах загроз національній безпеці………………….…………………… | 94 |
| 2.5. Пріоритети вдосконалення правових основ інформаційної безпеки в національній безпеці в умовах реформаційних змін…………. | 102 |
| ВИСНОВКИ………………………………………………………………… | 108 |
| ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ…………………………………. | 112 |

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

|  |  |
| --- | --- |
| ІБ | Інформаційна безпека  |
| ІКТ | Інформаційно-комунікаційні технології  |
| ІЗ | Інформаційна зброя  |
| ІПВ | Інформаційно-психологічний вплив  |
| ЄС | Європейський Союз  |
| СБУ | Служба безпеки України  |
| МО | Міністерство оборони  |
| ЗМІ | Засоби масової інформації  |
| НБ | Національна безпека  |

РОЗДІЛ 1 ПОЯСНЮВАЛЬНА ЗАПИСКА

*Актуальність теми*. В умовах євроінтеграції України, з урахуванням побудови інформаційного суспільства, все більшої актуальності набувають питання правового забезпечення інформаційної безпеки – запобігання й усунення різноманітними засобами і способами загроз людині, суспільству, державі в інформаційній сфері. Однак у сучасному багатогранному та динамічному світі проблеми інформаційної безпеки набувають принципово нових рис, тепер вони виходять далеко за межі запобігання війн і збройних конфліктів. Сьогодні вони стали їх підґрунтям, першоджерелом, основним ресурсом та головною зброєю.

В українських реаліях ці проблеми стали очевидними. У таких умовах стає пріоритетним осмислення сукупності інформаційних процесів у контексті правового забезпечення безпеки України. З огляду на це цілком природним вбачається пошук основоположних цінностей, цілей, інтересів та надбань в інформаційній сфері, які слугуватимуть орієнтирами європейської перспективи України, майбутнього розвитку українського суспільства, заснованої на інформаційних технологіях, закладуть фундамент подальшого розвитку інформаційного права в Україні.

У цьому контексті закономірно зростає роль правових механізмів у забезпеченні інформаційної безпеки України, потреба ефективного законодавчого врегулювання суспільних відносин, що виникають у досліджуваній сфері, визначення правових засад організації та координації дій суб’єктів забезпечення інформаційної безпеки України, розробці пріоритетних напрямів державної політики у сфері інформаційної безпеки. Дослідження інформаційної безпеки України з правничої точки зору пов’язане з формуванням якісної системи інформаційної безпеки, що відповідатиме сучасним вимогам та нагальним потребам України як повноправного члена й надійного партнера європейської спільноти.

Обравши євроінтеграційний курс та визначивши вступ до НАТО своїм стратегічним пріоритетом, Україна має орієнтуватися передусім на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфері. Для нашої держави імплементація європейських стандартів правового забезпечення інформаційної безпеки держави є пріоритетним засобом інтеграції в європейський правовий простір.

Актуальність теми дослідження зумовлюється передовсім гостротою самої проблеми забезпечення інформаційної безпеки України, особливо її правового складника, сфокусованого на забезпеченні безпеки людини, суспільства й держави.

*Об’єктом кваліфікаційної роботи* є суспільні відносини, що виникають у сфері інформаційної безпеки.

*Предметом* дослідження є інформаційна безпека як складова національної безпеки України в умовах глобалізацій них правових процесів

*Мета* роботи полягає у тому, щоб на підставі комплексного аналізу наявних наукових та нормативних джерел визначити зміст інформаційної безпеки як складової національної безпеки України.

Відповідно до посавленої мети поставлені наступні завдання:

* визначити поняття, ознаки, правовий режим інформаційної безпеки в системі національної безпеки в Україні
* охарактеризувати особливості правового забезпечення інформаційної безпеки в умовах загроз національній безпеці
* проаналізувати особливості забезпечення інформаційної безпеки людини в умовах загроз національній безпеці
* визначити пріоритети вдосконалення правових основ інформаційної безпеки в національній безпеці в умовах реформаційних змін

*Ступінь наукової розробки проблеми* З метою дослідження існуючих підходів до розуміння інформаційної безпеки людини та її правового забезпечення було проаналізовано праці з різноманітних сфер наукового знання – окремих галузей правової науки, соціології, політології, наукових знань про безпеку тощо. Під час дослідження вивчалися праці, не лише в галузі інформаційного права, а й теорії держави і права, конституційного, адміністративного, цивільного, кримінального та інших галузей, зокрема: Арістова І.В., Баранов О.А., Битяк Ю.П., Бєляков К.І., Бєлєвцева В.В., Брижко В.М., Довгань О.Д., Гаращук В.М., Голіна В.В., Гурковський В.І., Калюжний Р.А., Капліна О.В., Коновалова В.О., Кормич Б.А., Корж І.Ф., Кохановська О.В., Костецька Т.А., Красноступ Г.М., Логінов О.В., Ліпкан В.А., Матюхіна Н.П., Марущак А.І., Мукомела І.В., Настюк В.Я., Новицька Н.Б., Новицький А.М., Олійник О.В., Пазюк А.В., Панов М.І., Політанський В.С., Пилипчук В.Г., Савінова Н.А., Селіванов А.О., Сухорольський П.М., Тацій В.Я., Тихий В.П., Тихомиров О.О., Фурашев В.М., Цимбалюк В.С., Шепітько В.Ю., Шопіна І.М., та інші. Їх наукові здобутки, а також доробок таких вчених як Баулін Ю.В., Борисов В.І., Гуторова Н.О., Журавель В.А., Криницький І.Є., Кучерявенко М.П., Лукашевич В.Г., Нижник Н.Р., Оніщенко Н.М., Петришин О.В., Пришва Н.Ю., Скакун О.Ф., Степанюк А.Х, Шило О.Г., Шумило М.Є., Щур Б.В.

*Опис проблеми, що досліджується.*За останні роки парадигма інформаційної безпеки нашої держависуттєво змінилася. Насамперед трансформовано саму природу, авідповідно і стратегічний вимір концепції забезпечення інформаційноїбезпеки держави. При цьому інформаційна безпека України постає не якщось віртуальне, абстрактний об’єкт наукового пізнання, а як абсолютнореальна субстанція, в межах якої точаться запеклі бої, існують очевиднізагрози з явними наслідками. Можемо упевнено стверджувати, що вУкраїні створюється своя модель інформаційної безпеки, яка ґрунтуєтьсявиключно на власному досвіді як правового, так і оперативного їїзабезпечення. Ця модель почала будуватися в надзвичайно складнийперіод державотворчих процесів, під час практично неоголошеної війни зРосією. Отже, серед зовнішніх чинників, що спонукають до розробки тавпровадження власної концепції забезпечення інформаційної безпекиУкраїни, найбільш суттєвим убачається процес підриву за допомогоюінформації традиційних цінностей країн та народів і нав’язування чужогосвітосприйняття.

Перш ніж перейти до аналізу дійсної ситуації пропонуємо звернути увагу на зміст категорії, що досліджується. Термін «система» походить від давньогрецького σύστημα – «сполучення» і буквально означає ціле, складене з частин. Основною змістовною складовою системного підходу вирішення наукових проблем є система. В античній філософії онтологічне тлумачення системи передбачало упорядкованість та цілісність буття. Розуміння системи опирало на організованість Всесвіту як природний порядок, створений богами.

Важливими кроками в історії поняття «система» вважають постулати Анаксагора «все у всьому» і «з усього – все»; атомістичне вчення Левкіппа і Демокрита; висловлювання Цицерона про те, що світовий організм є нерозривним цілим і всі елементи світобудови гармонійно пов'язані між собою; систему знань Епікура; ідеї системності знання у давньогрецькій філософії Евкліда, Платона, Арістотеля, стоїків.

В працях Г. Гегеля предмети розглядаються як органічна цілісність: «Будь-який предмет – це щось ціле. Як ціле він складається з частин, а частини – з елементів. Відповідно, щоб пізнати предмет (отримати його поняття), необхідно спочатку виявити всі його частини та елементи, а потім подумки зв'язати їх воєдино так, щоб вийшло розуміння цілого. ... Але поодинокі предмети існують не самі по собі, не ізольовано від решти світу. Вони утворюють організовані системи. Такі системи також є цілим і тому визначають собою зміст всіх своїх частин та елементів. Отже, щоб отримати всебічне розуміння поодинокого предмета, необхідно вивчити не тільки сам предмет, а й ту систему (загальність), якій він належить. Тільки при такому підході поняття предмета буде визначено як з боку його одиничності, так і з боку його загальності».

Подальший розвиток принципів системної природи знання віднайшов у німецькій класичній філософії, зокрема у працях І. Канта (наукове знання як система, в якій ціле панує над частинами), Ф. Шеллінга й Г. Гегеля системність пізнання – найважливіша вимога діалектичного мислення).

У ХХ столітті в загальній теорії систем Л. Берталанфі об'єкт розглядався як складний з безліччю властивостей, якостей та їхній взаємозв'язків. В кінці XIX – на початку XX ст. принцип цілісності (холізму) став дуже популярним у наукових дослідженнях. Безперечно, такий підхід є цінний з позиції розуміння людини як складної системи, для якої цілісність її фізіологічного, психоемоційного та соціального станів є необхідною умовою існування і розвитку.

У соціології того часу в основі однієї з перших цілісних концепцій соціальної системи (В. Парето) мало місце механістичне розуміння суспільства як системи, що перебуває у стані рівноваги, але відносної, оскільки вона постійно порушується і відновлюється, оскільки елементи такої соціальної системи механічно впливають один на одного. Поступово відбувся відхід від елементаризму та механіцизму на користь органіцизму – методологічного принципу, за яким соціальні явища досліджувалися за аналогією з природними. В соціології системно-органістичні уявлення про суспільство розвивали О. Конт і Г. Спенсер, визначивши соціальну систему як складне ціле, що формується за законами доцільності. Як кожному живому організму їй властивий постійний розвиток. На відміну від механістичних уявлень про суспільство, органіцизм звертає увагу передовсім на динамічні процеси всередині соціальних систем.

Однак таке перенесення біологічних закономірностей на суспільство не сприялонауковому розумінню соціальних законів. Важливою подією у розвитку системних уявлень вважається публікація у 1948 р. «Кібернетики» Н. Вінера. На думку Д. Гіга, саме з моменту появи кібернетики системні дослідження почали свій справжній розвиток завдяки У.Ешбі, О. Ланге та багатьом іншим вченим, які забезпечили для цього наукову і технічну базу та досвід проектування автоматизованих систем. На відміну від Л. Берталанфі, який особливу увагу приділяв вивченню взаємодії системи із зовнішнім середовищем речовиною, енергією та інформацією, вінеровський підхід передбачав вивчення зв’язків усередині системи, а функціонування системи розглядав як реакцію на зовнішній вплив. Перетривавши історичну еволюцію, поняття «система» в середині ХХ ст. міцно увійшло у наукову термінологію як одне з ключових філософсько-методологічних і спеціально-наукових понять, фундаментальна й універсальна категорія. Аналіз словникових та енциклопедичних статей дає можливість виділити головні загальні риси категорії «система»: цілісність, єдність елементів, комплексність (сукупність елементів), упорядкованість розташування та взаємопов’язаність її складових частин. Семантика загального визначення поняття «система» пов’язана з термінами «ціле», «єдність», «елемент», «зв'язок», «структура».

Водночас, велика кількість визначень поняття «система» в залежності від контексту, цілей і галузі знань, де воно використовується, обумовлює також різні підходи до визначення властивостей системи. Зокрема, серед них: система прагне зберегти свою структуру (ця властивість заснована на об'єктивному законі організації — законі самозбереження); система має потребу в управлінні (існує набір потреб людини, тварини, суспільства, великого соціуму); у системі формуються складні зв'язки в залежності від індивідуальних властивостей її елементів і підсистем (система може мати властивості не властивих їй елементів, і може не мати властивостей своїх елементів); кожна система має вхідний вплив, систему переробки (обробки), кінцеві результати (вихід) і зворотний зв'язок; на вході система зазнає впливу з боку середовища, а через вихід вона впливає на зовнішнє середовище.

Слід також пам’ятати, що безпечний розвиток будь-якого суспільства, держави, людини безпосередньо обумовлений їх інформаційною безпекою, оскільки інформаційне середовище виступає системотворчим фактором розвитку.

Беручи до уваги вищезазначене, звернімося до бачення інформаційної безпеки як системного явища. Зважаючи на те, що інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки, питання її забезпечення має загальнонаціональне і загально державне значення. Водночас, інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Відсутність системи забезпечення інформаційної безпеки унеможливлює надійне забезпечення не лише інформаційної, а й національної безпеки.

Таким чином, обґрунтованим вбачається розглядати систему інформаційної безпеки з урахуванням її місця в системі національної безпеки України та концептуальних питань, опрацьованих на рівні доктрини національної безпеки України. Кожне із великого різноманіття визначень національної безпеки певним чином віддзеркалює її сутнісний чи функціональний аспекти. Зазначене також стосується інформаційної складової у забезпеченні національної безпеки. Очевидно, що інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні і внутрішні чинники, найважливішими з яких є: 1) політична обстановка у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітична обстановка в державі. Водночас, її компонентами є підсистеми безпеки особистості, держави і суспільства. Саме взаємозалежна, системна єдність останніх складає якісну визначеність, покликану здійснити захист життєво важливих інтересів людини, суспільства і держави, забезпечити їх існування і розвиток.

Розуміння категорії «система інформаційної безпеки» в науковій думці відображає в переважній більшості практично-діяльнісний підхід, водночас, як правило, відрізняється доктринальною складовою. Так, Кормич Б.А. складовими сучасної системи безпеки називає: доктрину і правову основу; інституціональний механізм; методологічна база, що використовується для реалізації конкретних завдань у межах політики безпеки.

Вивчення праць іноземних вчених, дозволило зробити висновок, що таким системам властиві низка ключових ознак: ієрархічність побудови системи; наявність керівного, а не дорадчого органу системи; організація взаємодії між усіма елементами системи; взаємозв’язок національної та міжнародної систем.

Загальне керівництво системою здійснюється, як правило, головою иконавчої влади через відповідний робочий орган, який розробляє державну політику інформаційної безпеки і координує діяльність її складових елементів. Найбільш розвинуті системи інформаційної безпеки функціонують у США, Великій Британії, Ізраїлі, ФРН, Російській Федерації, Китаї, тобто у тих країнах, які не лише знаходяться під потужним зовнішнім інформаційним впливом, а й володіють можливостями інформаційного впливу на інші держави та міжнародне співтовариство.

Використовуючи методологію системного дослідження, розроблену У. Баклі, К. Бейлі, Н. Луманом та ін., системний підхід при аналізі феномену інформаційної безпеки означає, що всі суспільні зв’язки і опосередковування, елементи і складові суспільства й держави, функції і проблеми, котрі стосуються забезпечення інформаційної безпеки, розглядаються як взаємопов’язане ціле, а застосування системного підходу дозволить встановити загальну орієнтацію досліджень проблем інформаційної безпеки й зафіксувати науковими засобами цілісність, організованість об’єкта (системи, проблеми, соціального явища, процесу тощо), що досліджується, в усій його повноті та в усій багатоманітності й поліаспектності зв’язків в об’єкті. На основі такого підходу пропонуємо власне бачення системи інформаційної безпеки, елементами якої вбачаються: 1) правова та наукова (доктринальна) основа; 2) об’єктно-суб’єктний склад, тобто об’єкти інформаційної безпеки, а також система органів (підрозділів), що здійснюють її забезпечення; 3) політика інформаційної безпеки; 4) засоби і способи забезпечення інформаційної безпеки. При цьому, для досягнення інформаційної безпеки конкретного об’єкта вбачається необхідною побудова системи забезпечення його інформаційної безпеки.

Звернемося до окремих складових запропонованого підходу.

Тому відразу перейдемо до об’єктно-суб’єктного складу. Ст. 3 Закону України «Про основи національної безпеки України» визначає, що об'єктами забезпечення національної безпеки є: людина і громадянин – їхні конституційні права і свободи; суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність. В наступній ст. 4 визначається, що суб'єктами забезпечення національної безпеки є: Президент України; Верховна Рада 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; Національне антикорупційне бюро України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України; органи і підрозділи цивільного захисту; громадяни України, об'єднання громадян.

На думку О.О. Тихомирова, суб'єкт забезпечення безпеки – одна з основних категорій, що використовується для розкриття змісту системи забезпечення як національної, так і інформаційної безпеки, якій традиційно приділяється багато уваги законодавцем, оскільки саме законодавство у сучасній правовій державі є засобом визначення повноважень суб'єктів та окреслення сфери їх компетенції. Слід звернути увагу, що більшість суб’єктів системи інформаційної безпеки також є її об’єктами – людина і громадянин, держава, окремі її органи, інститути тощо. Власне тому, вважаємо за потрібне говорити про об’єктно-суб’єктний склад як елемент системи інформаційної безпеки.

Аналіз наукових досліджень і законодавчих норм дозволяє зробити висновок про множинність підходів до суб’єктного складу системи забезпечення інформаційної безпеки. М.Б. Левицька, класифікуючи суб’єкти забезпечення національної безпеки акцентує увагу на функціях відповідних органів і виокремлює таким чином: 1) суб'єктів, діяльність яких безпосередньо підпорядкована завданням забезпечення відповідного рівня національної безпеки як у комплексі (Рада національної безпеки і оборони України), так і на окремих напрямках діяльності (правоохоронні та інші державні виконавчі органи спеціальної компетенції); 2) суб'єктів, для яких здійснення такої діяльності є суттєвим, але не єдиним напрямком їх діяльності (вищі органи законодавчої, виконавчої та державної влади); 3) суб'єктів, для яких участь у забезпеченні національної безпеки є допоміжним, другорядним завданням порівняно з основною діяльністю (всі інші державні і громадські організації, наприклад, Товариство сприяння обороні України, пункти охорони громадського порядку тощо).

Теорія національної безпеки відносить до суб'єктів забезпечення національної безпеки всі державні та суспільні інституції, які є учасникамипроцесу забезпечення національної безпеки, а саме: апарат держави як систему державних органів, органи місцевого самоврядування, громадян та їх об'єднання. З цього переліку виокремлюються дві групи суб'єктів (1) ті, що наділені державно-владними повноваженнями, (2) ті, що ними не наділені, хоча в окремих випадках можуть мати певний обсяг делегованих державно-владних повноважень. Екстраполюючи такий підхід, можна говорити про суб’єктів інформаційної безпеки, що здійснюють державне забезпечення і недержавне забезпечення.

Тихомиров О.О. додає ще міжнародний рівень і пропонує серед суб'єктів забезпечення інформаційної безпеки виділяти три групи: міжнародні організації; держава в особі державних організацій; недержавні організації, громадяни та їх об'єднання. Такий підхід був закріплений в уже згадуваній Доктрині інформаційної безпеки, яка передбачала що діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства і людини. Окрім того, заходи щодо забезпечення інформаційної безпеки України фактично відображали міжнародний, державний і недержавний рівні забезпечення інформаційної безпеки. В.І. Гурковський до системи суб’єктів щодо підтримання інформаційної безпеки відносить: 1) органи законодавчої влади і державного управління загальної компетенції; 2) Конституційний суд, суди загальної юрисдикції; 3) органи виконавчої влади: а) правоохоронні органи; б) галузеві органи державного управління, що регулюють інформаційні відносини в певних галузях; 4) громадські структури.

О.В. Олійник на основі аналізу чинного законодавства та враховуючи досвід інших держав запропонував чотири рівні організаційно-функціональної системи забезпечення інформаційної безпеки. Перший рівень – стратегічний, загальнодержавний, який включає Верховну Раду України, Кабінет Міністрів України та їх консультативно-дорадчі органи. Це рівень охоплює політичні рішення, законодавче і нормативно-правове забезпечення, встановлення порядку міжнародного співробітництва, застосування сил і засобів інформаційного протистояння, поведінки суб’єктів в критичних ситуаціях.

Другий рівень -організаційно-виконавчий, відомчо-територіальний, який включає центральні органи виконавчої влади і органи місцевого самоврядування, воєнну організацію держави, правоохоронні органи і органи судової влади. На цьому рівні здійснюється організаційне і методичне забезпечення інформаційної безпеки у відповідних галузях та адміністративно-територіальних утвореннях, координація і контроль діяльності у сферах відповідальності державно-владних структур. Третій рівень – критично важливі інфраструктури країни, до яких доцільним вбачається включення підприємств, установ і організацій, комунікацій національного простору та інших об’єктів, управління яким здійснюється з використанням електронно-комунікаційних засобів та інформаційних технологій. На цьому рівні мають виконуватись повноваження, спрямовані на забезпечення безпечного функціонування загальнодержавних, відомчо-територіальних критично важливих інфраструктур, гарантованого попередження зовнішніх та внутрішніх загроз і небезпек, які можуть завдати шкоду громадянам, суспільству і державі.

Хотілося б звернути увагу на важливість правового закріплення критичної інфраструктури держави в цілому, та її інформаційної складової зокрема, звернувшись до іноземного досвіду. В країнах ЄС та у США на законодавчому рівні визначено змістовне наповнення категорії "критична інфраструктура" та визначено план дій на випадок її ураження. У жовтні 2004 р. Європейська комісія здійснила розробку загальної методології із захисту критичної інфраструктури та рекомендувала посилити увагу на технологічних й інформаційних елементах захисту тих об’єктів, припинення функціонування яких матиме транскордонний вплив. Європейська інформаційна мережа попередження загроз критичній інфраструктурі - CriticalInfrastructureWarningInformationNetwork (CIWIN) була офіційно затвердженорішенням Ради 2008/0200, а у квітні 2009 р. Європейський парламент прийняв відповідне законодавче рішення про CIWIN. Зокрема, всім країнам ЄС рекомендовано вжити належних заходів: розробити національну програму захисту критичної інфраструктури; забезпечити такий рівень охорони здоров’я, технологічної безпеки, соціально-економічного добробуту, що гарантував би «стійкість» нації до загроз; об’єднати зусилля, спрямовані на захист критичної інфраструктури, визначивши єдиний державний орган, що звітує з цього питання, і наділений функціями координації дій державних органів влади, які спеціалізуються і тісно взаємопов’язаніз галузями промисловості до яких належать об’єкти критичної інфраструктури; визначити органи державної влади, відповідальні за сектори критичної інфраструктури, та відповідні приватні компанії; створити умови для ефективної взаємодії та обміну інформацією, даними і досвідом між країнами-членами ЄС, урядовими структурами та приватним сектором; брати участь у створенні гармонізованої методології на рівні ЄС та загальноєвропейської системи аналізу ризиків. Нормативно-правове визначення критичної інформаційної інфраструктури та органів відповідальних за її безпеку вбачається необхідною умовою створення безпечного інформаційного середовища, а також гарантування національного інформаційного суверенітету.

