НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет лінгвістики
Кафедра теорії, практики та перекладу англійської мови

«На правах рукопису»
УДК _____

«До захисту допущено»
В.о. завідувача кафедри
Л. І. Тараненко
(підпис) (ініціали, прізвище)
«___»_____20___р.

МАГІСТЕРСЬКА ДИСЕРТАЦІЯ

на здобуття ступеня магістра
зі спеціальності 035 «Філологія»

на тему: «Актуалізація концепту «CYBERSECURITY» у сучасних англомовних текстах нормативно-правової бази міжнародних організацій та особливості його відтворення українською мовою»

Виконав: студент 2 курсу, групи ЛА-91мп
Шумаков Вадим Дмитрович _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник:
к. філол. н., доц. каф. ТППАМ, О.В. Ткачик _____
(науковий ступінь, вчене звання, посада, ініціали, прізвище) (підпис)

Рецензент:
ст.викладач, к.філол.н. Чайковська О.Ю. _____
(науковий ступінь, вчене звання, посада, ініціали, прізвище) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2020

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет лінгвістики
Кафедра теорії, практики та перекладу англійської мови

Рівень вищої освіти – другий (магістерський)
Спеціальність (спеціалізація) – 035 Філологія (035.041 Германські мови та літератури (переклад включно), перша – англійська)

ЗАТВЕРДЖУЮ
В.о. завідувач кафедри
Л. І. Тараненко
(підпис) (ініціали, прізвище)
«___»_____20__р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Шумакову Вадиму Дмитровичу

1. Тема дисертації «Актуалізація концепту «cybersecurity» у сучасних англомовних текстах нормативно-правової бази міжнародних організацій та особливості його вербалізації відтворення українською мовою».

Науковий керівник дисертації: Ткачик Олена Володимирівна, к.філол.н., доц., каф. теорії, практики та перекладу англійської мови.

Затверджені наказом по університету від 29 жовтня 2020 р., № 3165-с.

2. Термін подання студентом дисертації: 27 листопада 2020 р.

3. Об’єкт дослідження: концепт «CYBERSECURITY», актуалізований в англомовних нормативно-правових документах міжнародних організацій, які регулюють питання кібербезпеки.

4. Предмет дослідження: засоби вербалізації концепту «CYBERSECURITY» в англомовних нормативно-правових документах та особливості їх україномовного перекладу.

5. Перелік завдань, які потрібно розробити:

1) вивчити теоретико-методологічну базу сучасної лінгвістики щодо розуміння суті, структури та способів репрезентації концептів;

2) з’ясувати жанрові особливості англомовних текстів нормативно-правової бази міжнародних організацій;

3) встановити структурніо-семантичні особливості вербальної репрезентації концепту “CYBERSECURITY»

4) визначити специфіку перекладу мовних засобів репрезентації концепту «CYBERSECURITY» у нормативно-правових актах та у текстах нормативно-правових документів.

6. Орієнтовний перелік ілюстративного матеріалу: 92 джерела.

7. Орієнтовний перелік публікацій: тези на XII Міжнародній студенскій науково-практичній конференції : «Людина як субєкт міжкультурної комунікації: сучасні тенденції у філології, перекладі та навчані іноземних мов» на тему «Семантичні особливості лексики та фразеології текстів з комп’ютерної безпеки». Також до друку подано статю в Міжнародний науковий журнал «Інтернаука» на тему «Актуалізація концепту «CYBERSECURITY» у сучасних англомовних текстах нормативно-правової бази міжнародних організацій»

8. Дата видачі завдання: 01 жовтня 2019 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	*Обґрунтування теоретичних передумов дослідження*	*до 20.12.2020*	*вик.*
2	*Формування програми й методики дослідження*	*до 20.05.2021*	*вик.*
3	*Аналіз ілюстративного матеріалу та виклад і оформлення результатів дослідження*	*до 10.11.2021*	*вик.*

Студент _____ В. Д. Шумаков
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ О.В Ткачик
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Магістерська дисертація складається зі вступу, трьох розділів, висновків до кожного з них, загальних висновків та списку використаної літератури, який налічує 92 джерела, 2 додатки. Загальний обсяг роботи 145 сторінок.

Актуальність теми пояснюється недостатньою кількістю ґрунтовних праць, які б досліджували способи вербалізації концепту «CYBERSECURITY» в англомовному юридичному дискурсі та особливості їх перекладу.

Ступінь розробленості проблеми у науковій літературі. Проблеми концептології досліджували Е.В. Будаєв (концептологія в аспекті сучасної політичної лінгвістики), Ю.А. Вєдєнєєв (концептологія в аспекті юриспруденції), А.Л. Голованівський (ідеологічні концепти в лексикографічному дискурсі: семантика, прагматика, синтагматика), Дж. Джозеф (концептуалізація понять у лінгвістиці), В.І. Карасик (базові характеристики лінгвокультурних концептів), Н.В. Сиромятнікова, К. С. Кубрякова, Т.Б. Крючкова (поняття концепту в когнітивній лінгвістиці) тощо; перекладознавчими аспектами займались І.С. Алексєєва, В.В. Алімов, Л.С. Бархударов, К. Басснетт, М. Бейкер, В.Н. Комісаров, В.М. Крупнов, Р.К. Міньяр-Бєлоручев, С.А. Манник, Л.Л. Нелюбін, П. Ньюмарк, Я.І. Рецкер, М. Снелл-Хорнбі, А.В. Федоров, Б. Хатім, А.Д. Швейцер тощо.

Об'єкт дослідження – концепт «CYBERSECURITY», актуалізований в англомовних нормативно-правових документах міжнародних організацій, які регулюють питання кібербезпеки.

Предмет дослідження засоби вербалізації концепту «CYBERSECURITY» в англомовних нормативно-правових документах та особливості їх україномовного перекладу.

Мета роботи полягає в дослідженні засобів вербалізації концепту «CYBERSECURITY» в англомовних нормативно-правових документах міжнародних організацій та їх перекладі.

Для вирішення поставленої у роботі мети необхідно розглянути низку **завдань:**

- вивчити теоретико-методологічну базу сучасної лінгвістики щодо розуміння суті, структури та способів репрезентації концептів;

- з'ясувати жанрові особливості англомовних текстів нормативно-правової бази міжнародних організацій;

- встановити структурніо-семантичні особливості вербальної репрезентації концепту "CYBERSECURITY»

- визначити специфіку перекладу мовних засобів репрезентації концепту «CYBERSECURITY» у нормативно-правових актах та у текстах нормативно-правових документів.

Цілі і завдання зумовили вибір **методів дослідження**. Для дослідження способів актуалізації концепту «CYBERSECURITY» в англомовних нормативно-правових документах міжнародних організацій та їх перекладу використано методи: ***описово-аналітичний метод***, що дозволяє детально і системно охарактеризувати досліджуваний матеріал; ***порівняльний аналіз*** оригіналу і перекладу, що виявляє схожість і відмінність у використанні мовних засобів двох розглянутих мов та дозволяє краще визначити особливості кожної із досліджуваних мов; ***метод класифікації*** для дитального класифікування видів концептів, та їх значень у текстах правового жанру; ***метод суцільної вибірки*** використовувався для добору фактичного матеріалу з текстів оригіналу; ***кількісний метод*** – для обрахунків результатів щодо перекладацьких трансформацій; ***методи аналізу та синтезу*** при дослідженні теоретико-методологічної бази, ***індуктивно-дедуктивний метод*** для виокремлення специфічних характеристик концептів та їх узагальнення при формулюванні висновків.

Матеріалом дослідження слугували 100 фрагментів нормативно-правових актів міжнародних організацій та їхні відповідні переклади українською. Приклади відібрано методом суцільної вибірки.

Наукова новизна дослідження полягає в тому, що концепт «CYBERSECURITY» як один з найважливіших вербально об’єктивованих позицій англомовної картини світу було розглянуто на матеріалі нормативно-правових документів міжнародних організацій, які регулюють питання кібербезпеки. Також було встановлено особливості мовного відтворення зазначеного концепту в українській мові на основі перекладу текстів нормативно-правових актів міжнародних організацій.

Теоретична значущість полягає у використанні в процесі концептуального аналізу елементів функціонального підходу, що передбачає аналіз функціональної природи мовних одиниць як засобів вираження мислення і формулювання думки. Це дозволяє підтвердити тезу щодо взаємозв'язку системності розумової і мовної ролі розпізнавальних (релевантних) ознак. Аналіз функціонування лексем, насамперед ядерних, виявив додаткові змістовні ознаки концепту «CYBERSECURITY».

Практична значимість. Полягає у тому, що результати представленого у ній дослідження можуть бути використані для подальших досліджень концепту "CYBERSECURITY" як невід’ємної складової нормативно-правових документів; також у перекладацькій діяльності, зокрема для покращення якості перекладу зазначених текстів; а також у навчальному процесі; в практиці вивчення англійської мови як іноземної; в навчанні теорії і практики перекладу, для підготовки професійних перекладачів, а також при складанні навчальних посібників з курсів "Когнітивна лінгвістика", "Практика перекладу" та інших.

Апробація результатів дослідження. Основні методологічні, теоретичні результати і концептуальні положення дослідження обговорювалися на: XII Міжнародній студенскій науково-практичній конференції «Людина як субєкт міжкультурної комунікації: сучасні тенденції у філології, перекладі та навчані іноземних мов».

Публікації. Основні положення і результати дисертаційного дослідження висвітлено в тезі на XII Міжнародній студенскій науково-практичній конференції : «Людина як субєкт міжкультурної комунікації: сучасні тенденції у

філології, перекладі та навчані іноземних мов» на тему «Семантичні особливості лексики та фразеології текстів з комп'ютерної безпеки». Також до друку подано статю в Міжнародний науковий журнал «Інтернаука» на тему «Актуалізація концепту «CYBERSECURITY» у сучасних англомовних текстах нормативно-правової бази міжнародних організацій»

Ключові слова: концепт, репрезентація концептів, кібербезпека, нормативно-правові документи, резолюції, перекладацькі трансформації.

SUMMURY

The master's dissertation consists of an introduction, three sections, conclusions to each of them, general conclusions, and a list of references, which includes 92 sources, 2 appendices. The total volume of the work is 145 pages.

Actuality of theme explained by the lack scientific works, that would explore ways to verbalize the concept of "CYBERSECURITY" in English-language legal discourse and the peculiarities of it’s translation.

The degree of elaboration of the problem in the scientific literature. Problems of conceptology were studied by E.V. Budaev (conceptology in the aspect of modern political linguistics), Yu .A. Vedeneev (conceptology in the aspect of jurisprudence), A. L. Golovanovsky (ideological concepts in lexicographic discourse: semantics, pragmatics, syntagmatics), J. Joseph (conceptualization of concepts in linguistics), V. I. Karasyk (basic characteristics of linguistic and cultural concepts), N. V. Syromyatnikov, K. S. Kubryakov, T. B. Kryuchkova (concept of concept in cognitive linguistics), etc .; IS was engaged in translation studies aspects. Alekseeva, V. V. Alimov, L. S. Barkhudarov, K. Bassnett, M. Baker, V. N. Komissarov, V. M. Krupnov, R. K. Minyar-Beloruchev, S. A. Mannik, L .L. Nelyubin, P. Newmark, Y. I. Retsker, M. Snell-Hornby, A. W. Fedorov, B. Khatim, A. D. Schweizer, etc.

Object of study is the concept of "CYBERSECURITY", actualized in English-language legal documents of international organizations that regulate cybersecurity issues.

Subject of study means of verbalization of the concept "CYBERSECURITY" in English-language legal documents and features of it’s translation into Ukrainian.

The purpose of the work is to study the means of verbalizing the concept of "CYBERSECURITY" in English-language legal documents of international organizations and it’s translation.

To solve the goal set in the work it is necessary to consider a number of **tasks**:

- to study the theoretical and methodological basis of modern linguistics in understanding the essence, structure and methods of representation of concepts;

- to find out the genre features of English texts of the legal framework of international organizations;

- to establish structural and semantic features of verbal representation of the concept "CYBERSECURITY"

- to determine the specifics of the translation of linguistic means of representation of the concept "CYBERSECURITY" in regulations and in the texts of regulations.

Goals and objectives led to the choice of **research methods**. To study ways to actualize the concept of "CYBERSECURITY" in English-language legal documents of international organizations and it's translation, the range of methods were used: ***descriptive-analytical method*** that allows detailed and systematic characterization of the studied material; ***comparative analysis*** of the original and translation, which reveals the similarities and differences in the use of language tools of the two languages and allows to better identify the features of each of the studied languages; ***classification method*** for detailed classification of types of concepts and their meanings in legal genre texts; ***the method of continuous sampling*** was used to select the actual material from the original texts; ***quantitative method*** - for calculations of results on translation transformations; ***methods of analysis and synthesis*** in the study of theoretical and methodological basis, ***inductive-deductive method*** for identifying specific characteristics of concepts and their generalization in formulating conclusions.

Research material served 100 fragments of regulations of international organizations and their respective translations into Ukrainian. Examples were selected by the method of continuous sampling.

Scientific novelty of the study is that, the concept of "CYBERSECURITY" as one of the most important verbally objectified positions of the English-language picture of the world was considered on the basis of legal documents international organizations that regulate cybersecurity issues. Peculiarities of linguistic reproduction of this concept in the Ukrainian language on the basis of translation of texts of normative legal acts of international organizations were also established.

Theoretical significance is to use in the process of conceptual analysis of the elements of the functional approach. The functional approach involves the analysis of the functional nature of language units and language in general, which emphasizes the purpose of the language unit. This allows us to confirm the thesis about the relationship between the systemic mental and linguistic role of cognitive (relevant) features. Analysis of the functioning of tokens, primarily nuclear, revealed additional substantive features of the concept of "CYBERSECURITY".

Practical significance. It is that the results of the study presented in it can be used for further research of the concept of "CYBERSECURITY" as an integral part of legal documents; also in translation activities, in particular to improve the quality of translation of these texts; as well as in the educational process; in the practice of learning English as a foreign language; in teaching the theory and practice of translation, for the training of professional translators, as well as in compiling textbooks for the courses "Cognitive Linguistics", "Translation Practice" and others.

Approbation of research results. The main methodological, theoretical results and conceptual provisions of the study were discussed at: XII International student scientific-practical conference "Man as a subject of intercultural communication: current trends in philology, translation and foreign language learning"

Publications. The main provisions and results of the dissertation research are highlighted in the thesis at the XII International Student Scientific and Practical Conference: "Man as a subject of intercultural communication: current trends in philology, translation and foreign language learning" on "Semantic features of vocabulary and phraseology of computer security texts ». Also published is an article in the International Scientific Journal "Internauka" on "Updating the concept of" CYBERSECURITY "in modern English texts of the regulatory framework of international organizations."

Keywords: concept, cybersecurity, legal documents, representation of concepts, translation transformations.