До четвертого рівня О.В. Олійник відніс суб’єктів невладного характеру, громадян України та їх об’єднання, державні і приватні засоби масової інформації. Для того, щоб на цьому рівні могло здійснюватись забезпечення інформаційної безпеки необхідним є закладення правових основ такої діяльності, зокрема закріплення їх правового статусу, надання достатнього обсягу прав і свобод, а також створення ефективної системи судочинства. Інакше, існування цього рівня не передбачатиме реального впливу.

Можливості забезпечення інформаційної безпеки значною мірою залежать від сильних та слабких сторін держави. Ф.Х. Гартман серед таких вирізняє: демографічний чинник – кількість населення держави, демографічна труктура і тенденції – зростання чи зменшення кількості населення; географічний чинник – положення, розмір території, клімат, географічні особливості; економічний чинник – сировинна база, потреби, об’єми валового виробництва, прогнозоване господарське зростання; історико-психолого-соціологічний чинник – історичний досвід, ставлення до життя, єдність суспільства; організаційно-адміністративний чинник – форма правління, ставлення суспільство до влади, ефективність діяльності влади; військовий чинник – спосіб організації і стан ефективності збройних сил, їх розмір у співвідношенні до населення призовного віку.

І.Р. Боднар пропонує національну безпеку України в інформаційній сфері розглядати як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки.

Тому в процесі визначення характеру ризиків він пропонує брати до уваги наступні елементи: концептуальні засади політичної безпеки, її принципів, стандартів та правил, погоджених із чинним законодавством й принципами забезпечення безперервності системи інформаційної безпеки особистості, суспільства, комерційних (корпоративних) структур та держави; визначення об’єктів та цілей; визначення прийнятних з погляду забезпечення інтересів усіх суб’єктів структур встановлення контролю над об’єктами безпеки, а також оцінки ризиків та управління ризиками; визначення статусно-функціональних ролей, очікувань та міри відповідальності задіяних суб’єктів включно зі звітністю про події, які несуть потенційні загрози.

На нашу думку, діяльність із забезпечення інформаційної безпеки людини має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства та людини за трьома головними напрямами - інформаційно-психологічному; технологічному, а також правовому. Такий підхід до внутрішньої будови інформаційної безпеки людини обумовлений відображає сфери, в яких можуть бути реалізовані загрози.

Інформаційна безпека зараз безперечно є популярною темою, яку експлуатують ЗМІ, політики, навіть бізнес. Щоб не повертатись до теоретичних розмірковувань, зазначимо, що, на нашу думку, проаналізовані підходи до інформаційної безпеки людини можна узагальнити в два основні. Перший підхід домінує в правових науках та безпекознавстві, і насамперед, наголошує на забезпеченні можливості людини вільно і безперешкодно реалізовувати права та свободи в інформаційній сфері. Починаючи з 40-х рр. ХХ ст. у світі набув розвитку власне напрям інформаційної безпеки людини. Тобто це питання почало формуватись не “згори” – від владних органів, а “знизу” – в контексті боротьби за реалізацію інформаційних прав людини, зокрема свободи слова, таємниці приватного життя тощо.

Чинники, що зумовлюють ескалацію загроз інформаційні безпеці, мають комплексний характер – вони охоплюють усі сфери життєдіяльності людини, суспільства і держави, а відповідно мають міжвідомчий характер. Таким чином, на практиці аналіз загроз – це завжди суб’єктивний процес сприйняття певною особою чи соціальною групою певних факторів через призму власних інтересів і фахового рівня. Разом із тим, об’єктивне визначення загроз передбачає чітке усвідомлення параметрів, поза межами яких певне явище втрачає можливості саморегуляції та потребує зовнішнього втручання для збереження стабільності соціальної системи, а також певних умов, що перетворюють ті ж самі фактори або на реальну, або на потенційну загрозу. Водночас, класифікація загроз дозволяє визначити, які саме загрози становлять переважний пріоритет в науковій чи нормативно-правовій перспективі. Відповідно до Закону України „Про основи національної безпеки України” до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп’ютерна злочинність та комп’ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що е власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Попередня редакція Доктрини інформаційної безпеки України визначала основні реальні та потенційні загрози інформаційній безпеці України класифікуючи їх за сферами життєдіяльності особи, суспільства і держави,зокрема: у зовнішньополітичній сфері, сфері державної безпеки, воєнній сфері, внутрішньополітичній сфері, економічній сфері, соціальній та гуманітарній сферах, науково-технологічній сфері, в екологічній сфері.

Нова редакція 2017 р. актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері визначила: здійснення спеціальних інформаційних операцій, спрямованих на підрив бороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально- економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні; проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах; інформаційне домінування держави-агресора на тимчасово окупованих територіях; недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України; неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

У Законі України „Про Основні засади розвитку інформаційного суспільства в Україні на 2007−2015 роки”, який все ще залишається чинним, загрозами інформаційній безпеці визначено: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; егативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. У Державному стандарті України „Захист інформації. Технічний захист інформації. Основні положення.” ДСТУ 3396.0-96 безпосереднє формулювання класифікації загроз відсутнє, проте в ньому передбачено можливі шляхи реалізації загроз. Саме вони дають можливість уявити або визначити ймовірні загрози інформаційним відносинам (відносинам щодо збору, обробки й накопичення інформації). В частині 4.1.3 підпункту 4.1 пункту 4 визначено, що загрози можуть здійснюватися: технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали; каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації; несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав’язування хибної нформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз. Державний стандарт України „Захист інформації. Технічний захист інформації. Терміни та визначення.” ДСТУ 3396.2-97 містить ряд термінів пов’язаних з інформаційною безпекою та які мають пряме відношення до класифікації загроз. Так, пункт 5 „Загроза для інформації” містить наступні визначення: витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання; порушення цілісності інформації – спотворення інформації, її руйнування або знищення; блокування інформації – унеможливлення санкціонованого доступу до інформації.

Класифікація загроз відповідно має наступний вигляд: загрози витоку інформації; загрози порушення цілісності інформації; загрози блокування інформації.

Можемо зробити висновок, що така різноманітність класифікацій в чинному законодавстві обумовлена не лише різноманітними підходами до вибору класифікаційних ознак та цілями класифікації, але й відсутність належного теоретичного обґрунтування сутності загроз інформаційної безпеки. До 2016 р. переважна увага приділялась технічному захисту інформації, то Доктрина інформаційної безпеки перемістила акценти на захист від інформаційної експансії з боку держави-агресора. Науковці також не дотримуються одностайності щодо класифікації загроз інформаційній безпеці. Професор В. Ліпкан пропонує класифікувати загрози інформаційній безпеці відповідно до загальної класифікації загроз національній безпеці: за джерелами походження: природного походження, техногенного походження, антропогенного походження; за ступенем гіпотетичної шкоди: загроза та небезпека; за повторюваністю вчинення: повторювані та продовжувані; за сферами походження: екзогенні та ендогенні; за ймовірністю реалізації: вірогідні, неможливі, випадкові; за рівнем детермінізму: закономірні та випадкові; за значенням: допустимі та неприпустимі; за структурою впливу: системні, структурні та елементні; за характером реалізації: реальні, потенційні, здійснені, уявні; за ставленням до них: об’єктивні та суб’єктивні; за об’єктом впливу - особа; суспільство; держава. В іншій праці, інтегруючи різноманітні підходи, а також пропозиції щодо розв’язання даного питання, запропоновано такі види загроз інформаційній безпеці: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання. Зокрема вчений визначає загрози як: розкриття інформаційних ресурсів; порушення цілісності інформаційних ресурсів; збій у роботі обладнання.

В свою чергу С. Гуцу та О. Литвиненко, у сходяться на тому, що основні загрози інформаційній безпеці можна представити у такому вигляді: загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання); загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову). Л. Євдоченко формуючи власний підхід до класифікації інформаційних загроз та з метою вироблення рекомендацій щодо організації державою дієвих форм і методів забезпечення інформаційної безпеки, визначає і класифікує загрози за кількома критеріями: за способом впливу на об’єкти інформаційної безпеки (інформаційні, фізичні й програмно-математичні, організаційно-правові); за джерелами надходження (внутрішні та зовнішні); за характером вияву (політичні, економічні, організаційно-технічні).

На нашу думку, підхід до розуміння суті інформаційної безпеки різних категорій суб’єктів може істотно відрізнятися, наприклад, безпека пересічних громадян або посадових осіб органів державної влади. Тому цілком логічними та вартими уваги є класифікації загроз які мають більш вузький, або іншими словами спеціальний характер, зокрема, загрози інформаційній безпеці мережевих ресурсів.

У цьому ж контексті більш ширшу класифікацію пропонує А. Погребняк, на його думку загрози можуть бути як випадковими, так і навмисними. До випадкових загроз відносяться: а) помилки обслуговуючого персоналу і користувачів; б) втрата інформації внаслідок не правильного її збереження; в) випадкове знищення або заміна; г) збій у роботі устаткування, електроживлення, дискових систем, комплектуючих елементів мережі; д) некоректна робота програмного забезпечення, зокрема внаслідок зараження комп’ютерними вірусами тощо. До навмисних загроз відносяться: а) несанкціонований доступ до інформації і мережевих ресурсів; б) розкриття і модифікація даних і програм, їх копіювання; в) розкриття, модифікація або підміна трафіка обчислювальної мережі; г) розробка і поширення комп’ютерних вірусів, введення в програмне забезпечення логічних бомб; д) крадіжка магнітних носіїв і розрахункових документів; е) руйнування архівної інформації або навмисне її знищення; є) фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому; ж) перехоплення та ознайомлення з інформацією, яка передана по каналах зв’язку.

Будь-яка з наведених класифікацій, до певної міри, є умовною, оскільки: 1) залежно від мети та методів наукового пізнання може здійснюватись за різними підставами; 2) має суб’єктивний характер, тобто в залежності від суб’єкта що її здійснює та його здатності розрізняти ознаки об’єкта класифікації. Доктриною інформаційної безпеки України визначено як життєво важливі інтереси особи в інформаційній сфері України наступні: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів. Відразу звернемо увагу, що вже в самій назві допущено підміна категорії «людина» на «особа».

Вважаємо, що проблеми захисту від інформації суттєво складніші за проблеми захисту інформації, оскільки загрози, що виникають внаслідок інформаційних впливів надзвичайно різноманітні, їх вплив не завжди очевидний, а відвернення цих загроз або їх нейтралізація вимагають різноманітних неординарних дій. Інформаційні загрози є складним ієрархічним утворенням з множиною різнорівневих зв’язків, їх вплив на людину комплексний і різноманітний.

Варто також звернути увагу, що закріплені інтереси певною мірою відрізняються від тих, що були закріплені в попередній редакції Доктрини: 1) забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; 2) недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних; 3) захищеність від негативного інформаційно-психологічного впливу.

Зокрема, слід звернути увагу на пп. 2 і 3 замість більш вузької категорії «персональні дані», нова редакція передбачає «захист приватного життя», а в п.3 уточнено , що захист потрібен від руйнівних інформаційно-психологічних впливів, а не від негативного інформаційно-психологічного впливу. Таким чином, держава зняла з себе повноваження визначати, що є негативним інформаційно-психологічним впливом. Донедавна єдиним органом, який визначав що саме є негативним інформаційно-психологічним впливом була Національна експертна комісія України з питань захисту суспільної моралі, яка в різних статусах проіснувала понад 10 років. Досвід її роботи свідчить, що коли державні органи мають повноваження визначати що є моральним, зокрема «сексуальний чи еротичний характер» або «культ насильства, жорстокості, порнографії» призводить до зловживань та цензури. Проте і її вже не існує. При цьому, чинне законодавство як не передбачало визначення «негативного інформаційно-психологічного впливу», так не передбачає і змісту категорії «руйнівних інформаційно-психологічних впливів». В чинному законодавстві і в правовій науковій літературі часто зустрічається некоректне використання категорій «загрози, ризики, виклики, небезпеки, впливи», що пов’язане з нерозумінням природи цих явищ, та їх місця в системі інформаційної безпеки.

Теорія безпеки окреслює категоріальний апарат, який може і, на нашу думку, повинен використовуватись в нормотворчості з метою уникнення підміни понять, а також з огляду на комунікативну правову доцільність. Існує також низка різноманітних визначень виклику, що вказують на наявність протидії (з боку об’єктивних обставин або суб’єктів) реалізації інтересів певного суб’єкта. Виклики не мають чіткого механізму розв’язання, проте ще не вимагають негайного втручання”. Водночас, він характеризується найнижчим ступенем ймовірної реалізації. Коли йдеться про ризики йдеться про усвідомлену можливість небезпеки, а також як можливість збитків або неуспіху у якійсь справі.

Сучасний тлумачний словник визначає загрозу як можливість, неминучість небезпеки. З усього різноманіття визначань загрозою можна вважати явище, чинник (и), що спроможні реально створити умови або стати причиною повної або часткової неможливості реалізації істотних інтересів суб’єкта. Небезпека, за А. Качинським, розуміється як «ситуація, постійно присутня в навколишньому середовищі, що за певних умов може призвести до реалізації небажаної події», має майже стовідсоткову ймовірність Г. Ситником пропонується класифікація видів небезпек, що розкриває взаємозв’язок між цими поняттями, і пропонує при кількісній класифікації небезпек спиратися на поняття „ризик”, а при якісній класифікації – на поняття „виклик” і „загроза”. Тоді: потенційний виклик (дуже малий ризик); реальний виклик (малий ризик); потенційна загроза (середній ризик); реальна загроза (великий ризик); потенційна небезпека (дуже великий ризик).

Категорія «вплив», в свою чергу, в теорії безпеки може розглядатись з кількох точок зору. Як взаємодію явищ (чинників) із об’єктом, що призводить до виникнення викликів, ризиків, загроз і небезпек, а також і як цілеспрямовану дію суб’єктів системи забезпечення з метою нейтралізації останніх.

Найбільш широко визначення сутності впливу відкриваються уконтексті філософської категорії “взаємодія”. “Філософський енциклопедичний словник” визначає “взаємодію” як філософську категорію, що відображає процеси впливу різних об’єктів один на одного, їхню взаємну обумовленість, зміну стану, взаємопереходи, а також породження одним об’єктом іншого. Власне з такої позиції Г. Ковальов вплив розуміє як “процес... який реалізується в ході взаємодії двох і більше рівномірно упорядкованих систем і результатом якого є зміна в структурі (просторово-тимчасових характеристиках), в стані хоча б однієї із цих систем”.

Категорія впливу є багатовимірною і складною. Існує також позиція, згідно якої феномену впливу має універсальність та всеохоплюючий характер, і може відображати взаємозв’язки, які існують між впливами, різними за своїм походженням та природою (фізичний, хімічний, соціальний, психологічний тощо).

Хоча, фахівці з психології вважають, що результат впливу завжди психологічний, навіть якщо за змістом він є фізичний, хімічний чи соціальний. Слід зауважити, що інформаційний вплив завжди визначає поведінку людини прямо чи опосередковано, через психічні механізми головного мозку. Інформаційні впливи досягають ефекту, коли вони змінюють, реструктурують психологічні властивості, стани і моделі поведінки особистості. Такий підхід певною мірою пояснює, чому терміни «інформаційний вплив» і «інформаційно-психологічний вплив» часто використовуються як взаємозамінні. Хоча, на нашу думку, ці категорії мають певні відмінності, про що буде далі.

Аналіз філософського розуміння категорії впливу дозволяє перейти до визначення інформаційних або інформаційно-психологічних впливів, як таких, що можуть бути руйнівними чи небезпечними. В теорії безпеки визначається «інформаційний вплив як організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення деструктивних змін у свідомість особистості, соціальних груп чи населення (корекція поведінки), в інформаційно-технічну інфраструктуру об'єкта впливу та (чи) фізичний стан людини». При цьому інформаційний вплив поділяють на інформаційно-технічний та інформаційно-психологічний впливи, де інформаційно-технічний вплив розглядається як вплив на інформаційно-технічну інфраструктуру об'єкта з метою забезпечення реалізації необхідних змін у її функціонуванні (зупинка роботи, несанкціонований доступ до інформації та її перекручування (спотворення), програмування на певні поминки, зниження швидкості оброблення інформації тощо), а також вплив на фізичний стан людини.

Інформаційно-психологічний вплив розглядається як вплив на свідомість та підсвідомість особистості й населення з метою внесення змін у їхню поведінку та світогляд; його базовими методами є переконання й навіювання.

Одна з найбільш ґрунтовних, на нашу думку, класифікацій видів психологічного впливу в спілкуванні запропонована О.В. Сидоренко: 1) переконання – свідомо аргументований вплив на іншу людину або групу людей, що має своєю метою змінити їхнє судження, ставлення, намір або рішення; 2) самопросування – відкритий прояв свідчення наявності у людини своєї компетентності й кваліфікації для того, щоб бути оціненою по здобуткам й завдяки цьому отримати перевагу; 3) маніпуляція – прихований від опонента вплив на нього, на його систему ставлень і орієнтацій; 4) прихиляння до наслідування – створення у іншої людини бажання “бути схожою”, подібною до зразка; 5) прохання – словесне звертання до людини із пропозицією задовольнити потребу або бажання ініціатора; 6) примус – вимога виконувати розпорядження ініціатора, підкріплюване прихованими або явними погрозами; 7) деструктивна критика – зневажливі або образливі судження висловлення про особистість опонента, грубий, а іноді агресивний осуд, ганьблення або осміяння його пороків, вчинків; 8) ігнорування – навмисна неуважність, підкреслене неприйняття людини, при якому ігнорування, найчастіше, виступає як тактична форма примусу або залучення уваги людини до чогось; 9) емоційне зараження – передача свого стану і ставлення іншій людині або групі осіб; 10) навіювання – навмисний свідомий вплив на підсвідомість людини або групи осіб з метою зміни їхнього стану або відношення до питання, а також створення схильності до певних дій. З цієї класифікації видно складність розмежування очевидно правомірних (наприклад, як переконання) і завідомо неправомірних (наприклад, як маніпуляція) способів інформаційного впливу на психіку особи, оскільки всі інші можуть бути використані для досягнення як законних, так і незаконних цілей, отже стати способом вчинення правопорушення. Наприклад, примус використовуватись в рамках закону для забезпечення правопорядку, а, водночас, може стати засобом порушення прав і свобод людини. Навіювання і емоційне зараження часто використовуються маркетологами та психологами в рамках закону, а, водночас, можуть бути використані в шахрайствах та інших правопорушеннях.

За результативністю інформаційні впливи поділяють на ефективні й неефективні; сутнісні, істотні, глибинні й неістотні, поверхневі; стабілізуючі та дестабілізуючі; організуючі та дезорганізуючі. За масштабом трансформацій, спричинених впливами, їх поділяють на глобальні та локальні, часткові. Сам цей масштаб може оцінюватись як за кількістю елементів, що зазнали впливу, так і за ступенем істотності викликаних змін. За масштабом змін може йтися: а) про вплив на актуальну поведінку через породження або зміну ситуативних мотивів, особистісних смислів або смислових установок, як це відбувається в ситуації міжособистісної маніпуляції чи вольової саморегуляції, б) про зміну стійкого ставлення до конкретних речей або людей через породження смислових диспозицій та іноді конструктів, як це робиться, зокрема, в рекламі та пропаганді, а іноді й у психологічному консультуванні; в) про формування чи зміну загальних смислових орієнтацій – світогляду, самостановлення, системи цінностей, із чим має справу практика виховання і психотерапії, а також про ідейну індоктринацію.

Наслідки інформаційних впливів виявляються у цілій низці ефектів, які класифікують таким чином: 1) когнітивні ефекти проявляються у зміні рівня поінформованості, збільшенні обсягу знань (як в усвідомлюваних, так і в неусвідомлюваних формах); формуванні нових когнітивних схем, способів осмислення дійсності, оперування інформацією; 2) емоційні ефекти виражаються у зміні емоційного стану, появі одних та зникненні інших почуттів, у зміні загального емоційно-психологічного фону людського буття, появі імпульсів до активних роздумів, до переробки, трансформації інформації, виникнення прагнення до отримання чи створення нової тощо; 3) ціннісні ефекти виявляються у формуванні нових чи зміцненні або послабленні вже наявних інтересів, смаків, ставлень, оцінок, ціннісних орієнтацій, настанов стосовно світу, окремих предметів, явищ, стосовно інших людей або самих себе; 4) психофізіологічні ефекти також спостерігаються і виявляють себе у зміні психофізіологічного стану особи; 5) поведінкові ефекти спостерігаються у вигляді певних дій, вчинків, відповідної поведінки у сфері предметної діяльності (зокрема, її організації), міжособистісної взаємодії та взаємодії із самим собою. Особливість інформаційних загроз виявляється в тому, що до появи поведінкових ефектів, їх виявлення і ідентифікація джерела у більшості випадків є неможливою, а отже неможливо і застосувати ефективні заходи щодо нейтралізації їх впливу.

Водночас, слід пам’ятати, що інформаційні впливи є невід’ємною складовою життєдіяльності людини в інформаційному середовищі, необхідною умовою існування суспільної та індивідуальної свідомості, формування людини та її нормальної життєдіяльності, а потреба в інформації – базовою потребою особистості. Інформаційне середовище з його інформаційними потоками та інформаційні впливами різного роду, характеризується сукупністю динамічних факторів,що здатні чинити на людину прямий або непрямий, негайний або відтерміновний вплив. Інформаційне середовище є засобом, що опосередковано транслює людині норми, цінності, установки та стереотипи поведінки в суспільстві. Достатність інформаційних впливів на свідомість забезпечує образ реальності, когнітивну модель світу і ситуації, розуміння себе і своїх можливостей. Фундаментальна властивість інформації (щодо людини) полягає втому, що вона існує самостійно, відокремлено від об’єкта відображення, стає вмістом пам’яті, тобто самостійно бере участь в психічних процесах, трансформується в уявлення, знання, вміння, навички.

Кожна людина, вступаючи в суспільні відносини, одержуючи і передаючи певну інформацію, вливається в це суспільство шляхом засвоєння й дотримання (або незасвоєння чи недотримання) тих норм, які історично в ньому склались.