ЗМІСТ

ВСТУП

На межі тисячоліть лексика англійської мови зазнала суттєвих змін, пов’язаних з виникненням нових понять, які потребували відповідної номінації. Через розширення сфер людської діяльності словниковий склад постійно оновлюється. До загальновживаних слів додаються нові лексеми. Кінець XX – початок XXI століть ознаменувався динамічним розвитком Інтернет-технологій, який призвів до тенденцій постійного поповнення англійської лексики. Інтернет-технології принесли не лише багато користі та величезний прогрес у суспільство, а й численні небезпеки та загрози, які породили новий вид діяльності – кібернетичну безпеку. Надійна і захищена робота мереж передачі даних, комп'ютерних систем і мобільних пристроїв є найважливішою умовою для функціонування держави і підтримки економічної стабільності суспільства. На безпеку роботи ключових інформаційних систем загального користування впливає багато факторів: кібератаки, порушення, викликані загрозою фізичної розправи, вихід з ладу програмного та апаратного забезпечення, людські помилки. Перераховані явища наочно демонструють, наскільки сучасне суспільство залежить від стабільності роботи інформаційних систем. Нормативно-правове регулювання такого нового для нашого суспільства явища, як кібербезпека, має мати системний характер і втілюватися як на науковоконцептуальному рівні, так і на рівні формування політики у цій сфері, а також на рівні механізму правового регулювання через приписи і норми, затверджені у нормативно-правових актах. Сьогодні швидкими темпами розвивається термінотворення й застосування термінів, які використовуються у законодавстві у галузі кібербезпекової політики. Вибір текстів нормативно-правових документів в якості джерела матеріалу для мовно-стилістичного аналізу обумовлений інтересом сучасної лінгвістики до своєрідної мовної структури нормативно-правового документа, його функціональної специфіки, до особливостей його змісту, цільового призначення, які відбивають специфіку мовної свідомості особистостей, які здійснюють комунікацію в сфері

правотворчості. Специфіка ця обумовлена не тільки своєрідністю мовної особистості комунікантів, а й особливостями самої сфери діяльності, яка має тривалу історію існування, що сформувалася під впливом різних мовних і немовних факторів особливої мови (мова закону), яка багато в чому відрізняється від природно національної української мови.

Магістерська дисертація складається зі вступу, трьох розділів, висновків до кожного з них, загальних висновків та списку використаної літератури, який налічує 92 джерела, 2 додатки. Загальний обсяг роботи 145 сторінок.

Актуальність теми пояснюється недостатньою кількістю ґрунтовних праць, які б досліджували способи вербалізації концепту «CYBERSECURITY» в англомовному юридичному дискурсі та особливості їх перекладу.

Ступінь розробленості проблеми у науковій літературі. Проблеми концептології досліджували Е.В. Будаєв (концептологія в аспекті сучасної політичної лінгвістики), Ю.А. Вєдєнєєв (концептологія в аспекті юриспруденції), А.Л. Голованівський (ідеологічні концепти в лексикографічному дискурсі: семантика, прагматика, синтагматика), Дж. Джозеф (концептуалізація понять у лінгвістиці), В.І. Карасик (базові характеристики лінгвокультурних концептів), Н.В. Сиромятнікова, К. С. Кубрякова, Т.Б. Крючкова (поняття концепту в когнітивній лінгвістиці) тощо; перекладознавчими аспектами займались І.С. Алексєєва, В.В. Алімов, Л.С. Бархударов, К. Басснетт, М. Бейкер, В.Н. Комісаров, В.М. Крупнов, Р.К. Міньяр-Бєлоручев, С.А. Манник, Л.Л. Нелюбін, П. Ньюмарк, Я.І. Рецкер, М. Снелл-Хорнбі, А.В. Федоров, Б. Хатім, А.Д. Швейцер тощо.

Об’єкт дослідження – концепт «CYBERSECURITY», актуалізований в англомовних нормативно-правових документах міжнародних організацій, які регулюють питання кібербезпеки.

Предмет дослідження засоби вербалізації концепту «CYBERSECURITY» в англомовних нормативно-правових документах та особливості їх україномовного перекладу.

Мета роботи полягає в дослідженні засобів вербалізації концепту «CYBERSECURITY» в англомовних нормативно-правових документах міжнародних організацій та їх перекладі.

Для вирішення поставленої у роботі мети необхідно розглянути низку **завдань:**

- вивчити теоретико-методологічну базу сучасної лінгвістики щодо розуміння суті, структури та способів репрезентації концептів;

- з'ясувати жанрові особливості англомовних текстів нормативно-правової бази міжнародних організацій;

- встановити структурніо-семантичні особливості вербальної репрезентації концепту "CYBERSECURITY»

- визначити специфіку перекладу мовних засобів репрезентації концепту «CYBERSECURITY» у нормативно-правових актах та у текстах нормативно-правових документів.

Цілі і завдання зумовили вибір **методів дослідження**. Для дослідження способів актуалізації концепту «CYBERSECURITY» в англомовних нормативно-правових документах міжнародних організацій та їх перекладу використано методи: ***описово-аналітичний метод***, що дозволяє детально і системно охарактеризувати досліджуваний матеріал; ***порівняльний аналіз*** оригіналу і перекладу, що виявляє схожість і відмінність у використанні мовних засобів двох розглянутих мов та дозволяє краще визначити особливості кожної із досліджуваних мов; ***метод класифікації*** для дитального класифікування видів концептів, та їх значень у текстах правового жанру; ***метод суцільної вибірки*** використовувався для добору фактичного матеріалу з текстів оригіналу; ***кількісний метод*** – для обрахунків результатів щодо перекладацьких трансформацій; ***методи аналізу та синтезу*** при дослідженні теоретико-методологічної бази, ***індуктивно-дедуктивний метод*** для виокремлення специфічних характеристик концептів та їх узагальнення при формулюванні висновків.

Матеріалом дослідження слугували 100 фрагментів нормативно-правових актів міжнародних організацій та їхні відповідні переклади українською. Приклади відібрано методом суцільної вибірки.

Наукова новизна дослідження полягає в тому, що концепт «CYBERSECURITY» як один з найважливіших вербально об'єктивованих позицій англомовної картини світу було розглянуто на матеріалі нормативно-правових документів міжнародних організацій, які регулюють питання кібербезпеки. Також було встановлено особливості мовного відтворення зазначеного концепту в українській мові на основі перекладу текстів нормативно-правових актів міжнародних організацій.

Теоретична значущість полягає у використанні в процесі концептуального аналізу елементів функціонального підходу, що передбачає аналіз функціональної природи мовних одиниць як засобів вираження мислення і формулювання думки. Це дозволяє підтвердити тезу щодо взаємозв'язку системності розумової і мовної ролі розпізнавальних (релевантних) ознак. Аналіз функціонування лексем, насамперед ядерних, виявив додаткові змістовні ознаки концепту «CYBERSECURITY».

Практична значимість. Полягає у тому, що результати представленого у ній дослідження можуть бути використані для подальших досліджень концепту "CYBERSECURITY" як невід'ємної складової нормативно-правових документів; також у перекладацькій діяльності, зокрема для покращення якості перекладу зазначених текстів; а також у навчальному процесі; в практиці вивчення англійської мови як іноземної; в навчанні теорії і практики перекладу, для підготовки професійних перекладачів, а також при складанні навчальних посібників з курсів "Когнітивна лінгвістика", "Практика перекладу" та інших.

Апробація результатів дослідження. Основні методологічні, теоретичні результати і концептуальні положення дослідження обговорювалися на: XII Міжнародній студенській науково-практичній конференції : «Людина як субєкт міжкультурної комунікації: сучасні тенденції у філології, перекладі та навчані іноземних мов» на тему «Семантичні особливості лексики та фразеології текстів

з комп’ютерної безпеки». Також до друку подано статю в Міжнародний науковий журнал «Інтернаука» на тему «Актуалізація концепту «CYBERSECURITY» у сучасних англомовних текстах нормативно-правової бази міжнародних організацій»

РОЗДІЛ 1

ЖАНРОВІ ОСОБЛИВОСТІ СУЧАСНИХ АНГЛОМОВНИХ ТЕКСТІВ НОРМАТИВНО-ПРАВОВОЇ БАЗИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ

Правовий текст є одним з найбільш затребуваних, актуальних і складних сучасних текстів, головним концептом якого є право, а ключовою складовою — мова права. Правовий текст орієнтований на всі верстви суспільства і об'єднує велику кількість учасників: державу, представлену органами правосуддя, офіційними і правоохоронними органами, а також юридичні та фізичні особи: компанії, громадяни, які виступають у різних якостях. Наприклад, як свідки, відповідачі, позивачі і так далі. Правовий текст дослідники визначають як особливий тип соціокомунікативні взаємодії, що реалізується в ситуації інституційного спілкування, підпорядкованого інтенції державно-правового регулювання (А. А. Атабекова, В. Т. Кабиш, Н. Н. Удіне, Н. Г. Храмцова та ін.).

1.1 Загальні жанрові особливості текстів нормативно-правової бази міжнародних організацій

Правовий текст реалізується через декілька каналів: по-перше, через усний (аудіальний) канал — наприклад, судова мова або допит свідків, по-друге, письмовий (візуальний) — в текстах правових документів — Конституції, кодекси, закони, акти і т. д. У цій роботі розглянемо письмову форму реалізації правового тексту, яка за своєю природою взаємодіє зі сферою уявлення тексту документа. Всі письмові форми реалізації правового тексту є документами. Під документом розуміється «письмовий текст, що виходить з інстанцій і від імені осіб, наділених особливими повноваженнями, який виконує регулятивну функцію, що містить суспільно значиму інформацію і оформлений в установленому порядку» [56, с. 53]. Текст документа охоплює особливим чином оформлені письмові зони інституційних текстів, що виконують офіційно задану

функцію регулювання поведінки людини як члена соціальної групи (технічні документи регулюють виробництво і використання технічних засобів, медичні — поведінку лікаря і пацієнта в інституті медицини, освітні — поведінку педагогів і студентів/учнів в інституті освіти і т. д.). Правовий текст в якості соціальної групи передбачає окрему державу і регулює поведінку громадянина і представників державних органів, а також громадян між собою. Метою правового тексту є державно-правове регулювання: «правовий текст являє собою соціально комунікативну діяльність суб'єктів правових відносин щодо встановлення необхідної нормативної впорядкованості поведінки в сфері правового спілкування. Взаємодія письмової форми правового тексту з текстом документа надає йому особливого значення: по-перше, документна специфіка визначає їх стабільність — такі тексти офіційно закріплені в законодавстві (на відміну, наприклад, від передвиборних промов політиків, які не мають нормативного закріплення в системі державного регулювання), по-друге, як наслідок, — вони отримують повсюдну поширеність і абсолютну впізнаваність, яка дає можливість транслювання авторитетної соціально значимої інформації. Правовий текст представлений сукупністю текстів, створених з метою формування сучасного правового простору.

В тематику текстів означеного тексту включається широкий спектр концептів права *(law, defamation, infringement, law, justice, reputation, evidence, dignity, security, threat, truth, plaintiff, guilt, witness, morality, court, honor, sentence* та ін.). Зміст юридичного тексту визначає його мету: інформаційну, аналітичну, оцінну, впливу і прогнозуючу. Поняття концепту тісно пов'язане з поняттям картини світу, юридичний або правовий концепт, відповідно, пов'язаний з юридичною (правовою) картиною світу. В юриспруденції правова картина світу є предметом дослідження порівняльного правознавства. Загальну правову картину світу можна представити у вигляді сукупності безлічі існуючих і функціонуючих в сучасному суспільстві взаємопов'язаних національних правових систем, які обумовлені системою і національними особливостями права конкретної держави. Термін «правова картина світу» дослідники

співвідносять з усталеним в теорії права терміном «правова дійсність», яка відображена в правовій картині світу і заломлюється в системі права. Правова картина складається з універсальних елементів, «притаманних усім або декільком правовим картинам світу (терміни і висловлені ними поняття, принципи, норми і т.п.) і специфічних, характерних для правової картини світу, сформованої законодавством конкретної держави» [70, с. 44]. Поряд з поняттям «правова картина світу» використовується також термін «юридична картина світу», під якою розуміється стійка і взаємоузгоджена система поглядів на світ і наше місце в ньому з точки зору юриспруденції [8, с. 65].

З точки зору юриспруденції достатньо розгорнуте уявлення про зміст категорії «юридична картина світу» було запропоновано Ю.А. Вєдєнєєвим. Дослідник пише про трирівневу модель правової реальності («три поверхи»), де на першому поверсі знаходяться правові ідеї і цінності, тобто система культурних нормативних координат або юридична картина світу, в якій перебуває конкретна правова система (метаправо). На другому поверсі, на думку вченого, розміщені правові норми та інститути, правила поведінки у форматі дозволів, приписів і заборон, тобто система конкретної позитивації юридичної картини світу або нормативних уявлень про порядок відносин. На третьому поверсі перебувають юридичні факти, дії і події, судові рішення, правові колізії, конфлікти і трансакції. На кожному рівні здійснюються власні юридичні процеси, в основі яких лежить юридична картина світу. Юридична картина світу визначається Ю.А. Вєдєнєєвим як «складова частина правової реальності» [13, с. 645], «система загальних рамкових ціннісно-нормативних орієнтацій і мотивацій» [13, с. 646], як «свого роду колективне несвідоме і свідоме, метауявлення про належний чи неналежний порядок соціальних відносин, очікування права і переживання відсутності права. Перш ніж стати юридичним текстом — нормою або правилом поведінки — право існує у свідомості, мові, комунікації» [13, с. 645]. На думку Ю.А. Вєдєнєєва, юридичне мислення є середовищем панування юридичної картини світу [13, с. 646].

Мова юридичного тексту фіксує свого роду примат юридичної повсякденної картини світу, а це безпосередньо характеризує орієнтацію юридичного дискурсу на реалізацію мети нормування суспільних відносин. Ключовим компонентом юридичної картини світу виступає юридичний концепт. В певній мірі концепт є згорнутою моделлю дискурсу або його фрагментом, в якому латентно присутні всі можливі потенційні реалізації. Кожен тип інституційного дискурсу містить в своїй основі базовий концепт, який імпліцитно проявляє себе на рівні макроінтенції мовців (в юридичному тексті — закон, в релігійному — віра, в політичному — влада тощо). У нашому дослідженні правового тексту зосередимо увагу на такому важливому концепті, як «CYBERSECURITY». На думку М. М. Безкоровайного та А.Л. Татузова, кібербезпека і пов'язаний з нею кіберпростір, може презентуватися такими ключовими складовими: інформаційні ресурси (information resources), комп’ютерна і мережева архітектура (computer and network architecture), способи взаємодії користувачів інформаційними ресурсами (how users interact with information resources) [9, с. 23].

Подібна точка зору є сильно звуженою і досить технократичною, оскільки не відображає повною мірою правові та управлінські аспекти забезпечення кібербезпеки у сучасному інформаційнму суспільстві. Відображення у англомовних нормативно-правових актах принципово інших концептуальних підходів підкреслює роль політичної, управлінської складової, її значення для забезпечення безпеки загалом. Будь-який текст має свою стильову, граматичну і мовну основу, організований з метою передачі інформації. Не є винятком тексти нормативно-правових документів. Від якості мови стилю правових актів залежать чіткість і визначеність вираження мовними засобами волі законодавця. Тексти нормативно-правового типупоєднують в собі риси двох функціональних стилів: офіційно-ділового та науково-технічного, який представлений термінологією різної тематики і способів функціонування. Лексика нормативно-правових документів представлена трьома типами слів. Так, лексичною основою будь-якого документу є загальновживана лексика, другий тип лексики

представлений спеціальною лексикою, що є властивою для офіційно-ділового стилю в цілому і нормативно-правових актів зокрема, третій прошарок – наукова та юридична термінологія, вибір якої обумовлений профілем питань, що регулюються актом. Оскільки мова текстів нормативно-правового типу міжнародних організацій наближається до стилю юридичної літератури, метою вживання спеціальної лексики є точність висловлювання. Спеціальна лексики означених документів завжди вживається в прямому, номінативному значенні. Мову документів нормативно-правових актів міжнародних організацій можна розглядати як приклад реалізації принципу «одне слово – одне значення, одне значення – одне слово». Тому за основу при укладанні юридичної документації приймається так зване «золоте правило інтерпретації» (golden rule of interpretation).