Тому саме суспільство виступає носієм однієї з найбільших загроз інформаційній безпеці людини – інформаційної дискримінації, яка проявляється не лише в розподілі людей на тих, які мають доступ до інформації, і тих, які його не мають. У зв’язку з цим поряд з терміном “інформаційне суспільство” у міжнародній практиці поширюється термін “цифровий розрив” або “цифрова нерівність”, про який ми дещо згадували раніше. На міжнародному рівні питання інформаційної нерівності вперше було порушене в підписаній улітку 2000 р. лідерами країн “вісімки” Окінавській хартії глобального інформаційного суспільства. Згідно з цим документом було утворено міжнародну експертну раду Dіgіtal Opportunіty Task Force, що виробила план дій, представлений лідерам країн “вісімки” на зустрічі в Генуї влітку 2001 р.

Як відомо, головною метою ООН, сформульованою в Декларації Тисячоліття, є зменшення бідності на планеті. В контексті боротьби з бідністю ООН вирішує й завдання подолання інформаційної нерівності. Що цілком природно, оскільки базовою нерівністю є нерівність економічна, соціальна і культурна, інформаційна ж нерівність є тільки одним з проявів цих базових нерівностей. Без подолання інформаційної нерівності неможливий ні процес глобалізації, ні ефективний розвиток інформаційного суспільства, ні запровадження електронних урядів.

Варто звернути увагу, що впроваджуючи в Україні зараз активно процеси е- урядування, пов’язані з ними реалії віддаленого голосування, електронних консультацій, публічних обговорень на сайтах тощо, опираються на ІКТ. І при охопленності близько 60% дорослого населення їх ефективність видається сумнівною. Це не означає, що не потрібно впроваджувати електронну демократію, а свідчить про необхідність гарантування рівних можливостей доступу до інформаційних технологій.

Міжнародне співтовариство вже з 2000 р. акцентує увагу на необхідності подолання ознак інформаційної та цифрової нерівності, зокрема, в Окінавській хартії глобального інформаційного суспільства серед інших позицій окрема увага зосереджується на необхідності “мобілізації ресурсів для покращення інформаційної та комунікаційної інфраструктур”, оскільки інформаційно-комунікаційні технології є найголовнішим чинником, що впливає на формування суспільства ХХІ ст. ЮНЕСКО визначає головні групи соціальних ознак, відповідно до яких формуються групи розривів: економічні ресурси; географія (асиметрія між міськими і сільськими зонами); вік; стать; мова; освіта, соціальні й культурні підвалини; фізична повноцінність. Економічні ресурси є одним із найважливіших чинників формування світових розривів. Економічно багаті країни мають більші ресурси для втілення технологічних новацій та залучення до них мас. Фінансово незалежні індивіди орієнтуються на найновіші телекомунікаційні та інші технічні засоби для задоволення власних потреб. Географічні розриви базуються на кількох сегментах, зокрема це міжнародний та внутрішній вектори. Міжнародний вектор характеризується суттєвими дисбалансами у доступі до інформації та комунікації через новітні телекомунікаційні канали до світової скарбниці знань між деякими країнами. Наприклад, доступ до Інтернету в країнах Скандинавії перевищує показник у 90 % населення, тоді як в Україні й інших пострадянських країнах цей показник коливається біля позначки 50 % населення, причому левова частка з них — це мешканці великих міст. Згідно з даними інтернет Асоціація України (опубліковано на їхньому офіційному сайті у квітні 2017 р.), які представляють результати опитування, проведеного протягом лютого 2017 р., на початку р. 64,7% дорослого населення України користуються інтернетом. Частка користувачів інтернет серед людей 15-29 років в Україні сягнула 97%. Старший вік та проживання у сільській місцевості значно зменшують вірогідність користування інтернетом. Опитування проводилось у всіх регіонах України крім окупованого Криму та тимчасово непідконтрольних Україні територій Донбасу.

Кількість користувачів інтернет продовжує зростати. Найчастіше виходять до інтернету за допомогою стаціонарного ПК - 51%, стільникових телефонів - 50%, ноутбуків - 42%, планшетний комп'ютер - 21%, стаціонарний ПК на роботі - 8%, ноутбук на роботі - 5%. В Україні користуються інтернетом близько 21,6 млн. користувачів. Жінки складають - 51% від усіх користувачів, чоловіки - 49%. Мешканці сіл складають 27% у загальній кількості, притому що серед усіх мешканців сіл уже 53% з них користуються інтернетом. Вікові розриви пов’язані з прагненням і відкритістю молоді до інновацій, тоді як люди середнього та старшого віку схильні до стабільності й певної статики. Все залежить від створених можливостей і мотивації. Гендерні проблеми виникають у суспільствах, в яких жінка через релігійні чи інші умовності розглядається як неповноправний суб’єкт громадського життя. У Камбоджі законодавчо заборонено ввезення до країни телефонів третього покоління, оскільки “удосконалені моделі сприяють поширенню порнографії” . В Україні ситуація за гендерною ознакою цілком прийнятна – 51 % жінки, 49 % чоловіки.

Однією з суттєвих нерівностей, які перешкоджають реалізації якісного мережевого спілкування, є мовна диспропорція, сформована на основі домінування англійської мови як головної мови інтернету та програмного ітехнічного супроводу комп’ютерних та телекомунікаційних засобів. Люди з обмеженими фізичними даними часто не мають можливості спілкуватися в Інтернеті, оскільки не всі комп’ютери налаштовані під потреби інвалідів зору чи слуху, і лише невеликий відсоток сайтів обладнаний програмами звукового супроводу текстового чи графічного матеріалів. Як наслідок, створюється ситуація, коли новітні технології не тільки не сприяють повноцінній реалізації будь-якої особистості, а виступають каталізатором для дискримінації окремих груп населення.

Саме висока інформаційна культура повинна стати перешкодою для розповсюдження інформаційної дискримінації. Інформаційна культура особистості формується в процесі соціалізації, як і інші – правова, економічна, екологічна тощо. На свідомому та підсвідомому рівнях відбувається засвоєння певних соціальних ролей та поведінкових моделей. В подальшому доросла людина повинна самостійно розвиватись і переживати становлення як особистість в суспільстві. Тому в особливий спосіб акцентуємо увагу на окремих загрозах, які особливо актуальні на початкових етапах соціалізації. Відбувається помітна уніфікація масової свідомості, оскільки люди “споживають” одні й ті ж інформаційні продукти глобального характеру (новини, реклама, художні твори і т.д.), йде масова пропаганда способу життя, притаманного цивілізації технологічно розвинених країн. Особливо значним є вплив механізму “глобалізації масової свідомості” на дітей та молодь. Втрачається національна ідентичність, відбувається деградація мови, нівелюються морально-етичні принципи, що не може не впливати на правову свідомість. Інформаційний простір зараз актуалізує багато латентних явищ. Так є, наприклад, з мовою ворожнечі. Єдиного визначення, закріпленого в національному чи міжнародному праві не існує. У різних міжнародних документах в різний спосіб згадується про поняття «hate speech» (у перекладі українською — «мова ворожнечі» або «мова ненависті»). Мова ворожнечі є виявом дискримінації, що виражається в дискримінаційне, некоректне висловлювання до окремих груп чи спільнот або до окремих людей як представників цих спільнот за різними ознаками — етнічною, расовою, національною, віросповіданням, статтю тощо. Як правило, такі висловлювання не просто ображають, а підбурюють до расової ненависті, ксенофобії (страх усього чужого, несвого), антисемітизму (неприязне ставлення до євреїв), гомофобії (страх людей із гомосексуальною орієнтацією), сексизму (зневажливе ставлення до жінки, чоловіка) тощо.

В публічному просторі ця тема все більш наголошується, зокрема й завдяки активній і видимій просвітницькій роботі, яку провадять правозахисники у сфері протидії дискримінації. Наприклад, шляхом розміщення рекламних сітілайтів у великих місах на тему різних проявів дискримінації, одним із яких є мова ворожнечі, вручення символічної премії «Дискримінатор р.». Мова ворожнечі — це інструмент маніпуляцій із метою розколу суспільства, це елемент його дестабілізації й зменшення довіри. І найбільшою помилкою тут може бути якраз недооцінювання негативного впливу таких явищ і проявів агресії на суспільну свідомість. У світлі цього окремо варто виділити питання відповідальності за поширення мови ненависті в публічному інформаційному просторі, точніше, її відсутності.

Для прикладу, німецький парламент нещодавно обговорював закон проти ненависті та цькування в соцмережах. Цей закон було подано на розгляд міністром юстиції Німеччини, який, з одного боку, він пропонує, щоби слова, вислови, заклики до цькування, якісь маркери ненависті блокувалися, й зобов’язує «Фейсбук» та інші соціальні мережі видаляти такі коментарі протягом 24 годин. У випадках, коли не можна чітко визначити порушення одразу, пропонується сім днів на ухвалення відповідного рішення. Якщо ж адміністрація соцмереж цього не зробить — пропонуються штрафи. Особливого значення набуває питання мови ворожнечі в умовах інформаційної війни.

Існує водночас і критика концепції узаконення відповідальності за мову ворожнечі. Мова ворожнечі як категорія тісно пов’язана з радикальним лібералізмом. Він впроваджується цілком систематично: на рівні державної політики, через широку мережу добре фінансованих громадських організацій, за активної підтримки ЗМІ, зі своєю мовою та системою координат, зі своєю цензурою. Сама по собі цензура є необхідним елементом суспільного життя. Нам дуже важко уявити суспільство, де існувала б абсолютна свобода слова. За адекватних умов цензура має наметі захист суспільного блага, а також універсальних моральних принципів. Прихильники цієї концепції, вважають «Hate speech» універсальним ярликом, за допомогою якого можна затаврувати думки, що суперечать догмам лібералізму. Руйнівне значення концепції “мови Щорічна антипремія «Дискримінатор року» вручається у трьох номінаціях: «Дискримінація «у законі», «Реально Г (ганебний вчинок)» та «Язик мій – ворог мій». В останній номінації 2016 року «переміг» народний депутат Антон Геращенко за коментар в одному з видань щодо нардепа Надії Савченко: він публічно порадив їй вийти заміж і займатися дітьми, а не політикою ворожнечі” не можна зводити виключно до того, що ця концепція має на меті заборонити називати речі своїми іменами. Засудження “мови ворожнечі” має сугестивну дію. Воно покликане паралізувати нашу здатність до адекватного етичного мислення.

До основних факторів інформаційно-психологічного ризику, що властиві самій людині, відносять: 1) незрілість особистості, що виражається в нездатності до самостійного, свідомого вибору інформації, релевантної своїм змінам, переконанням і планам; 2) установки особистості на конформізм, імітаторство, на готовність до сприйняття маніпулятивних інформаційних впливів; 3) негативні зміни функціонального стану головного мозку і психіки; 4) стан соціуму, що сприяє підвищеній сугестивності, масовому зараженню ідеями, закликами, що може бути спровокований на психофізіологічному рівні хронічним або гострим психоемоційним стресом, фрустрацією, тривожністю.

Таким чином, не можна залишити поза увагою ще одну загрозу – низький рівень інформаційної і правової культури, який породжує еклектизм як панівну ознаку інформаційної “культури мас”. В найширшому значенні еклектизм означає механічне поєднання в одному вченні різнорідних, органічно несумісних елементів, які запозичуються з протилежних концепцій. Низький рівень інформаційної культури за умов надміру інформації породжує, як наслідок, порушення цілісності особистості, знижує її спроможність критично сприймати, аналізувати, оцінювати отриману інформацію і формувати власну позицію.

Підтримуємо думку професора Арістової І.В.: “Хоча інформація є дійсно інструментом знання, але сама по собі вона не є знанням. Інформація, яка виникла із бажання обмінюватися знаннями та зробила більш ефективною їх передачу, залишається лише формою знання, точною й стабілізованою, індексованою за часом та користувачем. Інформація, навіть якщо вона може бути “покращена”, не обов’язково має правильне усвідомлення”.

Окрему категорію загроз становлять ті, що виникають зв’язку з використанням соцмереж та комунікаторів. Соцмережі містять величезну кількість інформації про особу, яку вона розмістила там особисто і добровільно, при цьому помилково вважаючи, що ця інформація надійно захищена паролем.Зловмисники активно крадуть паролі та логіни до соціальних мереж, які, за даними експертів «Лабораторії Касперського», на чорному ринку коштують усього близько 5 доларів США. Низький рівень інформаційної і правової культури населення дозволяють зловмисникам використовувати для отримання персональних даних різноманітні квести («Перевір своє знання географії», «Який у тебе словниковий запас», «Визнач свій психотип», «Як ти будеш виглядати через 50 років», «На якого звіра ти подібний», «Яка машина тобі личить» тощо). Для користування подібними ресурсами людина «логіниться» за допомогою власного аккаунта в соцмережі і надає згоду на використання інформації, що міститься у ньому. Так, «безневинні», на перший погляд, розваги, дозволяють легально стежити за особою – отримувати інформацію про її вподобання, геолокацію, друзів, активність тощо.

Німецькі правозахисники у галузі захисту приватності інформації вимагали видалити кнопку «Like» від адміністрації соцмережі Facebook, яка дозволяє користувачам оцінювати інформацію на сайті в режимі онлайн. Вони заявили, що її використання суперечить німецькому та європейському законодавству, оскільки таким чином персональна інформація про користувачів – інтереси, тривалість перебування на тій чи іншій сторінці, переходи з одного сайту на інший надходить до США, де згодом використовується для таргетування реклами, аналізу поведінки користувачів на сайті тощо. Представники соціальної мережі підтвердили, що, натискаючи цю кнопку, така інформація як IP-адреси, могла передаватися. Вони також зазначили, що ці дані, відповідно до європейського законодавства через 90 днів видаляються.

Окремо варто звернути увагу на системи візуального розпізнавання. Спеціальна програма аналізує фотографії і пропонує користувачеві різні варіанти імен того чи іншого знайомого. Ця система успішно впроваджена в США, у тому числі відповідна програма написана для мобільних пристроїв Apple і призначена для поліції. Поліція англійського графства Лестершир в 2014 також вперше в Британії стала використовувати систему NeoFace, яка дозволила порівнювати особу підозрюваного з наявною у поліції картотекою в 92 тисячі осіб. Як видається, нові технології можуть допомагати швидше і легше ідентифікувати злочинців, адже зафіксовані на камеру спостереження кадри можна порівняти з базами біометричних даних, про які йшлося раніше.

Facebook, так само, як Google, заявляють, що збір даних здійснюється в інтересах суспільства. По-перше, тому що вони показують реклами, і тому хочуть, щоб вона відповідала зацікавленням для людей. По-друге, іноді завдяки мережам правоохоронці мають більше можливостей у боротьбі зі злочинністю. Проте, як свідчить практика останніх місяців, і історія з передачею даних Cambridge Analytica, володіючи метаданими користувачів та мільйонів інших людей, які можуть бути об'єднані і проаналізовані за допомогою технологій Big Data, Фейсбук має і отже використовувати неконтрольовано безпрецедентний обсяг інформації щодо сучасних користувачів технології. Але збирання інформації і переслідування завдяки соціальним мережам є можливим не лише для поліції, комерційним організаціям, а й самим користувачам, які не завжди використовують його в законних цілях. Кібербуллінг і кібермоббінг, а також розшук лінчування правопорушників за допомогою соцмереж набувають все більшого поширення. Спільним знаменником для них є не лише використання інтернету і соцмереж з метою переслідування конкретної особи чи групи осіб, але й складність притягнення винних до відповідальності.

У первинному розумінні моббінгом вважався систематичний прояв ворожості, знущання та дискримінації на робочому місці, як з боку колег, так і зі сторони керівництва. Проте з часом ця категорія поширилась на будь-яке систематичне, повторюване протягом тривалого часу цькування, образу, приниження гідності іншої людини, наприклад, у школі, на робочому місці, у в'язниці, і через Інтернет (кібермоббінг).

Кібер-буллінґ (cyber-bullying), віртуальний терор, (від англійського слова bull – бик) із спорідненими значеннями: агресивно нападати, роз’ятрювати, задирати, прискіпуватися, провокувати, дошкуляти, тероризувати, цькувати. В українському молодіжному сленгу є дієслово аналогічного походження – «бикувати». Кібер-буллінґ часто плутають із моббінґом, або масовим цькуванням (від mob – натовп), хоча насправді агресивна поведінка, яка позначається цими двома поняттями, має різні соціально-психологічні механізми.

Ззовні і один, і другий виглядають приблизно однаково - це напади з метою завдання психологічної шкоди, а також шкоди репутації особи, які здійснюються через електронну пошту, сервіси миттєвих повідомлень, у чатах, соціальних мережах, на web-сайтах, а також за допомогою мобільного зв’язку. Така багаторазово повторювана агресивна поведінка має на меті зашкодити людині і базується на дисбалансі влади (фізичної сили, соціального статусу в групі).

Американські дослідники Р.Ковальскі, С. Лімбер і П. Агатстон виокремлюють такі основні типи поведінки властиві для кібербуллінґу:

1. Перепалки, або флеймінґ – обмін короткими запальними репліками між двома та більше людьми, що розгортається зазвичай у публічних місцях Мережі. Інколи перетворюється на затяжний конфлікт (holywar – священна війна). На перший погляд, флеймінґ – боротьба між рівними, але за певних умов вона може перетворитися на нерівноправний психологічний терор. Несподіваний випад може привести жертву до сильних емоційних переживань.

2. Нападки, постійні виснажливі атаки (harassment) – повторювані образливі повідомлення, спрямовані на жертву (наприклад, сотні sms на мобільний телефон, постійні дзвінки), з перевантаженням персональних каналів комунікації. Трапляються також у чатах і форумах, а в онлайн-іграх цю технологію найчастіше використовують ґрифери (grieffers) – група гравців, що мають на меті не перемогу, а руйнацію ігрового досвіду інших учасників.

3. Наклепи (denigration) – поширення принизливої неправдивої інформації. Текстові повідомлення, фото, пісні, які часто мають сексуальний характер. Жертвами можуть бути не лише окремі підлітки – часом трапляються розсилки списків («хто є хто в школі», «хто з ким спить»), створюються спеціальні «книги для критики» (slam books) із жартами про однокласників.

4. Самозванство, втілення в певну особу (impersonation) – переслідувач позиціонує себе як жертву, використовуючи її пароль доступу до аккаунту в соціальних мережах, у блозі, пошті, системі миттєвих повідомлень, або ж створює свій аккаунт із аналогічним нікнеймом та здійснює від імені жертви негативну комунікацію. Організація «хвилі зворотних зв’язків» відбувається, коли з адреси жертви без її відома відправляють друзям провокаційні листи.

5. Ошуканство, видурювання конфіденційної інформації та її розповсюдження (outing & trickery) – отримання персональної інформації і публікація її в інтернеті або передавання тим, кому вона не призначалася.

6. Відчуження (остракізм, ізоляція). Будь-якій людині притаманне бажання бути включеним у групу. Виключення ж із групи сприймається як соціальна смерть. Що більшою мірою людина виключається із взаємодії, то гірше вона почувається, й то більше падає її самооцінка. У віртуальному середовищі це може призвести до повного емоційного руйнування дитини. Онлайн-відчуження можливе в будь-яких типах середовищ, де використовується захист паролями, формується список небажаної пошти або список друзів. Кібер-остракізм проявляється також через відсутність відповіді на миттєві повідомлення чи електронні листи.

7. Кіберпереслідування – приховане вистежування жертви з метою організації нападу, побиття, зґвалтування тощо.

8. Хепіслепінґ (від англ. slap – ляпас) – назва походить від випадків в Лондонському метро, коли хулігани били випадкових перехожих заради сміху і підняття власного статусу, записуючи це на камеру мобільного телефону. Зараз так називають будь-які відеоролики із записами реальних сцен насильства, які після розміщуються в інтернеті без згоди жертви.

Бесіди з київськими підлітками підтверджують наявність більшості описаних типів поведінки в їхньому досвіді чи уявленнях. Навіть хепіслепінґ, який виник відносно нещодавно, трапляється серед українських дітей.

Відмінності кібер-буллінґу від традиційного реального зумовлені особливостями інтернет-середовища: анонімністю, можливістю сфальшування, наявністю величезної аудиторії, можливістю дістати жертву будь-де і будь-коли. На відміну від реального цькування, для кібер-буллінґу не потрібні м’язи чи високий зріст, а лише технічні засоби, час і бажання когось тероризувати. Хоча основною категорією ризику кібербулінгу є підлітки і молодь, проте трапляються і подібні випадки серед дорослих. Так, 31-річну жінку засудили до позбавлення волі за доведення до самогубства через соцмережу. Вона реєструвалася під різними іменами і публікувала на сторінці колишнього хлопця і сторінках його знайомих інформацію про його нетрадиційну сексуальну орієнтацію. Він не витримав цькування і покінчив життя самогубством.

Кібермобінг, на думку деяких дослідників, має «ширшу аудиторію» як серед жертв, так і серед переслідувачів. Хоча його види, які виділила N. E. Willard у праці «CyberbullyingandCyberthreats: RespondingtotheChallengeofOnlineSocialAggression, Threats, andDistress» є майже повністю подібні: flaming – образа, що має місце у публічному інтернет-просторі, за допомогою образливих коментарів, вульгарних звернень; harassment – цілеспрямовані, систематичні кібератаки від незнайомих людей, користувачів соціальних мереж, а також від людей з найближчого реального соціального оточення; denigration – навмисне очорнення, поширення чуток за допомогою публікації фото- або відеоматеріалів на інтернет-сторінках, форумах, в групах, через електронну пошту; impersonation – використання фіктивного імені для доступу до ресурсів від імені жертви, наприклад з метою зіпсувати її репутацію; outing and trickery – поширення особистої інформації, наприклад, інтимних фотографій, фінансового стану, роду діяльності з метою образити або шантажувати, наприклад, екс-партнера; exclusion - соціальна ізоляція, відмова спілкуватися (як на діловому, так і на неформальному рівні), що реалізується через видалення з друзів, груп тощо; cyberstalking - cистематичне переслідування за допомогою використання електронних засобів, у тому числі інтернету; може поєднувати погрози, заклики до сексу, фальшиві звинувачення, наклепи, крадіжку ідентичності та вандалізм; часто використовується в поєднанні з реальним переслідуванням, оскільки обидва є вираженням бажання контролювати, залякувати або маніпулювати жертвою; сyberthreats – погрози фізичної розправи вбивства або заподіяння тілесних ушкоджень.