Жанри офіційно-ділового стилю створюються в правовій сфері, де основним стилеутворюючим чинником виступає право як форма суспільної свідомості з відповідним йому видом діяльності. Право як форма суспільної свідомості включає в себе погляди і уявлення про різні юридичні явища, що існують в суспільній практиці під впливом права і його застосування. За правовими уявленнями про закон, правовідносини, законність, юридичну практику завжди в кінцевому рахунку стоять інтереси тих чи інших класів або суспільства в цілому, певні економічні, політичні, побутові та інші «реальні» відносини людей. Юридизація текстів нормативно-правових документів міжнародних організацій зумовлена системою сформованих і закріплених в юридичній практиці правил законодавчої техніки, тенденцією до спрощення, схематизації природної мови, а також потребами законотворчої практики, які полегшують процес комунікації в законодавчій
сфері [70, с. 43]. Мова-стильові аномалії текстів нормативно-правових документів міжнародних організацій обумовлені як низькою мовною компетенцією законодавця, так і характером юридизації природної мови в даній сфері людської діяльності узуально закріпленого характеру. Тексти нормативно-

правових документів несуть на собі відбиток мовної особистості законодавця в особливій сфері людської діяльності – законодавчо-правовій.

1.2 Семантична специфіка лексики документів Організації Об'єднаних Націй та Міжнародного союзу електрозв'язку

Семантичну специфіку лексики документів розглянемо на прикладах ділової документації ООН та Міжнародного союзу електрозв'язку (МСЕ).

Організація Об'єднаних Націй (ООН) — міжнародна організація, створена для підтримки і зміцнення міжнародного миру і безпеки, розвитку міжнародного співробітництва та сприяння глобальному прогресу.

Міжнародний союз електрозв'язку (МСЕ) – спеціалізована установа ООН у сфері глобального електрозв'язку, покликана здійснювати законодавчі, управлінські, виконавчі та консультативні функції, надавати технічну підтримку, розробляти стандарти і правила у сфері електрозв'язку та формулювати рекомендації, спрямовані на активізацію розвитку телекомунікацій та підвищення якості послуг.

Резолюції ООН і МСЕ можна розглядати як частину дипломатичних текстів. Дипломатична мова має свої семантичні та стилістичні особливості. Дипломатичний текст є одним з видів інституціонального дискурсу. Загалом, дипломатична мова поєднує в собі риси відразу декількох елементів різних дискурсів, що передбачає міждисциплінарний характер дослідження. Так, дипломатичний текст стикається, наприклад, з політичним текстом, таким чином, дослідженнями даного питання займаються вчені з різних галузей - політологи, дипломати, перекладачі, юристи та інші. Лінгвістами вивчається, в першу чергу, мова дипломатії як соціолінгвістичний феномен, виявлення особливостей і специфічних ознак, а також його відмінності від інших видів тексту.

Документи ООН та МСЕ можна розділити на два види: статутні та декларативні. Вони розрізняються за цільовими настановами і комунікативною

спрямованістю. Так, статутні документи спрямовані на країни-члени ООН, а декларативні на світове співтовариство.

Відмінною рисою мови сучасної дипломатії є публічність. Всі тексти резолюцій ООН та МСЕ представлені в широкому доступі на кількох Інтернет-ресурсах, що дозволяє провести детальний аналіз досліджуваних документів. Крім того, резолюції ООН та МСЕ публікуються відразу на всіх офіційних мовах організацій. Варто зазначити, що даному типу тексту притаманні особливі мовні кліше і протокольні формули, які дозволяють розглядати його як особливий тип дискурсу серед безлічі інших різновидів тексту.

Наприклад:

(1)*on behalf and instructions* - від імені та за дорученням;

(2)*I beg to inform you - маю честь повідомити;*

(3) *the ambassador presents his compliments - Посол висловлює свою повагу;*

(4)*international understanding - міжнародне взаєморозуміння;*

(5)*strict observance of the resolutions - суворе дотримання резолюцій;*

(6)*International Mother Language Day - Міжнародний День Рідної Мови;*

(7) *on an equitable basis - на справедливій основі;*

(8) *Coordinator for Multilingualism - координатор з питань багатомовності;*

(9) *linguistic diversity - лінгвістичне розмаїття.*

Також у дипломатичних документах використовується спеціальна міжнародна термінологія:

(10) *United Nations (UN) - Організація Об'єднаних Націй (ООН).*

(11) *Security Council (SC) - Рада Безпеки (РБ),*

(12) *General Assembly (GA) - Генеральна Асамблея,*

(13)*status quo - статус-кво,*

(14)*veto - право вето,*

(15)*Secretariat - Секретаріат,*

(16)*international peace and security - міжнародний мир і безпеку,*

(17) *human rights - права людини,*

(18)*official languages / non-official languages - офіційні мови / неофіційні мови,*

(19)*working languages - робочі мови,*

(20) *headquarter - штаб-квартира,*

(21) *member states - держави-члени* [91, с. 283].

Серед інституційних характеристик дипломатичного тексту можна виділити наступні. Багатосторонній характер взаємодії сторін, широкий інформаційний вплив і прагнення до співпраці.

Учасники дипломатичної комунікації поділяються на: 1) представників міжнародних організацій, таких як ООН, МСЕ тощо; 2) представників суспільства загалом.

Відзначимо, що багато дипломатичних документів, в тому числі резолюції ГА ООН, не мають формального автора. Дипломатичний текст можна розглядати з точки зору офіційно-ділового стилю. Основними рисами, характерними для даного стилю є: письмовий вид тексту, традиційні засоби вираження, часте використання кліше, термінів, абревіатур і скорочень, наявність синтаксичного паралелізму, сувора структура тексту. Письмова мова повинна розглядатися як особлива мовна норма, що реалізується в письмовому тексті. Існує 3 фактори, які зумовлюють специфіку писемного мовлення:

• Наявність власних засобів вираження (до них відносяться не тільки знаки алфавіту, але і розділові знаки, абзац, курсив тощо. В усному мовленні це виражається за допомогою інтонації).

• Наявність власних одиниць (букви і слова; на рівні фонем і графем може бути розбіжність усної (звукової) мови і письмової).

• Свій власний лад (одній лексичній одиниці писемного мовлення можуть відповідати дві одиниці усного мовлення або навпаки. Тобто по-різному проявляється омонімія (схожість слів в звуковому відношенні при розходженні значень)).

Використання письмової форми дозволяє будувати мовлення більш обдумано і поступово, підбираючи найбільш підходящі мовні засоби.

Виконуючи письмовий переклад будь-яких офіційних документів, в тому числі міжнародних, слід пам'ятати, що збереження основної частини змісту оригіналу є важливою метою комунікації [64, с.240].

Як зазначено на офіційному сайті Організації, Резолюції ООН є офіційним вираженням думки або волі органів Організації Об'єднаних Націй. Вони включають в себе дві частини: преамбула і постановляюча частина. Преамбула зазвичай містить загальні поняття, на основі яких приймається рішення, висловлюється думка або дається вказівка. Постановляюча частина містить кінцеву думку або міру, яка повинна бути прінята.

Резолюції також можуть мати спеціальні додатки з додатковими документами, наприклад тексти конвенцій. Для позначення офіційних дій, які зачіпають поточні питання використовується термін «рішення». До таких питань відносяться: призначення часу і місця засідань, прийняття доповідей, затвердження текстів з деяких питань, що приймаються за допомогою консенсусу всіх членів органу ООН. Тексти резолюцій та рішень ГА включаються в сесійні збірники, які завжди публікуються за результатами сесії — чергової, спеціальної або надзвичайної. Повні тексти всіх резолюцій ГА з 1946 року можна знайти за допомогою ЮНІСБЕТ (United Nations Biographic Information System), а також через систему офіційних документів ООН. Тексти резолюцій доступні на всіх офіційних мовах ООН (арабська, китайська, англійська, французька, іспанська та російська).

Тексти резолюцій та рішень Ради Безпеки також доступні на вищевказаних ресурсах. Доповіді усно перекладаються на інші п'ять мов. У разі якщо представник будь-якої країни виголошує промову на іншій мові, він сам повинен вжити заходів для того, щоб його промова була перекладена на одну з офіційних мов ГА. Інтерес дослідження текстів Резолюцій ООН та МСЕ обумовлений незвичністю граматичної структури і спеціальної лексики. Однією з особливостей подібних документів є їх функціонально-стилістична орієнтація. Відповідно до класифікації В. В. Калюжної, дипломатичні документи

міжнародних організацій класифікуються на інформативні, що регламентують, підсумкові і резюмуючі жанри [32, с.40].

Резолюції ГА ООН можна віднести до підсумкового жанру дипломатичного підстилю офіційно-ділового стилю писемної мови з суворою системою стилістичних прийомів і стильових рис. Самедовою І.А. були запропоновані такі стильові особливості, характерні для текстів Резолюцій, як:

1. логічність (логічний зв'язок, логічна послідовність викладу) — всі частини тексту пов'язані між собою, речення з'єднуються за допомогою паралельного зв'язку, тобто в більшій частині однотипні за граматичною структурою і мають один і той же суб'єкт. логічність реалізується в тексті на рівні синтаксису (документ починається з преамбули, в якій містяться загальні поняття, потім слідує постановляюча частина з кінцевою думкою).

2. офіційність (забезпечується за допомогою пасивних конструкцій: зусилля, прикладені Департаментом; робота, що проводиться мережею; рішення, прийняте Генеральною Конференцією).

3. неемоційність (початкові слова вживаються в прямому денотативному значенні і позбавлені будь-якої конотації, інформація позбавлена емоційно-оцінних елементів).

4. точність (саме точність забезпечує сувора побудова і вибір спеціальних зворотів в текстах Резолюцій. Точність досягається за рахунок використання спеціальної лексики і вибору граматичних структур) [55, с.166].

І.Р. Гальперін характеризує тексти подібних документів як інформуючі про прийняті рішення і рекомендації Організації [19, с.52].

Як уже було відзначено вище, документ ділиться на преамбулу і постановчу частини. Згідно з дипломатичним словником: «преамбула — це вступна частина міжнародного договору. Зазвичай містить: 1) перелік договірних сторін і осіб, уповноважених на підписання договору, із зазначенням їх звання і посади; 2) вказівка мотивів, що стали підставою для укладення самого договору».

У юридичному словнику преамбула це «вступна частина, що роз'яснює міжнародний договір, закон чи інший правовий акт» [72, с.296].

Преамбула починається з виділеного курсивом дієприкметника: (22) *визнаючи - recognizing;* (23) *підкреслюючи - stressing;* (24) *нагадуючи - recalling;*(25) *особливо відзначаючи - emphasizing;* (26) *підтверджуючи - reaffirming.*

У резолютивній частині пункти починаються з дієслів у теперішньому часі 3 особи однини, дійсного способу: (27) *зазначає - notes;* (28) *підтверджує - affirms;* (29) *закликає - calls upon;* (30) *підкреслює - underlines;* (31) *вітає - welcomes;* (32) *стверджує - endorses;* (33)*рекомендує - encourages;* (34) *просить - requests;* (35)*посилається - recalls;* (36)*настійно рекомендує – urges* [72, с.297].

Документи ООН та МСЕ наповнені лексикою щодо кібербезпеки. Бо інформаційна сфера та сфера захисту безпеки кіберпростору й надалі залишаються найвпливовішими галузями постачання лінгвальних інновацій. Прикладом цього може слугувати лексема information, за допомогою якої було створено парадигму інновацій таких як *information broker, information environmentalism, information fatigue syndrome, information scent, information foraging, information food chain, information pollution, information superiority, information tamer, information warfare.* Усі наведені словосполучення у своїй семантиці містять змістовні складові, що несе в собі семантичний неологізм *information* – належність до новітніх інформаційних комунікаційних технологій. Також все більшою частотністю характеризуються й інші поняття, які відносимо до концептосфери “Cybersecurity“, а саме: *cyberspace, information security, information threats, state information policy, cyberspace; cybersecurity, cyber threat, protection of the information space, cyberdefense policy, computer networks* та ін. Концепт «кібербезпека», який номінується в англійській мові як Cybersafety / Cybersecurity, виступає одним з ключових концептів і вербалізує одну з важливих умов життя в сучасному соціумі — явище інформаційної безпеки. Феномен кібербезпеки в сучасному світі отримало широке висвітлення в наукових лінгвістичних та інших суміжних галузях, що дозволяє говорити про

широку репрезентації даного концепту мовними засобами в лінгвокультурологічній свідомості людини. Внаслідок різноманітності когнітивних установок, залучених у формування ментального образу концепту «CYBERSECURITY» (кібербезпека), можна стверджувати, що останній є компонентом структури концептосфери informational security / safety. Словник термінів, що наповнюють концептосферу «CYBERSECURITY» подано у додатку (Додаток А).

1.3 Тексти резолюційного жанру

Поняття тексту є досить широким і включає в себе кілька смислів: це і зв'язний текст у сукупності з прагматичними, соціокультурними, психологічними та іншими факторами; і це текст у подієвому аспекті [12, с. 146]. Текст є невід'ємним атрибутом усіх сфер життя людини, у зв'язку з чим можна говорити про існування особливого нормативно-правового тексту, що виділяється суб'єктами правовідносин [75; 77; 79; 80].

М. Фуко зауважує важливу особливість у тексті: одні висловлювання вічні, належать до «безперервного», інші ж актуальні лише для певного періоду часу [66, с. 410]. Він передбачає, що завжди є група «незмінних, зв'язкових» понять, як наприклад, у граматиці: «слово», «дієслово». Правосвідомість одвічно звертається до понять «закону», «права», «справедливості», саме ці поняття в контексті правової реальності є незмінними, «зв'язковими».

Значимість висловлювання залежить від того «хто говорить». Ми розуміємо, що висловлювання, що знайшло вираження в тексті нормативно-правового акта і джерелом якого є глава держави має більшу цінність в громадському і державному значенні, ніж висловлювання, закріплене в тексті нормативно-правового акта глави регіону.

Крім того, значимість висловлювання залежить від критерію «новизни». Найцінніші нормативні висловлювання — вперше висловлені в нормативно-правових текстах; менш цінні — ті, що їх повторюють.

Нормативно-правовий текст може поєднуватися з іншими видами тексами різних соціальних інститутів, в залежності від об'єктів знання. Ці тексти відрізняються певними наборами відносин, які визначають межі дискурсів, наприклад: це відношення між площиною судового рішення про винуватість чи невинуватість особи та медичного висновку про осудність, наявність афекту (психологічна характеризація); судового допиту і медичної анкети, обмеження свободи в лікарні і обмеження волі у в'язниці. Як вказує М. Фуко, дисципліни, що вивчаються щодо один до одного можуть знаходитися у відношенні аналогії, опозиції і комплементарності [66, с. 138]. Тексти перебувають у відношенні взаємного обмеження через диференціацію своєї царини застосування, методології.

Відносини між різними текстами різних соціальних інститутів не є для них внутрішніми, «... вони не пов'язують між собою поняття або слова ... речення ...» не присутні в об'єкті, «не влаштовують дедуктивних і риторичних надбудов» [66, с. 103]. Крім того, кожен нормативно-правовий текст заснований на системі диференціації і відносин, адже в нормативно-правовому тексті завжди простежуються соціальні ролі, він заснований на запиті інформації та обмін нею (докази, угоди), крім того, можна говорити про ієрархічне співвідношення дискурсів, в залежності від того який статус текстової оболонки тексту і від того «хто говорить». Залежно від регульованої галузі правовідносин нормативно-правовий текст формують системи понять і текстових актів, які зводяться в теми і теорії. Теорії і теми М. Фуко називає стратегіями.