Польські дослідники, поєднуючи обидва типи під поняттям «agresja elektroniczna» (електронна агрессія) виокремлюють такі типи жертв: 1) жертва, для яких характерною особливістю є нерівність «сил» жертви і нападника, тобто коли жертва слабша; 2) знаменитості (селебріті), де знаменитістю вважається людина, що часто згадується в медіа і викликає громадський інтерес, незалежно від професії чи роду діяльності; 3) особи, що приналежать до певної групи (ang. bias bullying), об’єднаної спільними цінностями, такими раси, етнічної приналежності, сексуальної орієнтації, релігії, віку, сімейного статусу, фізичної або психічної неповносправності і ін.; 4) випадкові жертви, незнайомці «яким непощастило»; 5) електронне хуліганство, коли правопорушник і жертва, як правило, є членами однієї і тієї ж групи, як онлайн і в реальному житті.

Варто нагадати справу М. Майєр. У 2006 р. в маленькому американському містечку посварилися дві 13-річні школярки - Меган Майєр і Сара Дрю. Мати однієї з дівчаток сприйняла цю сварку близько до серця і вирішила встановити стеження за колишньою подругою дочки. Вона не стала наймати для цього приватних детективів, а просто створила в соціальній мережі MySpace аккаунт від імені симпатичного 16-річного хлопця на ім'я Джош Ивенс, який втерся в довіру до простодушної Меган Майєр і незабаром завів з нею роман. Лорі писала від імені Джоша втрьох з 13-річною Сарою і зі своєю молодою підпорядкованої на роботі Ешлі Гріллс. Одного дня міфічний Джош, який зумів до того моменту підкорити серце провінційної школярки, раптом почав її всіляко ображати, принижувати і прямо порадив дівчинці позбавити світ від своєї присутності. У той же день Меган Майєр наклала на себе руки, повісившись у шафі. І ФБР, розслідуючи обставини її самогубства, відразу вийшло на слід віртуального Джоша Івенса, чия порада призвела до загибелі дівчинки. Присяжні, під впливом природніх людських почуттів, визнали її винною за трьома пунктами пред'явленого їй звинувачення. А федеральний суддя, керуючись буквою закону, скасував їх вердикт, звільнивши Лорі Дрю від будь-якої відповідальності за вчинене. Лорі Дрю звинуватили в несанкціонованому доступі до комп'ютерних мереж на тій підставі, що вона зареєструвалася в MySpace, використовуючи вигадане ім'я, і, тим самим порушила правила використання цієї соцмережі.

Покарання за кожним з трьох пунктів звинувачення могло скласти до трьох років в'язниці і штраф до 300 000 доларів. Але ні американські юридичні експерти, ні професійний суддя не могли погодитися з подібним трактуванням «несанкціонованого доступу».

Відповіддю на цю колізію став внесений до Конгресу США законопроект HR1966, що передбачає відповідальність за «кіберцькування» (cyberbullying). Перспективи його прийняття в нинішньому вигляді вельми сумнівні: визначити межу між злочинним «цькуванням» і свободою висловлювання для американського законодавця ніколи не було легким завданням. А навіть якщо і приймуть такий закон, проблему, що спонукала до його створення, він все одно не вирішить. Кількість загроз інформаційні безпеці буде зростати і надалі, з огляду на поширенню інформаційних технологій у всіх сферах життєдіяльності людини і збільшенню їх впливу. В першу чергу, їх розвиток відбувається в комерційних цілях. Так було з Big Data, штучним інтелектом, інтернетом речей. В США з 1 серпня 2017 р. вже почалося чіпування людей. Американська компанія Three Square Market імплантує співробітникам чіпи розміром з рисове зернятко між великим і вказівним пальцями. З його допомогою люди можуть входити в офіс або платити за їжу. 50 із 80 працівників добровільно погодились на чіпування. «Компанії часто стверджують, що ці чіпи безпечні і зашифровані. Але "зашифрований" - досить розмитий термін. Незрозуміло, чи дійсно це безпечно, або все ж цей пристрій можуть зламати», - каже А. Аккісті, професор інформаційних технологій і державної політики в Університеті Карнегі-Меллон. Ще одна потенційна проблема, за словами Аккісті, полягає в тому, що технологія, розроблена для однієї мети, пізніше може бути використана для іншої. Мікрочіп, імплантований сьогодні, щоб забезпечити прохід до будівлі або платежі, пізніше теоретично може бути використаний інакше. Наприклад, можна відстежувати тривалість обідніх перерв співробітників без їх згоди або в іншій спосіб втручатись у їх приватне життя.

Ще одним суперечливим питанням є використання чат-ботів. Чат-боти – це програми, які здатні імітувати спілкування користувача з одним або декількома співрозмовниками. Як правило, вони створюються на базі таких додатків, як Telegram, FB, Messenger, Skype, Viber і ін. Для впровадження інновацій, таких як використання чат-бота, добре підходить сфера послуг - страхові, медичні, комунальні, банківські, транспорт, зв’язок, туризм, ресторанний бізнес і, навіть, юридичні послуги. Швидкість і простота виконання сценаріїв, як замовлення послуг, консультування з типових питань, претензії тощо дозволяє залучати нових клієнтів за рахунок підвищення якості обслуговування вже існуючих. В Україні юристи-боти в основному представлені в двох видах: у вигляді спливаючих вікон на сайтах, прямо або побічно пов'язаних з юридичною практикою, і у вигляді спеціальних сервісів або розділів сервісів (наприклад, юрист-бот в сервісі Telegram). По суті, юрист-бот є чат-ботом – набором алгоритмів, що обробляють ваш запит, а потім, шляхом пошуку по зовнішніх ресурсах, що видає найкращий за критеріями конкретного бота відповідь.

Бот постійно вдосконалюється. В 2015 р. компанія Microsoft впровадила технології, створені для визначення по міміці особи таких основних емоцій як гнів, щастя, апатія, здивування, байдужість, вказуючи їх у процентних співвідношеннях.

В 2017 р. вчені з Массачусетського технологічного інституту розробили алгоритм для аналізу твітів, який може визначати сарказм і емоційний підтекст. Визначення настрою в соціальних мережах корисно для відстеження відношення до брендам і продуктам, а також для виявлення тенденцій на фінансових ринках. Але більш точне розпізнавання сенсу твітів може допомогти комп'ютерам автоматично виявляти і контролювати емоції.

Спочатку дослідники хотіли розробити систему, здатну виявляти расистські повідомлення в Твіттері. Але незабаром вони зрозуміли, що сенс багатьох повідомлень не може бути правильно ідентифікований без розуміння сарказму.

Обидві технології використовують глибоке навчання - популярний метод машинного навчання, який базується на навчанні нейронної мережі для розпізнавання тонких патернів з використанням великої кількості даних.

Яким чином ці технології вплинуть на людство? Будь-яка технологія може бути використана в обидві сторони. К. Лоренц писав про « вагомі підстави вважати внутрішньовидову агресію найбільш серйозною небезпекою, яка загрожує людству в сучасних умовах культурно-історичного і технічного розвитку».

Не можливо надати вичерпний перелік інформаційних загроз людині, оскільки вони модифікують з розвитком інформаційних технологій і самого суспільства. Основна частина розглянутих була спрямована на порушення особистих прав людини. Сховатись від інформаційних загроз або закрити інформаційний простір від зовнішнього інформаційного впливу в жоден спосіб, чи то правовий, чи то технічний неможливо. Інформаційна безпека не зводиться винятково до захисту відомостей і даних.

На основі проведеного дослідження вважаємо за необхідне виокремити такі групи загроз інформаційній безпеці людини в залежності від цінностей, яким вони загрожують:

1) технологічні – випливають із постійного вдосконалення технологій та відставання правового забезпечення їх функціонування, реалізують, здебільшого, як загрози безпеці інформації, проте, можуть прогресувати до загроз інформаційній безпеці;

2) соціально-правові – пов’язані із становищем людини у суспільстві і державі, а також можливістю реалізовувати свої соціальні, культурні, політичні і економічні права і свободи;

3) істотні – пов’язані безпосередньо з фізичною і психічною безпекою людини, що є необхідною умовою її якісної життєдіяльності. Реалізація істотних загроз призводить до порушення найважливіших абсолютних прав і свобод людини – на життя, на здоров’я, тілесну недоторканість, повагу людської гідності, недоторканість приватного життя тощо.

Свобода, яка є найважливішою умовою буття людини, обумовлює необхідність гарантування інформаційної безпеки людини. Загрози інформаційній безпеці людини є складним ієрархічним утворенням з множиною різнорівневих зв’язків, їх вплив на людину комплексний і різноманітний. Тому запропонований поділ є певною мірою умовний.

В умовах інформаційного суспільства можливості реалізації прав і свобод людини суттєво залежать від адаптованості до них самої особи, інститутів суспільства і держави, а також системи права. Необхідною складовою такої адаптації і умовою реалізації і захисту прав і свобод людини є високий ступінь інформаційної та правової культури.

Особливої уваги вимагає дослідження загроз, які існують на початкових етапах соціалізації особистості, оскільки на цьому етапі формується інформаційна культура людини, яка в подальшому дозволить (або не дозволить) ефективно протистояти інформаційним загрозам, викликам та ризикам, а також використовувати можливості, які створює інформаційне суспільство.

Оскільки інформаційна безпека людини базується не лише на її захищеностівід інформаційних загроз, але й передбачає можливість людини як біологічногоорганізму і соціальної істоти функціонувати, розвиватись і досягати бажаних длясебе результатів в інформаційному суспільстві. Сучасні міжнародно-правові актипередбачають обов’язок держав створити рівні можливості для захисту своїх правонлайн в тій самій мірі, що і в реальному просторі. Комітет Міністрів РадиЄвропи в Рекомендації СМ/Rес (2014)6 зазначає, що існуючі права людинита основні свободи в рівній мірі відносяться як до оффлайн, так і до онлайнпростору. Ніхто не повинен бути об’єктом незаконного втручання в здійсненняправ людини та основних свобод під час перебування в інтернеті.

Швидкі темпи поширення і популярність інтернету пояснюютьсясвітоглядними установками інформаційного суспільства. Інтернет відповідаєціннісним очікуванням сучасної людини: доступність, необмеженість,варіативність, тиражування, оперативність. При цьому різні категорії осібзнаходяться у неоднакових умовах щодо можливості реалізації своїх прав і свободв інформаційній сфері, зокрема, відрізняється ступінь захищеності вінформаційному суспільстві, види і інтенсивність небезпек, що їм загрожують.

Серед об’єктів інформаційної безпеки можна виокремити категорії, щохарактеризуються наявністю спільних інформаційних загроз їх безпеці інеобхідністю особливого правового забезпечення. Зокрема, в цьому дослідженніспробуємо звернути увагу на наступні:

1) окремі вікові групи: насамперед, діти, підлітки і молодь, а також людипохилого віку;

2) люди з обмеженими фізичними можливостями, особливостямиінтелектуального розвитку та психічними порушеннями,

3) люди, що здійснюють діяльність, яка має або може мати важливі соціальнінаслідки – державні службовці, медійні особи та журналісти, правозахисники,громадські активісти і політичні діячі тощо;

4) населення окремих регіонів країни чи населених пунктів, що володієспецифічними соціокультурними особливостями, в т.ч. релігійними, етнічними,мовними, демографічними;

5) люди, що пов’язані з військовими діями на сході України –військовослужбовці, їх сім’ї, а також сім’ї загиблих, населення окупованихтериторій, «сірої» зони, внутрішньо переміщені особи тощо.

Цей перелік не є вичерпним, його метою є окреслення межі предметудослідження.

**Діти, підлітки і молодь.** За даними досліджень 2011 р. в США близько 80%дітей у віці до 5 років користувались інтернетом щотижня, більшість дітейпроводило принаймні три години на день, дивлячись телевізор, а час загаломвитрачений на медіа дітьми дошкільного віку становив 47%. Також зазначається,що 36% дітей у віці від 2 до 11 років одночасно використовують обидва засоби.Загалом, діти у віці від 8 до 10 років щодня проводять близько 5,5 годинвикористовуючи носій.

Використання домашнього інтернету зростає з віком. Кожен з трьох дітейвіком від трьох до п'яти років використовує інтернет вдома, у порівнянні з 54% 6-11-річних та 72 % з 12-17-річних. Компанія, що пропонує онлайн послуги щодозахисту дітей від небажаного вмісту мережі «Guardchild» наводить на своїйсторінці результати багатьох досліджень наукових установ і соціальнихінституцій США: 21% дітей дошкільного віку мають доступ до стільниковихтелефонів, 90% дітей у віці 8-16 років бачили онлайн порнографію, 70% дітейвіком від 7 до 18 років виконуючи домашнє завдання натикалися на порнографіюв мережі, 31% підлітків у віці 12-18 років завідомо неправильно вказали свій вік,щоб отримати доступ до сайтів з віковими обмеженнями, 95% батьків незнають/не розуміють онлайн сленгу чи скорочень, що використовують їх діти,кожен п’ятий з підлітків у віці отримував повідомлення з пропозиціямисексуального характеру, а 1 з 33 – були переслідуваними в мережі, 65% 8-14річних були втягнені в кібербуллінг19, 69% підлітків регулярно отримуючиповідомлення від незнайомих людей не повідомляють про це батькам чи опікунам.

Відповідні актуальні статистичні дані щодо України виявилось знайти доситьскладно. Всеукраїнське соціологічне дослідження, проведене Інститутомсоціології НАН України в 2009 р., виявило тривожні тенденції: понад 28%опитуваних дітей готові надіслати свої фотокартки незнайомцям у Мережі; 17%без коливань діляться інформацією про себе і свою родину (адреса, професія,графік роботи батьків, наявність цінних речей у домі тощо); 22% дітей періодичнопотрапляють на сайти для дорослих; 28% дітей, побачивши в інтернеті рекламуалкоголю або куріння, хоча б один раз спробували їх купити, а 11% − спробуваликупувати наркотики; близько 14% опитуваних час від часу відправляють платніSMS за бонуси в онлайн-іграх і лише деякі звертають увагу на вартість послуги. Лише у 18% випадків дорослі перевіряють, які сайти відвідує дитина, тільки 11% батьків знають про такі онлайн-загрози, як “дорослий” контент, азартні ігри, онлайн-насилля, кіберзлочинність.

Комітет ООН з прав дитини у 2011 р. відзначив, що відвідування порнографічних сайтів становило 70% усього трафіку на території України, а 5 млн. українських користувачів на місяць цікавляться дитячою порнографією Департамент молоді Ради Європи у 2012 р. провів онлайн-опитування щододосвіду молоді, пов’язаного з мовою ворожнечі в інтернеті. За його результатами69% не знають, де можна отримати допомогу жертві мови ворожнечі онлайн, 78%респондентів не отримували освіти щодо безпечної поведінки в інтернеті. Заданими міжнародної асоціації «INHOPE», видалення матеріалів сексуальногозловживання над дітьми в інтернеті допомагає попередити їх подальшеперетворення в жертву злочинних посягань. Профайл жертв розміщенняматеріалів сексуального характеру у 2014 р. виглядав таким чином: юнацтво –21% (у 81% випадках жертвами стають дівчата), підлітки – 72% (у 13% випадківжертвами стають хлопці діти), 7% (у 6% випадків – діти обох статей).

Водночас, незалежно від країни чи частини світу діти і молодь вважаютьінтернет невід’ємною частиною свого життя, благом, навіть якщо воно дороге,недостовірне або доступне лише за допомогою спільних пристроїв (як наприкладу деяких країнах Африки). Всесвітнє опитування показує, що діти вважають йогоправом людини, необхідністю. З урахуванням віку діти та молодь маютьправо на особливий захист і консультування при користуванні інтернетом. «Цеозначає, що: 1. право на вільне вираження своїх поглядів та участь у життісуспільства, на те, щоб бути почутими та вносити свій вклад у вирішення питань. Поглядам повинна приділятися належна увага з урахуванням вашого віку, ступеня зрілості та без дискримінації; 2. можливість очікувати на отримання інформації мовою, що відповідає віку, а також на навчання безпечному користуванню інтернетом, в тому числі щодо захисту вашого приватного життя, з боку вчителів, вихователів, батьків чи опікунів; 3. обов’язок знати, що контент, який створюєте в інтернеті, або контент про дитину, що створюється іншими інтернет-користувачами, може ставати доступним у будь-якому куточку світу і завдавати шкоду гідності, безпеці, приватному життю або іншим чином шкодити особі та її правам у цей час або на наступних етапах життя. На запит такий контент повиненбути вилучений або видалений протягом розумно короткого періоду часу; 4.можливість очікувати на отримання чіткої інформації про те, який онлайн-контент та поведінка є незаконними (наприклад, домагання в інтернеті), а такожмати можливість повідомити про потенційно незаконний контент. Такаінформація має бути адаптована до віку та обставин, а також повинні надаватисьпоради та підтримка з належною повагою до конфіденційності та анонімності; 5.повинен надаватися спеціальний захист від втручання у фізичне, психічне таморальне благополуччя, зокрема, захист від сексуальної експлуатації танасильства в інтернеті та від інших форм кіберзлочинності. Крім того, право наосвіту, яка покликане захистити від подібних загроз».

Таким чином, виникає суперечлива ситуація. З одного боку, права дитини надоступ до інформації, на вільний розвиток, персональні дані тощо, з іншого –необхідність забезпечити захист від кіберзагроз та інформаційну безпеку дитини,в цілому. Хто і якою мірою має за це нести відповідальність? Англійськадослідниця С. Лівінгстон, підкреслюючи, що один з трьох користувачівінтернету є дитиною, наголошує, що із зростанням технологій дитячі організації,представники приватного сектору, регулюючі органи мають опікуватись тим, щоправа дітей потребують такої ж реалізації онлайн, як і оффлайн. Права дитини,викладені в Конвенції ООН прав дитини, дослідниця застосовує до онлайнсередовища.

Серед загроз з якими дитина зіткнутись при використанні комунікаційнихтехнологій можна виокремити такі: технологічні: загроза як для дітей, так і длядорослих користувачів; доступ до інформації з неприйнятним (часто незаконним)змістом, зокрема, порнографічні, такі, що пропагують наркотики, психотропніречовини й алкоголь, тероризм і екстремізм, ксенофобію,сектантство,національну, класову, соціальну нетерпимість, нерівність, асоціальнуповедінку, насилля, агресію, суїцид, азартні ігри, інтернет-шахрайство,розголошення персональних даних та іншої конфіденційної інформації, яквласної, так і членів сім’ї, друзів чи знайомих, контакт з незнайомцями, що можепризвести наслідків як у віртуальному (кібербулінг, дитяча порнографія тощо),так і реальному житті (сексуальне використання, фізичні ушкодження,викрадення).

Не слід залишати поза увагою те, що інформаційна безпека, це не лишекібербезпека і не обмежується безпечним перебуванням у віртуальному просторі.Реалізація численних прав і свобод дитини в сучасному суспільстві залежить відгарантування дотримання її інформаційних прав. Зокрема, це стосується права нарівень життя, необхідний для їх розвитку, права дітей на вираження своїхпоглядів, право на існування власного майна, на свободу думки, совісті і релігії,асоціацій і мирних зборів, доступ дитини до поширення інформації, освіту,користування рідною мовою і культурою, сповідування своєї релігії, відпочинок ідозвілля.

Чи можливим є регулювання взаємодії між медіа і дітьми? Протягом другоїполовини століття телебачення суворо звинувачувалося в поширенні багатьохсоціальних хвороб, тепер цей акцент перенесено на інтернет. Сучасні медіапереважно знаходяться в комерційному використанні, а отже основнимрегулюючим фактором є фінансовий. Ресурси, які раніше були призначенівиключно для дорослих, тепер часто є доступними дітям.Глобалізаційні процеси впершу чергу в мережевому просторі дозволяютьуникати регулювання національним законодавством. Подібною є ситуація щодотелебачення і радіомовлення. Оскільки аудіовізуальні технології спрямовані насумісність з новими медіа, національні регулятори стикаються з практичнонереальними для вирішення завданнями - класифікації, обмеження абопланування всього того, що з'являється на екранах країни, а тим більш не маютьможливості впливу на споживачів. Виходячи із специфіки дитячого віку, слідсказати, що у профілактичній роботі з даною групою велике значення мають,насамперед, заходи не правового характеру, а педагогічні, психологічні, медичні. Дослідження свідчать, що з точки зору батьків, ті фактори, які ускладнюють державне регулювання нового медіа-оточення, тягнуть за собою аналогічні складності і для батьків. Батькам було складно відстежувати і впливати назміст того, що переглядали їхні діти вдома чи у своїх друзів в епоху телебачення.Тим більш, це завдання ускладнилось в епоху інтернету і портативних технологій(«гаджетів»). Таким чином, визначення змісту контенту, що споживають діти,виходить за межі можливостей батьківського контролю. Крім цього, як свідчатьзнову таки дослідження, значна кількість батьків не до кінця розуміють сенскомп'ютерних ігор та сторінок в інтернеті, якими користуються їхні діти.

На сторінці Майкрософт розміщені правила безпечного користуванняінтернетом. «Оскільки дорослі самостійно вирішують, який рівеньконфіденційності потрібно забезпечити дітям, цей список рекомендацій міститьорієнтовні правила користування комп’ютером, зокрема: відстежуйтевикористання інтернету; попросіть дітей ніколи не надавати особисті відомості,як-от ім’я, місцезнаходження, зображення, паролі, номери телефонів тощо;використовуйте програмне забезпечення для батьківського контролю; дозволяйтедітям переписуватися та спілкуватися лише з тими людьми, яких ви знаєте;розмовляйте з дітьми про незручні або неприємні ситуації в інтернеті; розкажітьдітям, що не слід відповідати на неочікувані або небажані повідомленняелектронної пошти; пам’ятайте про те, що практично нічого в інтернеті не єповністю приватним».

Існує думка, оскільки «інтернет здебільшого є продуктом приватнихкомпаній, то реалізація та порушення прав людини в інтернеті має трьохстороннійхарактер: людина-приватна компанія (провайдер інтернет-послуг чи інтернет-доступу тощо) -держава». Така позиція, на нашу думку не є однозначною,оскільки гарантування прав і свобод на національному рівні залишаєтьсяобов’язком держави, тому числі створення належного правового і організаційногозабезпечення для їх реалізації. Тоді як зі сторони юридичних і фізичних осібочікуваною і бажаною поведінкою є дотримання існуючих правових норм, непорушення прав інших учасників правовідносин та виконання покладених на нихобов’язків.

Повертаючись до питання щодо інформаційної безпеки дітей та молоді,важливо відзначити необхідність формування належного рівня інформаційноїкультури, в тому числі опанування навичок критичного мислення, культурибезпечної поведінки в інформаційному просторі. Важливим учасником цьогопроцесу є держава, оскільки саме вона через уповноважені органи встановлюєзміст навчальних програм, форми навчання і забезпечує підготовку педагогічнихкадрів.