Сама правосвідомість – це текст про сукупність ідей, теорій, почуттів, емоцій, поглядів, настроїв, установок і цінностей, в яких виражається ставлення людей до права і правових явищ. Носій повсякденної правосвідомості - первинний суб'єкт будь-якої правової реальності, учасник правової комунікації.

Тексти нормативно-правових актів, загалом, не беруться під сумнів, є готовими сполуками, що пов'язують між собою тексти учасників правовідносин.

Нормативний текст – це інформація про правові явища. Дослідники [15; 35; 39] виходять з того, що текст не тотожний мові і (або) мовленню. Текст про правові явища ґрунтується на нормативній мові і виражається у мовленні, нормативно-правових текстах, комунікативних актах. Текст грунтується на висловлюванні, це і є сукупність висловлювань [66, с. 205].

Особливість нормативно-правового тексту в тому, що сукупності висловлювань, розсіяних в часі спрямовані на певну сферу суспільних відносин – правовідносин. Крім того, йому притаманний певний стиль, характер висловлювань, єдиний словник, що дозволяє формувати нормативно-правові тексти (юридична мова), дескриптивні висловлювання (акти).

Висловлювання є атомом для нормативно-правового тексту. М. Фуко підкреслював відсутність тотожності між висловлюванням, з одного боку, і судженням, синтагмо, реченням, з іншого боку [66, с. 160].

Наприклад, «договір», «доказ» — висловлювання, але при цьому вони не є реченнями, думками, синтагмами. Знаки, речення — це форма для висловлювання, система побудови, а висловлювання для речення і судження свого роду наповнення.

Висловлювання є функція в нормативно-правовому тексті в тому сенсі, що носій правосвідомості висловивши щось далі аналізує своє мовлення, текст з тим, щоб переконатися чи правильно, чи коректно, зроблені висловлювання, валідні чи ні. Знайомлячись з текстом нормативно-правового акта носій правосвідомості співвідносить висловлене, відображене в ньому зі своїми інтересами, розумінням, формулюючи висловлювання і створюючи тим самим новий текст.

Вислів «…закликає до існування.» [66, с. 171], це означає, що навіть надрукована, безладна група букв — висловлювання, це все те, що я хочу видати до існування. Звідси випливає, що лінгвістична синтагма не диктує правил побудови висловлювань і тому вона не тотожна вислову.

Речення, судження стає висловлюванням, згідно Фуко, завдяки формуванню в його рамках асоційованого поля (колатерального простору) [66, с. 185].

Це поле формується низкою інших висловлювань, візьмемо, наприклад, послідовність тверджень, що описують обов'язки батьків щодо своїх неповнолітніх дітях, в асоційоване поле виявляємо опис підстав для позбавлення батьківських прав. У разі порушення певної статті настає відповідальність, передбачена Кримінальним кодексом України; асоційовані висловлювання повторюють, змінюють, застосовуються із застереженнями, протиставляються, тобто реактуалізують основне висловлювання або групу висловлювань. Причому висловлювання з асоційованого поля разом з основним розташовуються в асоційоване поле без урахування лінійного порядку. Так, основне висловлювання може міститися в гіпотезі і диспозиції одного нормативно-правового акта, а асоційовані висловлювання в санкції статті цього ж нормативно-правового акта або іншого. Висловлення організовують означувані сукупності. Асоційоване поле разом з основним висловлюванням можна виявити лише завдяки цим означуваним сукупностям.

Висловлювання не тотожне акту висловлювання. Відтворюючи текст нормативно-правового акта (його конкретну норму), носій правосвідомості тим самим здійснює акт висловлювання, який будучи подією відрізняється просторово-часовою неповторністю. М. Фуко писав: «одне і те ж речення, вимовлене двома людьми, хоча і в дещо різних обставинах, утворюють тільки один вислів» [66, с. 196].

Відтворюючи один вислів кілька разів, ми отримуємо кілька актів висловлювань, можна посилатися на одне і те ж нормативне положення, але інтерпретація положення позивачем і відповідачем різниться, оскільки здійснюється стосовно до власного асоціативного полю. В результаті отримуємо два акти висловлювання і два різних висловлювання, хоча вони і виходять з одного загального висловлювання.

Судові рішення завжди, почасти, відтворюють вже існуючі висловлювання - положення нормативно-правового акта. Звідси, відтворення не тотожне вислову. Коли суб'єкт висловлювання звертається до інших лінгвістичних форм (словам, синтаксису, умовному коду), але при цьому залишається в рамках стабілізаційного поля (тобто інформаційний зміст залишається тим самим) - мова йде про одне й те ж висловлювання.

Терміни «стабілізаційний поле» і «асоційоване поле» М. Фуко не розмежовує, і на наш погляд їх межі збігаються. Для нього стабілізаційне поле — це сукупність умов і меж, які пропонуються йому сукупністю інших висловлювань, серед яких воно фігурує, тією цариною, в якій його можна використовувати або застосувати, тією роллю або функціями, яке воно повинно виконувати, «це сукупність, а також схеми використання, правила вживання, констеляції утворюють для висловлювань поле стабілізації, яке, незважаючи на всі відмінності в акті висловлювання, дозволяє повторити їх в тотожності, але це ж поле може також визначити поріг, за яким вже не існує еквівалентності і потрібно визнати появу нового висловлювання» [66, с. 199-200].

Таким чином, вживаючи термін «стабілізаційне поле», М. Фуко позначає межі «невиходу», щоб не втратити тотожність використання висловлювання. Говорячи про асоційоване поле — артикулюється ідея про утворення висловлювань, необхідних для основного висловлювання. Висловлення можна наповнити різним семантичним змістом і на виході різні суб'єкти, в залежності від вкладених смислів отримають різні висловлювання. Наприклад, «чоловіки і жінки рівні» — бачення рівності різниться, залежно від розуміння сенсу індивідом і тим змістом, який вкладав сам законодавець. Правосвідомість визначає особливу дискурсивну практику, яка застосовується в правовій реальності, як в усному мовленні, так і в нормативно-правовому тексті. «Текстова практика — це сукупність анонімних, історичних, завжди детермінованих в часі і просторі правил, які в дану епоху і для даного соціального, економічного, географічного, лінгвістичного сектора визначили умови здійснення функції висловлювання» [66, с. 224].

Будь-який нормативно-правовий текст формується і транслюється в рамках цієї практики, і ось деякі її особливості.

1. Оповідальна структура нормативно-правового тексту як і будь-якого іншого — предикативна. Оповідальна синтагма тексту нормативно-правового акта має імплікативний вид: якщо..то..інакше... ». Ця словесна формула відображає класичний вид структури норми права. В інших випадках оповідальна структура розрізняється залежно від виду нормативно-правового тексту, так, судове рішення складається із: вступної, мотивувальної, описової та резолютивної частини. Дерріда вказував на те, що в літературному творі завжди є лінія, яку потрібно виявити, яка дозволяє пояснити його єдність і цілісність. Ця лінія організовує структуру твору, його внутрішню єдність членування. Для нормативно-правового тексту в таку лінію організовані принципи права, тобто основні, вихідні основи права, які визначають оповідальну синтагму, критерії для побудови тексту нормативно-правового акта.

2. Оповідь нормативно-правового тексту підпорядковується вимогам правдивості, але ні в якому разі не правдоподібності. Так, нормативно-правове встановлення будь-якого нормативно-правового акта несе в собі завдання-введення певних правил поведінки, і при цьому у встановленні імпліцитно закладений критерій власної валідності реальним потребам держави і суспільства. Ще одним видом мовлення, яке повинне відповідати вимозі правдивості є судова мова. В даному випадку правдивість означає те, що факти, на які посилається особа, повинні відповідати дійсності і закону.