Водночас аналіз листів МОН та регіональних органів виконавчої влади усфері освіти, зміст яких присвячений проблемам інформаційної безпеки: ЛистиМОН України "Про захист дітей та молоді від негативних інформаційнихвпливів", «Про проведення дня безпечного інтернету», «Про проведення конкурсу«Онляндія в моїй школі» свідчить про їх популістський і декларативний характер.

Основним завданням взаємодії батьків, соціальних інституцій і держави в процесі навчання і виховання підлітків з питань інформаційної безпеки повинно бути формування у них інформаційно-комунікаційних компетентностей щодо користування інтернетом. Зокрема серед таких компетентностей слід виділити: 1. Грамотний і успішний пошук інформації: розпізнавання інформаційних потреб; формулювання питань, що відображають інформаційні потреби; знання про існування багатьох інформаційних джерел; пошук, вибір і оцінка інформаційного джерела; зберігання інформації. 2. Критична оцінка інформації: розуміння змісту інформаційного повідомлення; вибір і оцінювання інформації; прийняття рішення про те, що є фактом, а що точкою зору; вирізнення рекламних текстів. 3. Творення, перетворення і презентація інформаційного змісту: творення нового інформаційного змісту; перетворення знайденого в інтернеті або раніше самостійно створеного інформаційного змісту; презентація нового або перетвореного інформаційного змісту. 4. Правові засади творення й поширення інформаційного змісту: усвідомлення правового й етичного вимірів творення інформації; знання, який інформаційний зміст можна перетворювати відповідно до правових засад; знання своїх прав як творця інформації, розміщеної в інтернеті; усвідомлення різниці між інтернет-комунікацією й спілкуванням поза інтернетом. 5. Емпатія й образотворення: знання про те, що інтернет є просторомспільної комунікації з іншими людьми; виявлення емпатії в мережі; створенняобдуманого й адекватного власного образу. 6. Безпека і приватність: знання прозагрози, пов’язані з перебуванням в інтернеті; уміння запобігти небезпекам вінтернеті; здійснення контролю над інформацією, яка передається іншим;усвідомлення різниці між інтернет-комунікацією й спілкуванням поза інтернетом;застосування гігієнічних засад, пов’язаних з використанням комп’ютера. 7.Участь у соціальних електронних мережах: розпізнання елементів інтернет-культури; активна участь у мережних соціальних спільнотах; ініціативність врозвитку мережних соціальних спільнот, створених для спільних дій.

Важливим є створення умов для співпраці батьків та осіб, що їх замінюють, з відповідними органами, що можуть надавати допомогу у випадку актуалізації загроз інформаційній безпеці дітей. Досвід такої допомоги є різний – від створення відповідних підрозіділів поліції до сприяння громадським організаціям, які забезпечують роботу інфоліній у випадку виникнення загрози (наприклад, при кібербулінгу чи кібермоббінгу), відслідковують дитячу порнографію онлайн і повідомляють уповноважені органи, а також здійснюють просвітницьку роботу як серед дітей та молоді, так і для батьків та осіб, що ними опікуються.

Процес комп’ютеризації шкіл, що відбувається сьогодні, безперечно, є прогресивним явищем, але без відповідної методичної підтримки, без перепідготовки учителів-предметників, без інтеграції комп’ютерних технологій у навчальний процес не буде забезпечено належного їх використання.

Використання технологій мультимедіа при викладання всіх шкільних исциплін дозволить підвищити якість засвоєння знань, а також зростання рівня індивідуалізації навчання, що є особливо важливим для дітей з особливими потребами.

За оцінками Всесвітньої організації охорони здоров’я, понад 1 мільярд людей мають якусь форму інвалідності, а це майже 15% населення світу. В Україніпонад 2 мільйони 800 тисяч людей мають статус інваліда, з них 151 тисяча – діти.

Це 6,1 відсотка до загальної кількості населення. І майже 80 % інвалідів – це людипрацездатного віку. **Особи з обмеженими фізичними можливостями,особливостями інтелектуального розвитку та психічними порушеннями**часто бувають виключені з повноцінного життя, зіштовхуючись з дискримінаціярізних форм, включно з фізичними і соціальними бар’єрами.

Поняття повноправного члена суспільства, яке є результатом соціалізації, маєна увазі, перш за все, визнання членами суспільства іншого як рівного. Інформаційні технології мають значний потенціал для покращення якостіжиття багатьох людей з обмеженими можливостями. Водночас, можуть статибар'єром, для прикладу, якщо сторінка має занадто дрібний шрифт, інформація наній недоступна людям з вадами зору; відсутність написів адаптованих для скрін-рідерів - додатків, які озвучують текст на екрані – стає перешкодою для незрячихлюдей; якщо сторінка не містить транскрипти аудіофайлів – інформаціянедоступна для глухих і слабочуючих людей, це лише найочевидніші перешкоди.

Окрім того, що в суспільстві існує стереотипне мислення і велика проблемапід назвою ейблізм, то ще й категорія «нормальності» викликає поділ натих, хто є «нормальним», і тих, хто «нормальним» не є, - поділ на «ми» і «вони» і,як наслідок, аутгруппову гомогенність.

Дослідниця Енн Гібсон змогла нарахувати як мінімум 26 різних ситуацій,коли можливості людей обмежені і у них виникає потреба в доступному інтернеті,наприклад, «хтось впав і зламав пальці - тепер для навігації в інтернеті він можевикористовувати тільки ліву руку і клавіатуру; хворому на епілепсію, яка інодівикликається яскравими контрастними кольорами, потрібно з обережністювідвідувати сайти з яскравим дизайном; військовослужбовець, що служив наплавучому маяку і, як це трапляється з багатьма, став погано чути на одне вухо -він повертає голову в бік звуку на комп'ютері, але так йому складно бачити екран;а у батьків малих дітей немає фізичних обмеженостей, проте якщо їх більш ніжодин, наприклад близнюки, яким по одному року, і це вже успіх, якщо, колитримаючи когось із них на одній руці, залишається хоча б один вільний палець наіншій руці для навігації по iPad або включення Siri».

У 1999 р. Консорціум Всесвітньої павутини, що займається розробкоюєдиних принципів і стандартів для інтернету, створив список рекомендаційWCAG 1.0 (WebContentAccessibilityGuidelines), спрямований на забезпеченнядоступності ресурсів Всесвітньої павутини для людей з обмеженими фізичнимиможливостями, у 2008 р. вийшла його друга версія рекомендацій WCAG 2.0. Ужовтні 2012 р. WCAG 2.0 була прийнята Міжнародною організацієюстандартизації як Міжнародним стандартом ISO, ISO / IEC 40500: 2012.

Для осіб з обмеженими можливостями доступність - це можливістьвикористовувати продукт або послугу так само ефективно, як це робила биздорова людина. Це означає, що потрібно використовувати принципи дизайну, якізабезпечують доступність продуктів і послуг для більшої кількості людей. Удеяких випадках це неможливо, тому для компенсації можуть використовуватисядопоміжні технології. Якщо це так, поширені технології повинні забезпечуватибезпроблемне програмне або апаратне підключення допоміжного пристрою, як вплані взаємодії, так і в плані портативності даних.

Знов таки, як і будь яка соціальна проблема, можливість реалізації прав ісвобод людини з обмеженими можливостями в інформаційному суспільстві єкомплексною, і її вирішення залежить від співпраці держави, громадянськогосуспільства, бізнес структур, міжнародного співтовариства і самої особи зобмеженими можливостями. При цьому кожному з них відведено власна роль.

Для прикладу, бізнес-група по доступним ІКТ розробила Хартію за доступнимитехнологіями в листопаді 2011 р.. Хартія містить 10 зобов'язань, які повиннідотримуватися корпорації, щоб доступність ІКТ була реалізована у всійорганізації, включаючи відділ кадрів, політики, поінформованість персоналу,зміни на робочих місцях і закупівлі. Першими цю хартію підписали 17 провіднихкомпаній, включаючи Cisco, Fujitsu, Microsoft і Oracle. Держави жзобов’язані створити таке правове поле, в якому були б гарантовані права іможливості осіб з обмеженими можливостями. Як свідчить міжнародний досвід,це можливо реалізувати різними шляхами.

Наступна категорія - люди, що здійснюють діяльність, яка має або можемати важливі соціальні наслідки - є надзвичайно широкою і неоднорідною.

Об’єднати державних службовців, медійних осіб та журналістів, правозахисників,громадських активістів і політичних діячів в одну групу з метою дослідженняособливостей загроз їх інформаційній безпеці спонукало суспільна значимість їхдіяльності. Адже кожен із них є публічною особою, має власну аудиторію, на якучинить інформаційний вплив, а окрім того виконує важливу державну чи/тасуспільну функцію.

На поверхні знаходяться конфлікти між правом публічних осіб наприватність та правом на свободу вираження поглядів, правом на захистперсональних даних і правом доступу до публічної інформації тощо. Ця теманеодноразово досліджувалась в наукових працях, як вітчизняних, так ізарубіжних, існує низка судових прецедентів в національних судах таЄвропейському Суді з прав людини.Питання балансу між правом на свободу вираження поглядів і захистомправа на приватне життя є досить неоднозначним. Нагнічук О. І. на підставіаналізу практики Європейському Суді з прав людини23 формулює принциписпіввідношення права на свободу вираження та права на приватність щодопублічних осіб: 1) будь-яке втручання в приватне життя можливе настільки,наскільки це сприяє публічним дебатам з питань загальної важливості; 2) якщозображення особи, яка вийшла на публічну арену, не містить інформації про їїприватне життя, воно може використовуватися, незважаючи на те, чи є ця особавідомою; 3) особи, які стали публічними не з власного бажання, користуютьсябільшим захистом приватного життя порівняно з іншими публічними особами; 4)публічні особи мають право бути захищеними від поширення пліток про їхнєприватне життя; 5) почуттям родичів і близьких померлої публічної особи можебути спричинено шкоду розголошенням конфіденційної інформації про публічнуособу, але чим більше часу проходить після смерті публічної особи, тим більшесуспільний інтерес в отриманні такої інформації перевищує необхідністьконфіденційності такої інформації; 6) не може бути конфіденційною інформацієюставлення політиків до суспільних явищ; 7) комерційні питання не є сфероюприватного життя публічної особи.

Водночас, право на доступ до інформації, якою володіють органи публічноївлади, є основоположним правом людини, а також гарантією функціонуваннядемократичної держави. Право на доступ до інформації вимагає від держави неутримання від втручання, а активних дій – забезпечення нормативних,організаційних та технічних умов реалізації права на інформацію, у тому числіналежного розгляду запитів на інформацію та оприлюднення в ініціативномупорядку суспільно важливої інформації.

Однак порушення балансу між цими правами призводить до виникненнязагрози основним демократичним цінностям, адже право на доступ до інформаціїє правом інструментальним, тобто таким, що необхідне для реалізації інших праві свобод людини, – без доступу до певної інформації, яка знаходиться в органіввлади чи інших суб'єктів, людина часто не може реалізувати свої інші права(наприклад, на доступ до суду, участь у виборах та в управлінні державнимисправами, на освіту тощо).

Окрім того, діяльність осіб, яка має соціальне значення, створює значнукількість обставин, що стають передумовами для втручання в приватнеспілкування, що здійснюється як санкціоновано – державними уповноваженимиорганами (право ініціювати таку діяльність мають Національна поліція, Державнебюро розслідувань, Служба безпеки України, Служба зовнішньої розвідки,Державна прикордонна служба, Управління державної охорони, Фіскальнаслужба, Національне антикорупційне бюро), так і неправомірно – журналістами,політичними опонентами та бізнес-конкурентами. Згідно ст. 9 Закону України «Про телекомунікації» «охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України. Зняття інформації з телекомунікаційних мереж заборонене, крім випадків,передбачених законом». При цьому на операторів, провайдерівтелекомунікацій покладено зобов'язання вживати відповідно до законодавстватехнічних та організаційних заходів із захисту телекомунікаційних мереж, засобівтелекомунікацій, інформації з обмеженим доступом про організаціютелекомунікаційних мереж та інформації, що передається цими мережами (ч.3ст.9).

Кримінально-процесуальним кодексом України передбачено, що длявтручання у приватне спілкування необхідна ухвала слідчого судді. При цьому підспілкуванням розуміється передання інформації у будь-якій формі від однієїособи до іншої безпосередньо або за допомогою засобів зв’язку будь-якого типу.

Спілкування вважається приватним, якщо інформація передається та зберігається за таких фізичних чи юридичних умов, при яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб. Стаття 258 КПК України визначає різновиди втручання в приватне спілкування є: (1) аудіо-, відеоконтроль особи; (2) арешт, огляд і виїмка кореспонденції; (3) зняття інформації з транспортних телекомунікаційних мереж; (4) зняття інформації з електронних інформаційних систем.

Але навіть, за умови дотримання процедури втручання слід пам’ятати, що зняття такої інформації часто зачіпає права і законні інтереси третіх осіб. Важливими гарантіями захисту прав людини при здійсненні втручання в приватне спілкування є: дотримання принципу законності – як щодо процедури, так і щодо обґрунтованості винесенні суддею відповідної ухвали, надійне і обмежене в часі матеріалів, а також невикористання і негайне знищення матеріалів,що не стосуються справи і порушують права третіх осіб. Прослуховування, фотографування чи відео зйомка є доступними і частовикористовуються в незаконних цілях. Поширеним прикладом останнім часомстало фотографування в парламенті та поширення особистої переписки народнихдепутатів, переважна більшість таких даних не пов’язана з державницькоюдіяльністю депутатів, є їхньою конфіденційною інформацією. Більше того,поширення фотознімків такої переписки також часто шкодить третім особам, якіспілкуються з депутатами, проте не перебувають на державних посадах(наприклад, журналістам, знайомим публічної особи).

Не до кінця врегульованою з точки зору захисту прав третіх осіб залишаєтьсяситуація з оприлюдненням електронних декларацій. Безперечно, схемаелектронного декларування в Україні є важливим кроком у боротьбі з корупцією.Головними завданнями е-декларування є контроль і протидія незаконномузбагаченню. Іншим аспектом е-декларування, на думку В. Чумака, є політичний, аконкретніше той факт, що ці декларації депутатів можуть стати додатковоюінформацією для виборців. При цьому не слід забувати, що поруч зінформацією про осіб, уповноважених на виконання функцій держави абомісцевого самоврядування, при поданні е-декларацій розкривається інформація їхчленів сім’ї. Водночас, самі декларанти висловлювали побоювання, що «відкритеелектронне декларування майна чиновників "дає пряму наводку для злочинців" тає питанням безпеки сотень тисяч людей», а також що воно стало«інструментом тиску на суддів для того, аби схиляти їх до прийняття тих чиінших рішень».

Ще одна загроза що пов’язана з функціонуванням численних електроннихреєстрів. Г. Колесник, голова комітету захисту прав адвокатів та гарантійадвокатської діяльності, зазначає, що через відкритий доступ до інформації промісце проживання або роботи, злочинцям набагато легше тиснути та здійснюватинапади на адвокатів. «Кожен завдяки відкритим реєстрам може знайти домашнюадресу адвоката. Крім ЄРАУ, де міститься інформація про місце роботи (вадвокатів, які провадять індивідуальну адвокатську діяльність, це домашняадреса), дані щодо проживання адвоката можна знайти, зробивши безкоштовнийзапит щодо пошуку відомостей в ЄРДР на сайті Мін’юсту (там адресизасновників адвокатських бюро та об’єднань). Та й в судових засіданнях зазвичай(з’ясовуючи особу) суд вимагає в адвоката вказати місце проживання, хоча упрокурора про це не запитують. Як результат, біля під’їздів та у власнихквартирах на адвокатів учиняють напади»Суперечливим щодо свободи вираження поглядів є намагання останнімчасом нормативно регламентувати діяльність окремих груп осіб в соціальнихмережах. Зокрема, Правила адвокатської етики доповнили розділом, щоврегульовує поведінку в соцмережах та на інтернет-форумах. Відповідно до новихвимог при користуванні соціальними мережами адвокат повинен приймати доуваги обмеження, що встановлені для адвокатської діяльності в частині повнотита сприйняття інформації, забезпечення її конфіденційності та збереження.

Адвокату слід обережно здійснювати адвокатську діяльність за допомогоюсоціальних мереж шляхом надання правової допомоги, професійних порад таюридичних консультацій, адресованих та/або доступних необмеженому колу осіб. При користуванні соціальними мережами необхідно враховувати параметри їх конфіденційності з метою відповідального їх використання, моніторингу та регулярного аналізу власних соціальних мереж та контентів, що розміщуються в соціальних мережах. При виявленні в них помилок або будь-якихневідповідностей конфіденційності вони підлягають негайному виправленнюта/або видаленню.

У соціальних мережах адвокатам рекомендовано обережно відноситись докоментарів, які можуть відображати позицію, що протилежна позиції клієнта. Привстановленні адвокатом контактів та спілкування у соціальних мережах, інтернет-форумах та інших формах спілкування в мережі з клієнтами, колегами, суддями,процесуальними опонентами та іншими особами та їх об’єднаннями, вінзобов’язаний виключити можливість виникнення конфлікту інтересів. Висловлювання адвоката в соціальних мережах, інтернет-форумах та інших формах спілкування в мережі не повинні мати притаманний правовий нігілізм, будь-який вид агресії, ворожнечі і нетерпимості. Адвокат зобов’язаний вести себешанобливо і не допускати образливої поведінки. Будь-які заяви, коментаріадвоката в соціальних мережах, інтернет-форумах та інших формах спілкування вмережі інтернет, в тому числі під час обговорення і роз’яснення правових норм,особливостей судочинства, дій його учасників, повинні бути відповідальними,достовірними і не вводити в оману.

Така сувора регламентація, водночас, залишає відкритим питанняідентифікації особи у соціальних мережах. Адже одна із головних цінностейінтернету – це можливість зберігати анонімність. Наприклад, адвокат О. Шевчукіз цього приводу зазначив, що в соціальних мережах неодноразово відкритопринижується честь і гідність не лише окремих адвокатів, а й діяльностіукраїнської адвокатури загалом. При цьому допускається варіант, що такіпублікації в соціальних мережах поширюються не просто учасником мережі, аучасником під чужим іменем діючого адвоката, або й учасником-адвокатом, алепід чужим іменем адвоката.Значно менша за обсягом, але подібна за змістом стаття 20 Кодексусуддівської етики визначає, що “участь судді у соціальних мережах, інтернет-форумах та застосування ним інших форм спілкування в мережі є допустимими,проте суддя може розміщувати, коментувати лише ту інформацію, використанняякої не завдає шкоди авторитету судді та судової влади”.

Щодо поведінки державних службовців, то на сьогодні основнимидокументами, що її регулюють є закон «Про державну службу» та закон «Прозапобігання корупції». Кабінет Міністрів скасував кодекс етичної поведінкидержавного службовця, аргументуючи це уникненням дублювання визначеннявимог до етичної поведінки держслужбовців у різних нормативно-правових актах. Кодекс етичної поведінки держслужбовця передбачав обов`язкову фіксацію телефонних розмов і зустрічей держслужбовців 1-2 категорії з політиками і представниками бізнесу. Також держслужбовцям заборонялося критикувативладу та чиновників. Спеціальних норм щодо поведінки в соціальних мережах таінтернеті він не містив.

В журналістській практиці є по-різному. У більшості закордонних таміжнародних медіа чітко прописані правила поведінки в соціальнихмережах. Наприклад, Працівники RFERL вільні використовувати соцмережі, алеколи журналіст пише щось у Facebook або Twitter, він має пам'ятати, що єпрацівником «Радіо Свобода». Тому в соцмережах він не може писати абоговорити те, що підриває репутацію «РС» як збалансованого і об'єктивного ЗМІ.

Фактично акаунти в соцмережах не діляться на приватні і корпоративні. Навіть наособистих сторінках у Facebook перед поширенням будь-якого посилання існуєнеобхідність переконатися, що інформація правдива, не повинні поширюватифейки чи звертати увагу на діяльність лише однієї політичної сили чи політика.

Оскільки така діяльність може створити враження певної заангажованості учитачів. Те ж стосується і «лайків», якщо зміст повідомлення може вдарити порепутації «Радіо Свобода». В ВВС дещо інакше виглядають редакційністандарти поведінки в соцмережах. Чітко розділені поняття особистогооблікового запису і сторінки ВВС. Образливі коментарі про працівників виданняможуть вважатися дисциплінарним проступком. Журналісти не повинні писатите, що дискредитуватиме ВВС. Працівникам видання заборонено писатиобразливі пости і коментарі. Не можна використовувати інтернет для атак наколег жодним чином.

Українські видання (наприклад, Kyiv Post, «Сегодня», «Українська правда»)здебільшого не мають чітко прописаних правил поведінки у соціальнихмережах. Проте очікують від журналістів розуміння, що навіть на особистихсторінках вони є представниками свого видання, і категорично «не вітаютьсяхейтспіч і дискримінаційні висловлювання».

Звертаючи увагу на медіа, слід відмітити, що преса, радіо і телебаченняУкраїни переживають глибоку кризу. Сьогодні в країні фактично немає газет іжурналів, телекомпаній і радіостанцій, які б отримали справжню економічнунезалежність. Економічний успіх друкованого видання, телеканалу,інформагентство чи онлайн-медіа - в силу діючого законодавства, існуючихправових, адміністративних і економічних регламентів медіаринку - майже зовсімне залежить від чисельності аудиторії. Найбільші та найвпливовіші медіаналежать олігархам, які передовсім дбають про власні інтереси, а не інтересидержави чи свободу слова. В той же час журналіст чи особа, що здійснює медійнудіяльність24, щодня зіштовхується з загрозами, що пов’язані з можливістюзнищення чи викрадення інформації, інформаційно-психологічними впливами,зокрема, пов’язаними з тим, що ЗМІ розглядаються як інструмент впливу ідосягнення своїх цілей бізнесменами та політиками.

Перш ніж перейти до наступних категорій, вважаємо необхідним зупинитисьна соціокультурних особливостях комунікативного процесу. У статті"Комунікація" в "Енциклопедії соціальних наук" відзначається, що "дляформування суспільства, його об’єднань і підрозділів, а також для забезпеченнявзаєморозуміння між його членами необхідні якісь процеси комунікації". Ефективна комунікація є передумовою становлення демократичногосуспільства. Особливого значення вона набуває у багатонаціональних державах,де культура спілкування відрізняється не лише на мікрорівні (особистість, група),а й на макрорівні (регіони, віросповідання, історичний досвід). Таким чином,соціокультурна ситуація значною мірою визначає наскільки ефективним будекомунікативний процес в суспільстві, зокрема між органами влади та населенням,між центральними органами влади, місцевим самоврядуванням та органамисамоорганізації населення, між селом та містом, а також між різними регіонамидержави. І зрештою від цього залежить, які саме загрози інформаційно-психологічній безпеці людини і суспільства можуть актуалізуватись.

Спілкування є складовою соціокультурної ситуації, яка по-різному впливаєна його структуру, функції, способи здійснення. Культура втілює стиль мисленнялюдини, охоплює всі аспекти суспільного життя, характеризує глибину знаньособистості, її вихованість, уміння висловлювати свою думку, слухати інших,робити правильні висновки. Складовою культури особистості та соціальногосередовища, в якому відбувається її взаємодія, є культура спілкування, щовіддзеркалює ціннісні орієнтації, позиції, соціальні ролі індивіда у суспільстві.

Впливовими чинниками є звичаї та приписи стосовно сім'ї, статевої моралі, розподілу праці, а також відносини власності, особливості політичної влади, товариська етика, магічна практика, віра, уявлення про світ, природу і місце людини в ній. Рівень культури спілкування в групі характеризують: рівень загальнокультурного розвитку країни, її матеріальний, духовний стан на конкретному історичному етапі; рівень розвитку конкретної особистості, стан її комунікативного потенціалу, зв'язки із соціумом; рівень комунікативного розвитку групи, стан її соціально-психологічного простору; система зовнішніх зв'язків, наявність партнерів по взаємодії, каналів доступу іншої культури спілкування, інтенсивність, об'єктивний чи суб'єктивний характер таких зв'язків; комунікативно-правовий та організаційно-культурний порядок у групі; загальнолюдські, національні, галузеві, групові схеми взаємодії учасників спілкування, які забезпечують запрограмований рівень культури спілкування учасників групи.

Слід зважати, що культура спілкування нерозривно пов'язана з культуроюмовлення. А. Потебня, досліджуючи соціокультурні особливості особистості якпроблему денаціоналізації, бачив органічну участь національної (етнічної) мовине тільки у формуванні народного світосприйняття, але й у самім розгортаннідумки. Вчений підкреслював загальнолюдську цінність кожної мови – у якості щеоднієї, відбитої саме в цій мові, картини світу: "Якби об’єднання людства замовою і взагалі за народністю було б можливим, воно було б згубним длязагальнолюдської думки, як заміна багатьох почуттів одним, хоча б це одне булоне дотиком, а зором... Для існування людини потрібні інші люди; для народності –інші народності". Переконання в тім, що люди бачать світ по-різному– крізь призму своєї рідної мови – лежить в основі теорії "лінгвістичноївідносності" Е. Сепіра і Б. Ворфа25. Вони прагнули довести, що розходження міжкультурами обумовлені розходженнями в мовах. І хоча ця теорія й дотепервважається недоведеною, окремі аспекти її вивчення вплинули на інтерес доаналізу впливу соціокультурних особливостей особистості на проблемутрансформації не тільки суспільства в цілому, але й багатьох його структур, утому числі й мовного середовища як одного із суб’єктів соціокультурногопроцесу. Причому більшість дослідників приділяли увагу комунікаційнимпроблемам соціокультурних змін. Так, той же Е. Сепір розглядав впливкомунікативних процесів на життя особистості і суспільства.

Тому мовне питання та його правове врегулювання є важливою складовоюдержавної інформаційної політики і необхідною умовою гарантуванняінформаційної безпеки людини, захисту її інформаційних прав та свобод.

Система національно-психологічних особливостей індивіда базується накількох сферах: мотиваційній (своєрідність мотивів, спонукальних сил діяльностіпредставників тієї чи іншої національної спільноти); інтелектуально-пізнавальній (своєрідність сприймання й мислення носіїв національної психіки, щовиражається в наявності специфічних пізнавальних та інтелектуальних якостей,які дають змогу особливо сприймати навколишню дійсність, оцінювати її,будувати плани діяльності, моделі способів досягнення її результатів); емоційно-вольовій (своєрідність емоційних та вольових якостей, від яких в багатьохвипадках залежить результативність діяльності); комунікативно-поведінковій (цясфера охоплює інформаційну і міжособистісну взаємодію, стосунки і спілкування,показує різницю подібних проявів у представників різних національнихкультур).

Однак потрібно при цьому зважати на те, що специфіка національноїпсихології того чи іншого народу виражається не в яких-небудь неповторнихпсихологічних рисах і особливостях спілкування, а скоріше в їх неповторномупоєднанні, прояві в певних звичаях, історичних традиціях, поведінці, вчинкахОб’єктивна оцінка соціокультурних та етнопсихологічних особливостейспілкування свідчить, що властивості національної культури спілкування івластивості індивідів, із яких складається етнос, не тотожні. А це означає, щокомунікативні процеси залежатимуть від різних чинників, а отже ймовірністьреалізації інформаційних загроз відрізнятиметься.

Савінова Н.А. враховуючи регіональні відмінності населення України, атакож необхідність захисту населення від залякування, спотворення офіційноїінформації, пропонує систему рівневих комунікативних заходів яка бзабезпечувала прямий і зворотній зв’язок населення з владою на макро-, мезо- тамікро- рівні. При цьому кожен з учасників цієї системи має забезпечувати певнеколо інформаційних потреб решти, надаючи виключно корисну та легітимнуінформацію, утворюючи, таким чином систему спілкування «центральна влада» -«регіональна влада» - «населення» у послідовності та компетенції, чітковизначених на законодавчому рівні. Оскільки формування первинної комунікації відбувається на вищому рівні, така інформація первинно походить від центральних органів влади і, з використанням, насамперед, офіційних джерел, а у другу чергу – ЗМІ, потрапляє на мезо- та мікрорівень. До населення (на мікрорівень) така інформація нерідкопотрапляє вже неповною, перекрученою, забарвленою ставленням преси,неналежно прокоментована. Внаслідок недоліків офіційної комунікації усуспільстві утворюються відчуття нерозуміння, непочутості, обманутості,покинутості, незадоволення.

*Апробація результатів роботи.* Результати кваліфікаційної роботи були обговорені на засіданнях кафедри конституційного та трудового права Запорізького національного університету. Положення даної кваліфікаційної роботи були враховані автором в ході підготовки наукових статей для опублікування в українській науковій періодиці, під час участі у роботі наукових конференцій: щорічна науково-практична конференція «Запорізькі правові читання» м. Запоріжжя, 06 травня 2019 р., Всеукраїнська науково-практична конференція «Правова освіта та правова наука в умовах сучасних трансформаційних процесів» м. Запоріжжя, 20 листопада 2019 р., Збірка студентських наукових статей «Майбутні юристи про проблеми права в Україні» м. Запоріжжя, грудень 2019 р.

РОЗДІЛ 2 ПРАКТИЧНА ЧАСТИНА

2.1. Інформаційна безпека людини інтегральне явище в системі національної безпеки









2.2. Поняття, ознаки, правовий режим інформаційної безпеки в системі національної безпеки в Україні

Доктрина інформаційної безпеки України

1. Загальні положення

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Принципи, пріоритети та напрями забезпечення кібербезпеки України визначені [Стратегією кібербезпеки України](https://zakon.rada.gov.ua/laws/show/ru/96/2016#n11), затвердженою Указом Президента України від 15 березня 2016 року № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».

Доктрина інформаційної безпеки України (далі - Доктрина) визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Правовою основою Доктрини є [Конституція України](https://zakon.rada.gov.ua/laws/show/ru/254%D0%BA/96-%D0%B2%D1%80), закони України, [Стратегія національної безпеки України](https://zakon.rada.gov.ua/laws/show/ru/287/2015#n14), затверджена Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Терміни, що вживаються у Доктрині, мають таке значення:

стратегічні комунікації - скоординоване і належне використання комунікативних можливостей держави - публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави;

урядові комунікації - комплекс заходів, що передбачають діалог уповноважених представників Кабінету Міністрів України з цільовою аудиторією з метою роз'яснення урядової позиції та/або політики з певних проблемних питань;

кризові комунікації - комплекс заходів, що реалізуються державними органами України у кризовій ситуації і передбачають їх діалог із цільовою аудиторією з питань, що стосуються кризової ситуації;

стратегічний наратив - спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію.

2. Мета та принципи Доктрини

Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

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

3. Національні інтереси України в інформаційній сфері

Національними інтересами України в інформаційній сфері є:

1) життєво важливі інтереси особи:

забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

забезпечення конституційних прав людини на захист приватного життя;

захищеність від руйнівних інформаційно-психологічних впливів;

2) життєво важливі інтереси суспільства і держави:

захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації;

захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації;

забезпечення вільного обігу інформації, крім випадків, передбачених законом;

розвиток та захист національної інформаційної інфраструктури;

збереження і примноження духовних, культурних і моральних цінностей Українського народу;

забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;

вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;

зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;

розвиток медіа-культури суспільства та соціально відповідального медіа-середовища;

формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;

створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;

розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;

безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;

розвиток системи стратегічних комунікацій України;

ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;

забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;

формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти;

розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України.

4. Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері

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

здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

інформаційне домінування держави-агресора на тимчасово окупованих територіях;

недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

5. Пріоритети державної політики в інформаційній сфері

Пріоритетами державної політики в інформаційній сфері мають бути:

1) щодо забезпечення інформаційної безпеки:

створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері;

законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку;

визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ та населення; заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передачі інформації через комп'ютерні мережі в умовах запровадження правового режиму воєнного стану;

оптимізація законодавчих механізмів реалізації зобов'язань України в межах Європейської конвенції про транскордонне телебачення щодо держав, які не є підписантами зазначеної Конвенції;

створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав - членів НАТО;

розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;

забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій;

розвиток цифрового мовлення, унеможливлення впливу на його інфраструктуру суб'єктів, що пов'язані з державою-агресором;

побудова дієвої та ефективної системи стратегічних комунікацій;

розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України;

боротьба з дезінформацією та деструктивною пропагандою з боку Російської Федерації;

посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення суспільно-політичної ситуації;

виявлення та притягнення до відповідальності згідно із законодавством суб'єктів українського інформаційного простору, що створені та/або використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни, національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення;

проведення розвідувальними органами України акцій сприяння реалізації та захисту національних інтересів України в інформаційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави за межами України;

недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;

2) щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію:

стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів;

забезпечення функціонування Суспільного телебачення і радіомовлення України, у тому числі його належного фінансування;

створення системи мовлення територіальних громад, яка сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад;

підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек;

розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;

комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності;

підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності;

удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці;

задоволення потреб населення тимчасово окупованих територій в об'єктивній, оперативній і достовірній інформації;

повне покриття території України цифровим та інтернет-мовленням замість аналогового і надання рівних можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет;

формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту;

пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз;

3) щодо відкритості та прозорості держави перед громадянами:

розвиток механізмів електронного урядування;

сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних;

інформування громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами;

проведення реформи урядових комунікацій;

розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень органами державної влади та органами місцевого самоврядування;

сприяння формуванню культури суспільної дискусії;

4) щодо формування позитивного міжнародного іміджу України:

ґрунтовне реформування системи представлення інформації про Україну на міжнародній арені;

розвиток публічної дипломатії, у тому числі культурної та цифрової;

активізація скоординованої інформаційної роботи закордонних дипломатичних установ України;

сприяння поширенню та розвитку системи іномовлення України;

створення та забезпечення функціонування правового механізму взаємодії державних органів з інститутами громадянського суспільства з метою інформаційної підтримки комерційної, гуманітарної, просвітницької, культурної та іншої діяльності таких інститутів за межами України;

постійний моніторинг пропаганди держави-агресора, розроблення та оперативна реалізація адекватних заходів протидії;

недопущення використання міжнародного інформаційного простору в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;

реформування системи взаємовідносин з українською діаспорою шляхом забезпечення більш тісної співпраці та проведення ефективних заходів, зокрема в рамках комунікацій «від людини до людини»;

участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності;

запровадження міжнародних культурних фестивалів в Україні з метою популяризації української культури та розвитку комунікацій «від людини до людини».

6. Механізм реалізації Доктрини

Рада національної безпеки і оборони України відповідно до [Конституції України](https://zakon.rada.gov.ua/laws/show/ru/254%D0%BA/96-%D0%B2%D1%80) та у встановленому законом порядку має здійснювати координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері.

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

На Міністерство інформаційної політики України мають бути покладені в установленому порядку організація та забезпечення:

моніторингу засобів масової інформації та загальнодоступних ресурсів вітчизняного сегмента мережі Інтернет з метою виявлення інформації, поширення якої заборонено в Україні;

моніторингу загроз національним інтересам і національній безпеці в інформаційній сфері;

сприяння Міністерству закордонних справ України щодо донесення офіційної позиції України до іноземних засобів масової інформації;

формування поточних пріоритетів державної інформаційної політики, контролю їх реалізації;

координації діяльності центральних та місцевих органів виконавчої влади у сфері забезпечення інформаційного суверенітету України;

урядових комунікацій;

кризових комунікацій, зокрема під час проведення антитерористичної операції та в особливий період;

вжиття заходів в інформаційній сфері, пов'язаних із запровадженням правових режимів надзвичайного чи воєнного стану;

розроблення стратегічного наративу і його імплементації;

вироблення і впровадження стратегії інформаційного забезпечення процесу звільнення та реінтеграції тимчасово окупованих територій;

розроблення та впровадження єдиних стандартів підготовки фахівців у сфері урядових комунікацій для потреб державних органів.

Для сприяння координації діяльності органів виконавчої влади у сфері забезпечення інформаційного суверенітету України та взаємодії з іншими державними органами в інформаційній сфері у Міністерстві інформаційної політики України може утворюватися в установленому порядку допоміжний орган.

На Міністерство закордонних справ України має бути покладено в установленому порядку:

формування та реалізацію стратегії публічної та культурної дипломатії України;

координацію інформаційної діяльності державних органів у зовнішньополітичній сфері;

забезпечення просування інтересів України за кордоном інформаційними засобами;

забезпечення донесення позиції України до керівництва іноземних держав, парламентів та урядів, зовнішньополітичних відомств, представників бізнесу та експертних кіл, широкої громадськості, сприяння просуванню позитивного іміджу України;

сприяння просуванню українських телеканалів у кабельні та супутникові мережі за кордоном;

забезпечення налагодження взаємодії з міжнародними партнерами як на двосторонній, так і на багатосторонній основі з метою застосування міжнародного досвіду та найкращих практик у контексті протидії інформаційним загрозам.

Міністерство оборони України має забезпечувати функціонування системи військово-цивільних зв'язків у місцях постійної дислокації та розгортання підрозділів Збройних Сил України, інших військових формувань, а також організовувати і забезпечувати:

зв'язки з українськими та іноземними засобами масової інформації щодо висвітлення ситуації в районі проведення антитерористичної операції в Донецькій та Луганській областях;

протидію спеціальним інформаційним операціям, спрямованим проти Збройних Сил України та інших військових формувань;

супроводження інформаційними засобами виконання завдань оборони України;

донесення достовірної інформації до військовослужбовців Збройних Сил України, інших військових формувань, зокрема через засоби масової інформації Збройних Сил України.

Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України відповідно до компетенції братимуть участь у забезпеченні захисту українського інформаційного простору від пропагандистської аудіовізуальної та друкованої продукції держави-агресора; розроблятимуть пріоритети і стимули розвитку українського кіно, телевізійного контенту, книгодрукування, зокрема висвітлення героїчного спротиву Українського народу російській агресії.

Служба безпеки України у межах компетенції має здійснювати:

моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері;

протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій.

Розвідувальні органи України у процесі здійснення розвідувальної діяльності мають сприяти реалізації та захисту національних інтересів України в інформаційній сфері за кордоном, протидіяти зовнішнім загрозам інформаційній безпеці держави.

Державна служба спеціального зв'язку та захисту інформації України забезпечуватиме в межах компетенції формування і реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України.

Національний інститут стратегічних досліджень має забезпечити науково-аналітичне та експертне супроводження процесу формування і реалізації державної інформаційної політики.

7. Прикінцеві положення

Зважаючи на особливі умови і ведення проти України агресивної інформаційної війни не лише на її території, але й у світі, забезпечення реалізації Доктрини можливе лише за умови належної координації заходів, здійснюваних усіма державними органами. Ключові заходи відповідно до положень Доктрини визначатиме Рада національної безпеки і оборони України.

2.3. Особливості правового забезпечення інформаційної безпеки в умовах загроз національній безпеці

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

Концепція інформаційної безпеки України (далі – Концепція) спрямована на створення передумов для розвитку такого потенціалу інформаційної сфери України, за якого забезпечується її випереджальний розвиток, а зовнішні негативні впливи не створюють реальних небезпек національній інформаційній безпеці держави. Ключовезавдання системи інформаційної безпеки – забезпечити сталість такого розвитку, недопускаючи негативних впливів з боку сторонніх суб’єктів.

Реалізація на практиці такого підходу до інформаційної безпеки держави можездійснюватись виключно за участі всіх внутрішніх суб’єктів інформаційних відносин таза умов ефективної взаємодії держави з громадянським суспільством, приватнимсектором та окремими громадянами в інтересах ефективного розвитку інформаційноїсфери і спільного захисту такого розвитку від зовнішніх загроз.

Розділ І. Загальні положення

Стаття 1. Мета Концепції

Метою Концепції є забезпечення інформаційного суверенітету та визначенняпідходів до захисту та розвитку національного інформаційного простору для всебічногоінформаційного забезпечення українського суспільства.

Стаття 2. Визначення термінів

1. У цій Концепції наведені нижче терміни вживаються у такому значенні:

інформаційна безпека – стан захищеності життєво важливих інтересів людини ігромадянина, суспільства і держави, при якому запобігається завдання шкоди черезнеповноту, несвоєчасність і недостовірність поширюваної інформації, порушенняцілісності та доступності інформації, несанкціонований обіг інформації з обмеженимдоступом, а також через негативний інформаційно-психологічний вплив та умиснеспричинення негативних наслідків застосування інформаційних технологій;

загрози інформаційній безпеці – наявні та потенційно можливі явища ічинники, які створюють небезпеку життєво важливим інтересам людини і громадянина,суспільства і держави в інформаційній сфері;

стратегічний контент – це національний інформаційний продукт, який має наметі забезпечити політичну, культурну та духовну цілісність і розвиток політичноїнації;

національний інформаційний продукт – це аудіовізуальний, друкований чиінший продукт, призначений для задоволення інформаційно-комунікативних потребгромадян України, суспільства і держави, створений громадянами або юридичнимиособами України згідно з чинним законодавством;

державна інформаційна політика – це діяльність держави, спрямована наформування та регулювання середовища, в якому задовольняються інформаційно-комунікативні потреби громадян України, суспільства і держави;

сталий розвиток національного інформаційного простору – такий станнаціонального інформаційного простору, за якого забезпечується достатній рівеньосновних потреб та життєво важливих інтересів громадянина, суспільства і держави вінформаційній сфері;

національний інформаційний простір – сукупність всіх інформаційнихпотоків як національного, так й іноземного походження, які доступні на територіїдержави;

інформаційна сфера – сукупність інформаційних технологій, ресурсів,продукції і послуг, інформаційної інфраструктури, суб’єктів інформаційної діяльностіта системи регулювання суспільних інформаційних відносин;

інформаційний суверенітет України – це виключне право України відповіднодо Конституції і законодавства України та норм міжнародного права самостійно інезалежно з додержанням балансу інтересів особи, суспільства і держави визначати йздійснювати внутрішні й геополітичні національні інтереси в інформаційній сфері,державну внутрішню й зовнішню інформаційну політику, розпоряджатися власнимиінформаційними ресурсами, формувати інфраструктуру національного інформаційногопростору, створювати умови для його інтегрування у світовий інформаційний простірта гарантувати інформаційну безпеку держави;

інформаційна інфраструктура – сукупність організаційних структур і систем,які забезпечують функціонування та розвиток інформаційного простору, засобівінформаційної взаємодії та доступу користувачів до інформаційних ресурсів;

забезпечення інформаційної безпеки – діяльність, спрямована на запобігання,своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загрозінформаційній безпеці України;

кібернетична безпека (кібербезпека) – стан захищеності життєво важливихінтересів людини і громадянина, суспільства та держави в кіберпросторі;

кіберпростір – середовище, яке виникає в результаті функціонування на основієдиних принципів і за загальними правилами інформаційних (автоматизованих),телекомунікаційних та інформаційно-телекомунікаційних систем;

кіберзлочин – суспільно небезпечне винне діяння у кіберпросторі, передбаченечинним законодавством України про кримінальну відповідальність;

кібертероризм – терористична діяльність у кіберпросторі або з йоговикористанням.

2. Інші терміни вживаються у значенні, визначеному законодавством України.

Стаття 3. Правові основи інформаційної безпеки

1. Правову основу інформаційної безпеки становлять Конституція України,Закон України «Про основи національної безпеки України» та інші закони України,міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

2. Відповідно до цієї Концепції розробляються і затверджуються стратегії,програми та плани якими визначаються цільові настанови, принципи і напрямидіяльності суб’єктів забезпечення інформаційної безпеки України.

Стаття 4. Базовий підхід до забезпечення інформаційної безпеки

1. Діяльність державних органів у сфері забезпечення інформаційної безпеки

зосереджується на двох напрямах:

забезпечення сталого розвитку інформаційного простору України з метоюдосягнення ним такого рівня, який завдяки своїм властивостям міг бипротистояти зовнішнім та внутрішнім загрозам;

забезпечити створення і функціонування системи захисту процесу розвиткуінформаційного простору від загроз.

2. Інформаційна безпека України забезпечується шляхом захисту національногоінформаційного простору від інформаційних загроз та через сприяння його сталомурозвитку задля реалізації життєво важливих інтересів та потреб громадянина,суспільства і держави в інформаційній сфері.

Стаття 5. Принципи державної політики в сфері інформаційної безпеки.

1. Основними принципами забезпечення інформаційної безпеки України є:

верховенство права;

пріоритетність захисту прав і свобод людини і громадянина в інформаційнійсфері;

своєчасність і адекватність заходів захисту життєво важливих національнихінтересів України від реальних і потенційних загроз інформаційній безпеці;

захист інформаційного суверенітету України;

свобода думки і слова та вільне вираження своїх поглядів і переконань;

свобода збирати, зберігати, використовувати та поширювати інформацію;

захищеність особи від втручання в її особисте та сімейне життя;

обмеження доступу до інформації виключно на підставі закону;

гармонізація особистих, суспільних і державних інтересів, відповідальністьвсього Українського народу за забезпечення інформаційної безпеки;

розмежування повноважень, взаємодія та відповідальність державних інедержавних суб’єктів забезпечення інформаційної безпеки;

пріоритетність розвитку та поширення національних інформаційних технологій,ресурсів, продукції та послуг, а також політика постійного поліпшення кількості татехнічної якості каналів передачі інформації;

можливість задіяння в інтересах забезпечення інформаційної безпеки Українисистем і механізмів міжнародної та колективної безпеки;

гармонізація інформаційного законодавства з нормами міжнародного права іправовими актами Європейського Союзу.

захист інформаційного суверенітету, державного суверенітету, конституційноголаду і територіальної цілісності України;

формування в інформаційному просторі української ідентичності як невід’ємноїскладової сталого суспільно-політичного дискурсу;

формування дуальної системи суспільного та комерційного мовлення;

сприяння розвитку в національному інформаційному просторі контенту, якийпідтримує збереження і захист загальнолюдських цінностей, інтелектуальний,духовний і культурний розвиток Українського народу.

2.4. Особливості забезпечення інформаційної безпеки людини в умовах загроз національній безпеці

Розділ ІІ. Основи державної політики у сфері інформаційноїбезпеки

Стаття 6. Життєво важливі інтереси і потреби громадянина, суспільства ідержави в інформаційній сфері

1. Державна політика у сфері інформаційної безпеки зосереджена на задоволенніта захисті життєво важливих інтересів та потреб громадянина, суспільства і держави вінформаційній сфері щодо:

продукування, споживання, розповсюдження і розвитку національногостратегічного контенту та інформації в інтересах громадянина, суспільства і держави.

функціонування та захищеності кібернетичних, телекомунікаційних та іншихавтоматизованих компьютерних систем, що формують інфраструктурну основу

внутрішньодержавного інформаційного простору.

Стаття 7. Напрями державної політики у сфері інформаційної безпеки

1. Основними напрямами державної політики у сфері забезпечення

інформаційної безпеки є:

забезпечення балансу між неухильним дотриманням конституційних прав ісвобод людини в інформаційній сфері, зокрема свободи слова, та реалізацієюдержавних функцій щодо своєчасного виявлення, запобігання, припинення танейтралізації загроз інформаційній безпеці людини і громадянина, суспільства ідержави;

розвиток нормативно-правової бази для регулювання процесів розвиткуінформаційного простору і його захисту від зовнішніх загроз та її гармонізація знормами міжнародного права, вимогами міжнародного співробітництва, нормами істандартами Європейського Союзу;

розробка та реалізація ефективної державної інформаційної політики з метоюрозвитку національного інформаційного простору та гармонізації системи управління ікоординації між суб’єктами, які реалізують державну інформаційну політику тадержавну політику в сфері інформаційної безпеки;

налагодження співпраці держави з громадським та приватним секторами, атакож сприяння міжнародному співробітництву з метою реалізації державноїінформаційної політики та забезпечення інформаційної безпеки, а також створенняякісного національного інформаційного продукту;

всебічне сприяння, державна підтримка та пріоритетність створення ірозповсюдження національного інформаційного продукту, в тому числі за межіУкраїни;

використання українського національного інформаційного продукту дляпоширення в міжнародному інформаційному середовищі загальнолюдських цінностейта інформаційного розвитку людства, зокрема обмін із закордонними партнерамиУкраїни баченням, підходами та механізмами протистояння новітнім викликам,спрямованим на демократичні цінності та свободу слова в інформаційному просторі,що були інспіровані деструктивною політикою інших держав.

Стаття 8. Загрози інформаційній безпеці України

1. Державна політика у сфері інформаційної безпеки здійснюється з метоюнедопущення перешкоджання реалізації життєво важливих інтересів і потребгромадянина, суспільства і держави зовнішніми і внутрішніми загрозами національнійбезпеці в інформаційній сфері, що є запорукою сталого розвитку національногоінформаційного простору.

2. Загрозами національній безпеці України в інформаційній сфері є:

загрози комунікативного характеру всфері реалізації потреб людини ігромадянина, суспільства та держави щодо продукування, споживання,розповсюдження та розвитку національного стратегічного контенту та інформації;

загрози технологічного характеру в сфері функціонування та захищеностікібернетичних, телекомунікаційних та інших автоматизованих систем, що формуютьматеріальну (технічну, інструментальну) основу внутрішньодержавногоінформаційного простору.

3. Загрози комунікативного характеру всфері реалізації потреб людини ігромадянина, суспільства та держави щодо продукування, споживання,розповсюдження та розвитку національного стратегічного контенту та інформаціївключають:

а) зовнішні негативні інформаційні впливи на свідомість людини таспільноти через засоби масової інформації, а також мережу Інтернет, що здійснюютьсяна шкоду державі та мають на меті:

спроби змінювати психічні та емоційні стани людини, її психологічні тафізіологічні характеристики;

здійснювати керований вплив на свободу вибору, шляхом поширення унаціональному інформаційному просторі культу насильства і жорстокості,зневажливого ставлення до людської і національної гідності, розпалюванняміжрелігійної, міжетнічної та міжнаціональної ворожнечі, ненависті за етнічною,мовною, релігійною та іншими ознаками;

поширення закликів до сепаратизму, повалення конституційного ладу чипорушення територіальної цілісності держави;

б) інформаційний вплив на населення України, у тому числі на особовийсклад військових формувань, мобілізаційний резерв, з метою послаблення їх готовностідо оборони держави та погіршення іміджу військової служби;

в) поширення суб'єктами інформаційної діяльності викривленої,

недостовірної та упередженої інформації для дискредитації органів державної влади,дестабілізації суспільно-політичної ситуації, що значно ускладнює прийняттяполітичних рішень, завдає шкоди національним інтересам України чи створюєнегативний імідж України;

г) загрози свободі слова, що виражається у:

втручанні в редакційну політику з боку власників засобів масової інформації;

відсутності правової бази для посилення ролі творчих (трудових) колективів іредакцій у процесі здійснення редакційної політики засобами масової інформації усіхформ власності;

монопольна концентрація власності на засоби масової інформації та засобидонесення інформації до споживача, що надає можливість здійснюватицілеспрямований вплив на споживачів інформації;

створення адміністративних і нормативно-правових передумов для обмеженнясвободи слова, маніпулювання суспільною свідомістю як під зовнішнім впливом, так і збоку внутрішніх політичних організацій, комерційних структур та окремих осіб;

д) створення, розповсюдження, передача та зберігання інформації з метоюпідтримки, супроводження чи активізації злочинної та терористичної діяльності.

4. Загрози технологічного характеру в сфері функціонування та захищеностікібернетичних, телекомунікаційних та інших автоматизованих систем, що формуютьматеріальну (технічну, інструментальну) основу внутрішньодержавногоінформаційного простору включають:

а) використання іноземними державами кібервійськ, кіберпідрозділів, новихвидів інформаційної зброї та зброї кібернетичного характеру на шкоду Україні;

б) прояви кіберзлочинності, кібертероризму чи кібернетичної військовоїагресії, що загрожують сталому та безпечному функціонуванню національнихінформаційно-телекомунікаційних систем, шляхом втручання, несанкціонованованогодоступу або порушення функціонування телекомунікаційних, кібернетичних,автоматизованих комп’ютерних систем, незалежно від форми власності, з метою:

вчинення диверсій чи терористичних актів;

здійснення підтримки, супроводження чи активізації злочинної, екстремістськоїчи терористичної діяльності;

здійснення з їх допомогою деструктивного інформаційного впливу;

перехоплення інформації в телекомунікаційних мережах;

створення радіоелектронних перешкод чи блокування інформаційних систем,засобів зв'язку та управління, реалізація програмно-математичних засобів, щопорушують функціонування інформаційних систем;

включення у програмно-технічні засоби прихованих шкідливих функцій.

в) недостатній рівень розвитку національної інформаційної інфраструктури,зокрема:

залежність національної інформаційної інфраструктури від іноземнихвиробників високотехнологічної продукції;

використання неліцензованого і несертифікованого програмного забезпечення,засобів і комплексів обробки інформації;

невідповідність норм юридичної відповідальності за скоєні правопорушеннясучасним викликам і загрозам інформаційній безпеці;

недостатній рівень захищеності об'єктів критичної інформаційноїінфраструктури держави.

г) порушення порядку доступу, поводження та встановлених регламентівзбору, обробки, зберігання, поширення чи передачі інформації, яка захищаєтьсядержавою (державна таємниця, конфіденційна інформація, персональні дані, авторськіправа чи інтелектуальна власність), або роботи з інформаційними ресурсами, що їїмістять;

д) відсутність громадського контролю за діяльністю суб’єктів забезпеченняінформаційної безпеки, захищеністю національної інформаційної інфраструктури таінформаційного простору України.

Розділ ІІІ. Суб’єкти та механізми забезпечення інформаційноїбезпеки України

Стаття 9. Суб’єкти забезпечення інформаційної безпеки України

1. Суб’єктами забезпечення інформаційної безпеки є:

громадяни України, об'єднання громадян, громадські організації та іншіінститути громадянського суспільства;

Президент України, Верховна Рада України, Кабінет Міністрів України, іншіцентральні органи виконавчої влади та органи сектору безпеки і оборони України;

засоби масової інформації та комунікації різних форм власності, підприємства,заклади, установи та організації різних форм власності, що здійснюють інформаційнудіяльність;

наукові установи, освітні і навчальні заклади України, які, зокрема, здійснюютьнаукові дослідження та підготовку фахівців за різними напрямами інформаційноїдіяльності, в галузі інформаційної безпеки.

Стаття 10. Завдання і повноваження органів державної влади у сфері

інформаційної безпеки

1. Центральним органом, спеціально уповноваженим здійснювати координаціюта контроль забезпечення інформаційної безпеки як складової національної безпеки іоборони в межах компетенції та покладених на нього функцій, є Рада національноїбезпеки і оборони України, яка, відповідно до своїх повноважень:

визначає стратегічні національні інтереси України, концептуальні підходи танапрями забезпечення національної безпеки і оборони в інформаційній сфері;

формує проекти державних програм, доктрин, законів України, указівПрезидента України, директив Верховного Головнокомандувача Збройних СилУкраїни, міжнародних договорів, інших нормативних актів і документів з питаньінформаційної безпеки України;

координує і здійснює контроль над іншими державними органами секторунаціональної безпеки і оборони в сфері забезпечення інформаційної безпеки України;

здійснює постійний моніторинг впливу на національну безпеку процесів, щовідбуваються в інформаційній сфері;

визначає стан інформаційної агресії та звертається до Верховної Ради України зпропозицією про введення спеціального правового режиму захисту інформаційногопростору держави.

2. Основними суб’єктами реалізації державної політики в сфері інформаційноїбезпеки, в межах їх повноважень та завдань, є:

Служба безпеки України;

Міністерство внутрішніх справ України;

Міністерство оборони України;

Служба зовнішньої розвідки України;

Центральний орган виконавчої влади із спеціальним статусом, який забезпечуєформування та реалізує державну політику у сферах організації спеціального зв’язку,захисту інформації, телекомунікацій і користування радіочастотним ресурсом України.

3. Формування, реалізацію та координацію державної інформаційної політики, атакож забезпечення інформаційного суверенітету України здійснює спеціальноуповноважений центральний орган виконавчої влади відповідно до покладених нанього функцій.

Завданнями центрального органу виконавчої влади в сфері державноїінформаційної політики є:

розробка концептуальних документів в сфері сталого розвитку інформаційногопростору та контроль за їх виконанням в системі органів виконавчої влади;

координація діяльності центральних органів виконавчої влади щодозабезпечення сталого розвитку інформаційного простору України;участь у формуванні та реалізації стратегій, програм та планів, якимивизначаються цільові настанови, принципи і напрями реалізації положень цієїКонцепції;

підготовка нормативних документів, що регламентують порядок зв’язків згромадськістю органів державної влади та оприлюднення інформації про їх діяльність,а також координація та контроль діяльності підрозділів центральних органів виконавчоївлади, що здійснюють комунікацію з громадськістю.

4. Основними суб'єктами реалізації державної інформаційної політики України єтакі центральні органи виконавчої влади, які формують та реалізують державнуполітику в наступних напрямах:

1) у сферах освіти і науки, інтелектуальної власності, наукової, науково-технічної та інноваційної діяльності, інформатизації, формування і використаннянаціональних електронних інформаційних ресурсів, створення умов для розвиткуінформаційного суспільства, а також у сфері здійснення державного нагляду(контролю) за діяльністю навчальних закладів незалежно від їх підпорядкування іформи власності;

2) у сферах культури та мистецтв, охорони культурної спадщини,вивезення, ввезення і повернення культурних цінностей, державної мовної політики, атакож у сфері формування та реалізації державної політики у сфері кінематографії(останнє – це Держкіно);

3) у сфері інформатизації, електронного урядування, формування івикористання національних електронних інформаційних ресурсів, розвиткуінформаційного суспільства;

4) у сфері телебачення і радіомовлення, інформаційній та видавничійсферах.

5. Спеціально уповноважений центральний орган виконавчої влади, що здійснюєформування, реалізацію та координацію державної інформаційної політики, а такожосновні суб'єкти реалізації державної інформаційної політики, здійснюють своюдіяльність у взаємодії з:

1) постійно діючим колегіальним органом, метою діяльності якого є наглядза дотриманням законів України у сфері телерадіомовлення, а також здійсненнярегуляторних повноважень (Національна рада України з питань телебачення ірадіомовлення);

2) органом державного регулювання у сфері телекомунікацій,інформатизації, користування радіочастотним ресурсом та надання послуг поштовогозв`язку;

3) органами саморегуляції медіасфери України.

2.5. Пріоритети вдосконалення правових основ інформаційної безпеки в національній безпеці в умовах реформаційних змін

Механізми реалізації Концепції. Концепція інформаційної безпеки України, її ключові положення тазавдання реалізуються через сукупність нормативно-правових актів, відповідальність зарозробку і виконання яких несуть суб'єкти забезпечення сталого інформаційногорозвитку та інформаційної безпеки, визначені цією Концепцією.

2. Спеціально уповноважений центральний орган виконавчої влади всферіреалізації державної інформаційної політики вживає заходів щодо забезпеченняцілісності та узгодженості політики у сфері інформаційної безпеки та захистуінформаційного суверенітету України.

3. Спеціально уповноважений центральний орган виконавчої влади в сферіреалізації державної інформаційної політики формує та подає на розгляд КабінетуМіністрів України пропозиції щодо розробки, прийняття та виконання нормативно-правових актів, які скеровують та координують інформаційну діяльність Кабінетуміністрів України, Прем’єр-міністра України, членів Кабінету міністрів України,міністерств та інших центральних органів виконавчої влади та їхніх посадових осіб, атакож Антимонопольного комітету України, Фонду державного майна України та їхніхпосадових осіб.

4. Спеціально уповноважений центральний орган виконавчої влади в сферіреалізації державної інформаційної політики формує та подає на розгляд Радинаціональної безпеки та оборони України пропозиції щодо розробки, прийняття тавиконання нормативно-правових актів, які скеровують та координують інформаційнудіяльність Президента України, Ради національної безпеки та оборони України,Міністерства оборони України, вищого командування Збройних Сил України,Міністерства закордонних справ України, Служби безпеки України, Національногоантикорупційного бюро України, Державної прикордонної служби України,розвідувальних та контррозвідувальних органів, місцевих державних адміністрацій.

5. Спеціально уповноважений центральний орган виконавчої влади в сферіреалізації державної інформаційної політики формує та подає на розглядНаціонального банку України та Генеральної прокуратури України пропозиції щодорозробки, прийняття та виконання нормативно-правових актів, які регулюють їхнюінформаційну діяльність.

6. Кабінет Міністрів України, Рада національної безпеки та оборони України,Національний банк України, Генеральна прокуратура України розглядають увстановленому порядку пропозиції спеціально уповноваженого центрального органувиконавчої влади в сфері реалізації державної інформаційної політики та приймаютьвідповідні рішення в межах своїх повноважень.

7. На виконання розпоряджень Кабінету Міністрів України, Ради національноїбезпеки та оборони України, прийнятих на основі пропозицій центрального органувиконавчої влади в сфері реалізації державної інформаційної політики, органивиконавчої влади, які є суб’єктами реалізації державної інформаційної політики,забезпечують реалізацію положень цієї Концепці.

8. Спеціально уповноважений центральний орган виконавчої влади всферіреалізації державної інформаційної політики приймає та розглядає звернення іншихдержавних органів, громадян України, громадських об’єднань і організацій для їх

врахування під час розробки пропозицій Кабінету Міністрів України та іншим органамвиконавчої влади.

9. Нормативно-правовими актами, які забезпечують реалізацію цієї Концепції, є:

Державна програма розвитку інформаційного простору України;

Державна програма доступу до мережі Інтернет;

Державна програма підтримки вітчизняного ІТ-виробництва;

Державна програма з питань іномовлення та представлення України вміжнародному інформаційному просторі;

Державна програма з питань єдиної офіційної комунікативної політики;

Державна програма розвитку державно-приватного партнерства в інформаційнійсфері;

Державна програма захисту культурних та інформаційних потреб громадянУкраїни;

Державна програма заезпечення кібернетичної безпеки УкраїниДержавна програма підготовки і перепідготовки спеціалістів з інформаційноїбезпеки;

Державна програма наукового та моніторингового забезпечення інформаційноїсфери.

10. Розробка та виконання зазначених документів є складовою частиноюобов'язків суб'єктів забезпечення сталого інформаційного розвитку та інформаційноїбезпеки України.

11. Контроль за дотриманням виконання зазначених документів, їх узгодженостіміж собою за цілями та заходами в межах конкретних напрямів, покладається наоргани, що згідно з положеннями цієї Концепції відповідають за координацію таконтроль забезпечення сталого інформаційного розвитку та інформаційної безпекиУкраїни.

Розділ IV. Громадський контроль та державно-громадськепартнерство всфері реалізації державної інформаційної політики тазабезпечення інформаційної безпеки

Стаття 12. Громадський контроль у сфері реалізації державноїінформаційної політики та забезпечення інформаційної безпеки

1. Форми громадського контролю у сфері реалізації державної інформаційноїполітики визначаються нормативно-правовими актами України про діяльністьгромадських рад та нормами цієї Концепції.

2. Громадський контроль у сфері забезпечення інформаційної безпекиздійснюється у формах, що визначені Радою національної безпеки та оборони України іне суперечать чинному законодавству України з питань громадського контролю.

Стаття 13. Експертні радив системі забезпечення громадського контролю усфері реалізації державної інформаційної політики

1. Основним напрямом здійснення громадського контролю у сфері реалізаціїдержавної інформаційної політики є формування спеціальних Експертних рад приспеціально уповноваженому центральному органі виконавчої влади в сфері реалізаціїдержавної інформаційної політики. Експертні ради створюються задля здійсненняконтролю громадськості за процесом формування, виконання та результативностінормативно-правових актів, що вказані в цій Концепції та забезпечують її реалізацію.

2. Положення про Експертні ради розробляється та затверджується спеціальноуповноваженим центральним органом виконавчої влади всфері реалізації державноїінформаційної політики. Склад Експертних рад формується з науковців, освітян,представників органів самоорганізації населення та громадських організацій (занапрямом конкретної державної програми). До складу Експертних рад можуть бутидодатково включені (без права голосу) представники державних структур, у тому числітих, що відповідають за реалізацію конкретних програм. За рішенням керівникаспеціально уповноваженого центрального органу виконавчої влади в сфері реалізаціїдержавної інформаційної політики голови Експертних рад, що обрані зі складу цихЕкспертних рад, призначаються радниками керівника спеціально уповноваженогоцентрального органу на громадських засадах.

3. Основні завдання профільних Експертних рад з контролю за виконаннямнормативно-правових актів, які забезпечують реалізацію цієї Концепції:

підготовка пропозицій на етапі формування проектів нормативно-правовихактів, які забезпечують реалізацію цієї Концепції;

опрацювання проміжних звітів та незалежна оцінка процесу виконаннязазначених програм, що надається суспільству незалежно від оцінки спеціальноуповноваженого центрального органу виконавчої влади в сфері реалізації державноїінформаційної політики;

підготовка цільових пропозицій щодо підвищення ефективності реалізаціїположень програм;

запрошення на засідання Експертних рад представників структур, що визначенів якості відповідальних за виконання програм;

формування фінальних звітів щодо ефективності реалізації державних програм.

Розділ VI. Прикінцеві положення

1. Ця Концепція набирає чинності з дня її опублікування.

2. На підставі цієї Концепції внести відповідні зміни до діючих законодавчихактів: Закону України «Про інформацію», Закону України «Про Кабінет МіністрівУкраїни» (п.4 Статті 3; п.1 Статті 47) та інших номативно-правових актів; привести їх увідповідність до цієї Концепції.

3. Доручити Кабінету міністрів України:

привести у відповідність підзаконні нормативно-правові акти;внести на розгляд Верховної Ради України проекти законів про наступнідержавні програми:

- Державну програма розвитку інформаційного простору України;

- Державну програма доступу до мережі Інтернет;

- Державну програма підтримки вітчизняного ІТ-виробництва;

- Державну програма з питань іномовлення та представлення України вміжнародному інформаційному просторі;

- Державну програма з питань єдиної офіційної комунікативної політики;

- Державну програма розвитку державно-приватного партнерства вінформаційній сфері;

- Державну програма захисту культурних та інформаційних потреб громадян України;

- Державну програма забезпечення кібернетичної безпеки України

- Державну програма підготовки і перепідготовки спеціалістів з інформаційної безпеки;

- Державну програма наукового та моніторингового забезпечення інформаційної сфери.

ВИСНОВКИ

Дослідження джерельної бази дало змогу визначити три концептуальні підходи до тлумачення інформаційної безпеки України: 1) статичний (безпека як стан захищеності інформаційного середовища/інформації, система гарантій тощо); 2) діяльнісний (безпека як процес її забезпечення, здатність держави ефективно захистити національні інтереси і цінності); 3) комплексний (безпека як стан і процес). Найбільш прийнятним із них є комплексний. За такого підходу інформаційну безпеку України вперше визначено як 1) стан, за якого в умовах дії реальних та потенційних загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їхніх субʼєктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері; 2) забезпечення інформаційної безпеки України визначено як постійний процес діяльності компетентних органів, спрямований на запобігання, протидію загрозам інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час. Доведено, що основна мета забезпечення інформаційної безпеки України – це створення безпечного інформаційного середовища, що означає і захист національних інтересів і цінностей (пасивна форма), і протидію, активні контрзаходи (активна форма).

Підтверджено, що основними об’єктами інформаційної безпеки України є: а) особа (людина і громадянин) – її конституційні права і свободи, фізичне та психічне здоров’я, захищеність від негативного впливу інформаційних технологій та інформації; б) суспільство і держава – захищеність їхніх законних інтересів в інформаційній сфері; в) інформаційні ресурси та інформаційна інфраструктура – їхня цілісність, доступність та захищеність. Доведено, що об’єкти правового забезпечення інформаційної безпеки держави втілюються в національних інтересах, цінностях, цілях та надбаннях в інформаційній сфері.

Обґрунтовано, що реалізація національних інтересів в інформаційній сфері, визначених Доктриною інформаційної безпеки України, буде дієвою в разі законодавчого визначення національних цінностей і зумовлених ними національних інтересів. До національних цінностей в інформаційній сфері віднесено: а) матеріальний добробут населення (у т. ч. на основі розвитку ІКТ); б) інформаційна захищеність людини, суспільства, держави; в) духовність, доступність віросповідання, попередження релігійного фанатизму та екстремізму; г) мова; ґ) культура інформаційних відносин; д) свобода інформації, захищеність інформаційних прав людини, доступ до інформації, нейтралізація негативних інформаційних впливів та ін. До національних цілей в інформаційній сфері віднесено: а) покласти край спотворенням поглядів людей на навколишній світ і самих себе (духовна безпека); б) забезпечити впровадження інформаційних технологій у військову сферу та забезпечити їх захист (воєнна безпека); в) прискорити розробку та впровадження новітніх ІКТ у суспільно-економічну сферу (економічна безпека); г) досягти належного рівня культури інформаційних відносин (соціальна безпека); ґ) створити загальнодержавні інформаційні системи для постійного моніторингу стану навколишнього середовища (екологічна безпека); д) сприяти інтеграції національної інформаційної інфраструктури зі світовою інфраструктурою; е) посилити захист інформаційних прав людини; є) вжити термінових заходів для створення позитивного іміджу держави в умовах інформаційної глобалізації.

Виходячи із розробленої моделі взаємодії національних цінностей, інтересів цілей та надбань в інформаційній сфері, запропоновано основними критеріями оцінки негативного впливу на інформаційну безпеку держави вважати деструктивні трансформації національних цінностей в інформаційній сфері, які можливо встановлювати шляхом соціологічних опитувань та вивчення громадської думки. Такі критерії доцільно акумулювати в методологічній базі і на її підставі моніторити стан і динаміку вітчизняної інформаційної сфери, виявляти найбільш вразливі сфери.

Доведено, що в основу вдосконалення інформаційної безпеки України доцільно покласти принципи: а) формування та застосування норм міжнародного права як складової правової системи України; б) забезпечення балансу інтересів людини, суспільства і держави; в) узгодженості діяльності органів державної влади щодо вдосконалення правового забезпечення інформаційної безпеки України.

Обґрунтовано доцільність правового забезпечення інформаційної безпеки України досліджувати як цілісну систему правового регулювання суспільних відносин, що виникають у процесі протидії загрозам національній безпеці України в інформаційній сфері. Зазначений правовий феномен має власний предмет правового регулювання. Об’єктом відносин, які належать до такої діяльності, є інформація та відповідна інфраструктура. Із згаданим предметом правового регулювання формується новий комплексний інформаційний феномен – інформаційне право, а в його межах і на основі чинного вітчизняного законодавства – модель формування структурного утворення з правового забезпечення інформаційної безпеки. Це зумовило теоретичне підтвердження існування в системі права галузі інформаційного права, а також правового забезпечення інформаційної безпеки як підгалузі інформаційного права.

Доведено, що механізми протидії інформаційним загрозам від зовнішніх джерел повинні передбачати: а) мету забезпечення безпеки, що полягає у збереженні цілісності й захищеності інформаційної сфери у процесі її функціонування; б) рівень безпеки, що виокремлює складники системи, які можуть стикатися з потенційними і реальними небезпеками; в) сфери безпеки, що визначають можливості функціонування й розвитку інформаційної сфери; г) параметри безпеки, що встановлюють припустимі межі відхилень у потенціалі системи інформаційної безпеки, кількості її елементів, їх якості, зв’язки; ґ) перелік загроз, наслідки їх реалізації та механізми запобігання.

Методи протидії інформаційним загрозам від зовнішніх джерел умовно поділено на дві групи: 1) профілактичні (превентивні) – використовуються для недопущення розгортання відповідних загроз або для запобігання виникненню нових ризиків на початковому етапі розгортання таких загроз; 2) оперативні – застосовуються безпосередньо у відповідь на агресивні кроки зовнішніх джерел інформаційних загроз та пов’язані з їх розгортанням та реалізацією.

Доведено необхідність удосконалення функціональних обов’язків суб’єктів забезпечення інформаційної безпеки України в частині здійснення координації та взаємодії. Запропоновано для вироблення узгоджених рішень щодо напрямів і заходів реалізації державної політики інформаційної безпеки створити при Раді національної безпеки і оборони України міжвідомчу комісію (або координаційну раду) у складі представників профільного Комітету Верховної ради України, Кабінету Міністрів України, Міністерства інформаційної політики, Міністерства оборони, Служби безпеки України, Міністерства внутрішніх справ, Міністерства закордонних справ та інших державних органів, спеціально уповноважених на виконання завдань щодо забезпечення інформаційної безпеки. Крім того, у статті 10 Закону України «Про Службу безпеки України» йдеться, що у структурі Центрального управління Службу безпеки України діє підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, котрий може виконувати координуючу функцію у сфері забезпечення інформаційної безпеки держави. Реалізація цього положення потребуватиме внесення змін до Закону України «Про національну безпеку України», а також до Доктрини інформаційної безпеки України та Стратегії кібербезпеки України.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов А.А., Брижко В.М., Базанов Ю.К. Права людини і захист персональних даних. URL: http:/library.khpg.org/files/docs/Kn\_L\_.pdf
2. Безпека України: якою її бачать американські політичні діячі // MIND UA. 12 ГРУДНЯ 2017. URL: https://mind.ua/publications/20179511-bezpeka-ukrayini-yakoyu-yiyi-bachat-amerikanski-politichni-diyachi
3. Беларусь: Национальный ИКТ-профайл (Информационная безопасность и защита информации). URL: https://digital.report/belarusinformatsionnaya-bezopasnost/
4. В Евросоюзе приняли новый закон о защите даннях. URL: https://threatpost.ru/v-evrosoyuze-prinyali-novyj-zakon-o-zashhitedannyh/15749/
5. В Евросоюзе приняли новый закон о защите даннях. URL:https://threatpost.ru/v-evrosoyuze-prinyali-novyj-zakon-o-zashhitedannyh/15749/
6. В Финляндии открылся центр информационной безопасности. URL: http://www.goodnewsfinland.ru/cgi-otkryvaet-v-finlyandii-novyj-tsentrinformatsionnoj-bezopasnosti/.
7. Всіх перевірять: Рада підтримала новий захист від РФ. URL: http://ua.korrespondent.net/ukraine/3820536-vsikh-pereviriat-vlada-prydumalanovyi-zakhyst-vid-rf
8. Доктрина кибезбезопасности Польщи. URL:constitutions.ru/?p=11083
9. Европарламент принял резолюцию с осуждением Венгрии. URL: http://www.novayagazeta.ru/news/ 54209.html
10. Европейская Конвенция по киберпреступлениям. URL: http://inter.criminology.onua.edu.ua/?p=2263
11. Европейская Конвенция по киберпреступлениям. URL: http://inter.criminology.onua.edu.ua/?p=2263
12. Зайцев М. Суб’єкти забезпечення інформаційної безпеки України. URL: http://nbuv. gov. ua/j-pdf/FP\_index. htm\_2013\_3\_40.pdf
13. Закон України "Про боротьбу з тероризмом" від 20 березня 2003 року. URL: http://zakon5.rada.gov.ua/laws/show/638-15
14. Закон України "Про внесення змін до Кримінального та Кримінально-процесуального кодексів України" від 23 грудня 2004 року. URL: http://zakon0.rada.gov.ua /laws/show/2289-iv
15. Закон України "Про доступ до публічної інформації" від 13 січня 2011 року. URL: http://zakon2.rada.gov.ua/laws/show/2939-17
16. Закон України "Про запобігання корупції" від 14 жовтня 2014 року. URL: http://zakon5.rada.gov.ua/laws/show/1700-18
17. Закон України "Про інформацію" від 02 жовтня 1992 року (в редакції від 01 січня 2017 року). URL:http://zakon5.rada.gov.ua/laws/show/2657-1
18. Закон України "Про науково-технічну інформацію" від 25 червня 1993 року. URL: http://zakon5.rada.gov.ua/laws/show/3322-12
19. Закон України "Про телекомунікації" від 18 листопада 2003 року. URL: http://zakon2.rada.gov.ua/laws/show/1280-15
20. Закон України "Про центральні органи виконавчої влади" від 17 березня 2011 року. URL: http://zakon3.rada.gov.ua/laws/show/3166-17
21. Закон України «Про внесення змін до деяких законів України щодо зовнішньополітичного курсу України» від 08.06.2017 року. URL: www.zakon.rada.gov.ua/laws/show/2091-19
22. Закон України «Про Державну службу спеціального зв’язку та
23. Закон України «Про засади внутрішньої і зовнішньої політики» від 01.07.2010 року. URL: www.zakon.rada.gov.ua/ laws/show/ 2411-17.
24. Закон України «Про захист інформації в інформаційнотелекомунікаційних системах" від 5 липня 1994 року. URL:http://zakon3.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
25. Закон України «Про Кабінет Міністрів України» від 27 лютого 2014 року. URL: http://zakon3.rada.gov.ua/laws/show/794-18
26. Закон України «Про Національний банк України» від 20 травня 1999 року. URL: http://zakon2.rada. gov.ua/laws/show/679-14
27. Закон України «Про національну безпеку України» від 21.06.2018 №2496: URL: http://zakon3.rada.gov.ua/laws/show/2469-19
28. Закон України «Про Національну поліцію» від 02 липня 2015 року. URL: http://zakon5.rada.gov.ua/ laws/show/580-19
29. Закон України «Про Національну раду України з питань телебачення і радіомовлення» від 23 вересня 1997 року. URL: http://zakon2.rada.gov.ua/laws/show/538/97-%D0%B2%D1%80
30. Закон України «Про основи національної безпеки України» від 19 червня 2003 року: URL: http://zakon5.rada.gov.ua/laws/show/964-15
31. Закон України «Про основи національної безпеки України» від 19.06.2003 р. – 28.07.2017 URL: www.rada.gov.ua
32. Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року: URL: http://zakon3.rada.gov.ua/laws/show/2163-19
33. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 року: URL: zakon5.rada.gov.ua/laws/show/537-16
34. Закон України «Про Раду національної безпеки і оборони України» від 05 березня 1998 року. URL: http://zakon3.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80
35. Закон України «Про Регламент Верховної Ради України» від 10 лютого 2010 року. URL: zakon.rada.gov.ua/go/1861-17
36. Закон України «Про розвідувальні органи України» від 22 березня 2001 року. URL: http://zakon3.rada.gov.ua/laws/show/2331-14
37. Закон України «Про Службу безпеки України» від 25 березня 1992 року. URL: http://zakon3.rada. gov.ua/laws/show/2229-12
38. Закон України «Про Службу зовнішньої розвідки України» від 01 грудня 2005 року. URL: http://zakon3.rada.gov.ua/laws/show/3160-15
39. Закон України «Про телекомунікації» від 18.11.2003 року: URL: zakon2.rada.gov.ua/laws/show/1280-15
40. Захаренко К.В. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі. Гуманітарний вісник ЗДІА. 2018. Випуск 72. С. 44-52
41. Захисту інформації України» від 23 лютого 2006 року. URL: http://zakon2.rada.gov.ua/laws/show/3475-15
42. Золотар О.О. Інформаційна безпека людини:теорія і практика : монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 446 с
43. ІТ-індустрія опинилася на третьому місці в структурі експорту України https://news.finance.ua/ua/news/-/411572/it-industriya-opynylasya-natretomu-mistsi-v-strukturi-eksportu-ukrayiny-infografika
44. Как сегодня обезопасить кибербезопасность завтрашнего дня? URL: https://www.kaspersky.ru/blog/ dublin-forum-2016/13013/
45. Картка законопроекту «Про основні засади забезпечення кібербезпеки України»: URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\_2?pf3516=2126%D0%B0&skl=9
46. Коментар до проекту Доктрини інформаційної безпеки України. URL: http://www.rainbow.gov.ua/news/942.html
47. Конвенція про кіберзлочинність. URL: http://zakon0.rada.gov.ua /laws/show/994\_575
48. Конвенція Ради Європи "Про доступ до офіційних документів". URL: http://zakon3.rada.gov.ua/laws/show/994\_a33
49. Конституція України: Основний Закон України від 28.06.1996 № 254к/96-ВР. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
50. Литвин М.М., Кохан В.Г. Умови та фактори внутрішньої загрози національній безпеці України. URL: plesetsk-info.ru/uchebnoeposobie/umovi-ta-faktori-vnutrshno-zagrozi-natconalni-bez
51. Маркеева А.В. Интернет вещей (IOT): возможности и угрозы для современных организаций. URL: https://cyberleninka.ru/article/n/internetveschey-iot-vozmozhnosti-i-ugrozy-dlya-sovremennyh-organizasiy
52. Мирошниченко М.М. Правове забезпечення інформаційної безпеки держави: автореф. дис. ... канд. юрид. наук: 12.00.07. Київ, 2018. 19 с.
53. Мнения экспертов Молдовы: Законопроекты в области информационной безопасности противоречат друг другу, то есть ведут к злоупотреблениям. URL: http://www.allmoldova.com/ru/project/mnenie/mnieniia-ekspiertov-moldovyzakonoproiekty-v-oblasti-informatsionnoi-biezopasnosti-protivoriechat-drughdrughu-to-iest-viedut-k-zloupotrieblieniiam
54. Молдова: Национальный ИКТ-профайл (Информационная безопасность и защита информации). URL: https://digital.report/moldovainformatsionnaya-bezopasnost/
55. Палата представників Конгресу США підтримала законопроект з $250 млн для оборони України. URL: https://www.pravda.com.ua/news/2018/05/25/7181305/
56. Персональные данные: новые правила в Европейском Союзе. URL: https://habrahabr.ru/post/300348/
57. Пилипчук В.Г. Інформаційна сфера як складова гібридної війни. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ : Нац. акад. СБУ, 2018. 408 с
58. План дій Україна-НАТО (за матеріалами Національного центру з питань Євроантлантичної інтеграції України. URL: http://www.nceai.gov.ua/plan.phtml
59. Польща створює Доктрину інформаційної безпеки. URL:http://www.eurointegration.com.ua/news/2015/07/26/7036321/
60. Попова Т. Безпека інформаційного простору України. Координувати чи ні? URL: http://www.radiosvoboda.org/a/28337376.html
61. Про доступ до інформації, яка знаходиться в розпорядженні державних органів: Рекомендації Ради Європи № R (81)19. URL: http://medialaw.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-doinformatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv
62. Проблеми застосування в Україні норм інформаційної безпеки НАТО. URL: http://www.db.niss.gov.ua/docs/ polmil/1fgs93.htm
63. Програма «Шлях Європи до Інформаційного Суспільства. План Дій» (Europe’s Way to the Information Society. An Action Plan)" URL: http://i.lekciya.com.ua/doc/3177/index.html?page=17; Europe’s Way to the Information Society. An Action Plan: URL: https://publications.europa.eu/en/publication-detail/-/publication/deed9eb9-0b6e-11e4-a7d0-01aa75ed71a1/language-en
64. Проданюк Р. І. Інформаційна безпека в соціологічному контексті: до постановки проблеми. Науково-теоретичний альманах «Грані». 2018. Т. 21. № 4. С. 84-90
65. Проект Закону України «Про державне стратегічне планування». URL: me.gov.ua http://me.gov.ua/Documents/Detail?lang=ukUA&isSpecial=True&id=e7b8af7a-7c03-4d5b-aaa5-e1c0d7e84388&title=ProektZakonuUkrainiproDerzhavneStrategichnePlanuvannia
66. Рада ухвалила закон про кібербезпеку: URL: https://www.epravda.com.ua/news/2017/10/5/629817/
67. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://journ.univ.kiev.ua/trk/publikacii/satshuk\_publ.php
68. Страны СНГ будут сотрудничать в борьбе с киберпреступностью: URL: https://www.ritmeurasia.org/news--2017-08-28--strany-sng-budut-sotrudnichat-v-borbe-s-kiberprestupnostu-32043
69. Структура керівних документів державної політики в інформаційній сфері: нагальні проблеми та шляхи впорядкування: URL: http://www.niss.gov.ua/articles/572/
70. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. URL: http://nbuviap.gov.ua/index.php?option=com\_content&view=article&id=2760:doktrina-informatsijnoji-bezpeki-yak-zasib-protidiji-informatsijnim-zagrozam2&catid=63&Itemid=393
71. Ткачук Т. Ю. Аксіологічні константи інформаційної безпеки держави. Актуальні проблеми управління інформац. безпекою держави : мат. всеукр. наук.-практ. конф. (Київ, 30.03.18). НА СБУ, 2018. С. 167–169
72. Ткачук Т. Ю. Аксіологічні складові об’єкта правового забезпечення інформаційної безпеки України. Сучасна юриспруденція Європейського Союзу: взаємодія права, нормотворчості та практики: мат. міжнарод. наук.-практ. конф. (Люблін, 17.04.18). 2018. С. 83–86
73. Ткачук Т. Ю. Взаємозв’язок національних цінностей, інтересів та цілей у концепції правового забезпечення інформаційної безпеки держави. Права, свободи і безпека людини в інформаційній сфері : мат. наук.-практ. конф. (Київ, 10.05.18). 2018. С. 47–50
74. Ткачук Т. Ю. Інформаційна безпека держави у національному законодавстві європейських країн. Visegrad Journal on Human Rights. 2018. № 1. С. 145–150
75. Ткачук Т. Ю. Інформаційний чинник у гібридній війні. Кібербезпека у системі нац. безпеки України: пріоритетні напрями розвитку : мат. наук. круглого столу (Маріуполь, 26.04.18). МДУ, 2018. С. 39–42
76. Ткачук Т. Ю. Политика информационной безопасности НАТО. Legea si Viata. 2018. № 5. С. 187–191
77. Ткачук Т. Ю. Теоретичний дискурс пошуку основних складових системи інформаційної безпеки держави. Jurnalul juridic national: teorie şi practică. 2018. № 2. С. 45-47
78. Ткачук Т. Ю., Довгань О. Д. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. Інформація і право. 2018. № 2 (25). С. 73–85
79. Ткачук Т. Ю., Довгань О.Д. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. 2018. № 1 (24). С. 89–104.
80. Ткачук Т. Ю., Кравченко О.О. Яким має бути Закон «Про комерційну таємницю»? Вісник АПСВТ. 2017. № 2. С. 10–19
81. Ткачук Т.Ю. Інформаційна безпеки у системі національної безпеки держави. Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку : збірник наукових праць за матеріалами Міжнародної науково-практичної конференції (8 червня 2018 р., м. Острог). Острог: Видавництво Національного університету «Острозька академія», 2018. С. 138-140
82. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 17 січня 2018 року «Про проект Закону України "Про національну безпеку України» від 5 лютого 2018 року № 21/2018: URL: http://zakon3.rada.gov.ua/laws/show/21/2018/paran2#n2
83. Уханова Н.С. Інформаційно-психологічна безпека особистості, суспільства та держави: URL: ippi.org.ua/ ukhanova-ns-informatsiinopsikhologichna-bezpekaosobistosti-suspilstva-ta-derzhavi
84. Уханова Н.С. Інформаційно-психологічна безпека особистості, суспільства та держави: URL: ippi.org.ua/ukhanova-ns-informatsiinopsikhologichna-bezpekaosobistosti-suspilstva-ta-derzhavi
85. Феденько С. Взаємодія України з НАТО у сфері інформаційної безпеки. URL: http://nato.pu.if.ua/old/ jornal/2009/2009-35.pdf
86. Федеральный совет Швейцарии прокомментировал закон об информационной безопасности. URL: http://goldblum.eu/ru/pravovyenovosti/federalnyy-sovet-shveycarii-prokomm/
87. Федеральный совет Швейцарии прокомментировал закон об информационной безопасности. URL: http://goldblum.eu/ru/pravovyenovosti/federalnyy-sovet-shveycarii-prokomm/
88. Хорватія повернула свої території за три дні, а інформаційна війна тривала ще 15 років. URL: http://milnavigator.com.ua/%D1%85%D0%BE%D1%80%D0%B2%D0%B0%D1%82%D1%96%D1%8F-%D0%BF%D0%BE%D0%B2%D0%B5%D1%80%D0%
89. Швейцария признала незаконным сбор IP-адресов в интересах правообладателей URL: http://www.itsec.ru/newstext.php?news\_id=70187
90. Як бачать в ЄС війну на сході України // Український інститут досліджень екстремізму. URL: http://uire.org.ua/novyni/yak-bachat-v-yesviynu-na-shodi-ukrayini/
91. Common Criteria for Information Technology Security Evaluation URL: https://www.commoncriteriaportal.org/
92. Federal Financial Institutions Examination Council (FFIEC).
93. Information Technology Examination Handbook (IT Handbook): Information Security (2016): URL: https://www/ffiec.gov/press/ pdf/ffiec-ithandbook\_information\_security\_booklet.pdf
94. Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri. An Introduction to Information Security: URL: https://doi.org/10.6028/NIST.SP.800-12r1
95. Microsoft вложит в дата-центр в Ирландии дополнительные 170 млн евро. URL: https://www.bka.gv.at/DocView.axd?CobId=52251 http://www.itsec.ru/newstext.php?news\_id=97395
96. National Cyber Security Strategy: Securing our Digital Future. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM: 2009 0149:FIN:EN:PD
97. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec): URL: www.cnss.gov/Assets/pdf/nstissi\_4011.pdf
98. Radicalisation Awareness Network (RAN): URL: http://ec.europa.eu/dgs/hame-affairs/what-we-do/networks/radicalisation\_awareness\_network/ index-en.html