Вимога правдивості, реальності забезпечується якісним, референціальним вибором, здійснюваним в процесі референції законодавця і іншого агента комунікації (суб'єкта висловлювання) і забезпечує відповідність мовного вираження референту. Правдоподібним, згідно Р. Барту, вважається все те, про що домовилися вважати таким і що цілком підпорядковане думці суспільства [8, с. 399]. Тут необхідно уточнити, що правдоподібність цілком може забезпечуватися думкою окремої соціальної групи.

Судовий процес, як нормативно-правовий дискурс, супроводжується трансляцією цілої низки повідомлень, які передаються синхронно, в різних ритмах, мають різні джерела (суддя, сторони тощо). Це все виражається у вигляді лексики і синтаксису повідомлення (усного або письмового). Але суть (сенс) дискурсу: клопотання, скарга, відгук, запитання тощо, в них його реальність. Сама обстановка («атмосфера», технічна оснащеність) судового
процесу важлива, оскільки і через неї транслюються ідеї справедливості, відповідальності носія правосвідомості, законності. Якщо зі статті нормативно-правового акта витягти фрагмент тексту, то апріорно ніщо не відрізняє його від такого ж за інформативною наповненістю фрагмента (повідомлення), висловленого в рамках триваючих правовідносин, наприклад, договірного. Якщо правовідносини є правовою дійсністю, в просторі якої створюється і реалізується нормативно-правовий акт, то останній, в свою чергу, є зразком повинності для самої дійсності. Таким чином, текст нормативно-правового акта містить в собі модель поведінки і в цьому його основне повідомлення, тоді як правова реальність складається із фактичних даностей.

Логос, виражений в нормативно-правовому тексті, не збігається з праксисом правової реальності повністю, але цього і не потрібно для ефективної роботи правової системи, необхідна синхронна робота, динамізм їхнього взаємодії. Нормативно-правовий текст, володіючи властивістю транзитивності, висловлює деякі аспекти правової реальності і бере участь в її становленні, іноді випереджаючи ще не існуюче (приклад, Конституція), а іноді лише трансформуючи. Відносно означуваного нормативно-правового тексту важливо не допустити їх крайнього розбіжності (протилежності). Смисли, закладені в нормативно-правовому тексті повинні бути однозначними, зрозумілими, не повинні суперечити. Законодавець повинен мінімізувати межі між означуваним нормативно-правового тексту.

3. Текст нормативно-правового акта завжди догматичний, оскільки складається зі стверджувальних речень. Навіть незважаючи на те, що диспозиція статті може надавати альтернативи поведінки — проте він представляє собою

догматичний дискурс. Дискурс, закріплений у тексті нормативно-правового акта, відрізняється відсутністю демонстрації аргументів і наявністю стійких формул.

4. Текст нормативно-правового акта абсолютно вільний від діалогу, при цьому, в основі будь-якого нормативно-правового тексту лежить відмінність, а саме відмінність інтересів. Різниця в нормативно-правовому тексті береться під контроль самим фактом включення його в матерію, буття нормативно-правового тексту. Він стає текстуальним, а значить регульованим, обмеженим владним приписом і владою ж гарантованим.

Незважаючи на відсутність в структурі тексту нормативно-правового акта діалогу, такий текст як соціальний простір вимагає співпраці з боку кожного носія правосвідомості.

Будь-який нормативно-правовий текст містить в собі логіку «відповіді або невідповіді адресату тексту». Ж. Дерріда пише: «право, мораль, філософія, політика - ці інститути створювалися як призначені для надання звіту перед ними, тобто відповіді за взяту на себе відповідальність» [26, с. 45]. Ця логіка пронизує всі галузі права, наприклад, у цивільному праві: розділ «зобов'язальне право», «цивільно-правова відповідальність,« договірне право», інститут шлюбу, аліментні зобов'язання членів сім'ї тощо.

5. Нормативно-правовий текст відрізняється специфічною і функціональної лексикою, він найсуворіше кодифікований. При цьому йому не властива емфатичність, за винятком рідкісних випадків, наприклад: преамбула Конституції України як раз емфатична, крім того, принципи законодавства в тій чи іншій галузі права також емфатичні. Говорячи про функціональність лексики, мається на увазі, зокрема, її головна функція – функція переконання.

6. Процес читання і сприйняття нормативно-правового тексту — це рух від загального до конкретного, від одного юридичного терміну до іншого (процес номінації), від принципу до його реалізації.

7. Важливість і значимість ясності мови нормативно-правового акта, як вимоги риторики, була позначена ще Гегелем і актуальна і донині. Наразі ясність юридичної мови, дискурсу є цінністю.

Р. Барт відзначав, що ясність є атрибутом такого типу мовлення, в якому закладена мета — переконати, впливати на людину [8, с. 91]. А також вказує на те, що «універсальність будь-якої мови є фактом говоріння» [8, с. 108], позначаючи проблему «різних мов» окремих соціальних груп. Звідси випливає, що людина є бранцем своєї мови, як мови своєї групи, в першу чергу. «За межами своєї мови вона виявляє себе кожним вимовлених словом, кожне слово виявляє її всього і виставляє напоказ разом зі своєю історією» [8, с. 108]. Таким чином, носій правосвідомості виявляє себе, свою правосвідомість через свій дискурс.

Отже, між правосвідомістю і текстом існує прямий і необхідний зв'язок. Вимога ясності має застосовуватися не тільки до природної мови але і до юридичної мови тексту нормативно-правового акта, а також до мови інших нормативно-правових текстів.

Нормативно-правове мовлення, яким оперує індивід, висловлює суть його правосвідомості. Виникає питання: чи можливе примирення, тобто універсалізація мови нормативно-правового акта і мови носія правосвідомості? Подібне «примирення» є ідеальною метою держави (саме держави) і тоді його відповідальність перед суспільством буде повною і реальної, а звернення до принципу «незнання закону не звільняє від відповідальності» стане непотрібним. Але наразі проблема є в наявності, оскільки, коли дискурс є чужим, незрозумілим, далеким для правосвідомості індивіда, тоді діра в культурному коді тягне несприятливі наслідки і для нього, і для суспільства.

Тож, нормативно-правовий текст включає в себе механізми формування правил поведінки, імперативного або диспозитивного характеру, їх тлумачень, описів, виражених в мові, нормативно-правових текстах і комунікативних актах, джерелом яких є правова свідомість.

Висновки до розділу 1

У розділі визначено, що правовий текст – це особливий тип соціокомунікативної взаємодії, що реалізується в ситуації інституційного спілкування, підпорядкованого інтенції державно-правового регулювання. Основною метою правового тексту є державно-правове регулювання, оскільки означений текст є соціально комунікативною діяльністю суб'єктів правових відносин щодо встановлення необхідної нормативної впорядкованості поведінки в сфері правового спілкування. Тексти нормативно-правового типу поєднують в собі риси двох функціональних стилів: офіційно-ділового та науково-технічного, який представлений термінологією різної тематики і способів функціонування. Особливість нормативно-правового тексту в тому, що сукупності висловлювань, розсіяних в часі спрямовані на певну сферу суспільних відносин – правовідносин. Крім того, йому притаманний певний стиль, характер висловлювань, єдиний словник, що дозволяє формувати нормативно-правові тексти (юридична мова), дескриптивні висловлювання (акти). Визначено, що лексика нормативно-правових документів включає три типи слів. Лексичною основою будь-якого нормативно-правового документу є загальновживана лексика, другий тип лексики представлений спеціальною лексикою, що є властивою для офіційно-ділового стилю в цілому і нормативно-правових актів зокрема, третій прошарок – наукова та юридична термінологія, вибір якої обумовлений профілем питань, що регулюються актом.

З’ясовано, що правосвідомість визначає особливу дискурсивну практику, яка застосовується в правовій реальності, як в усному мовленні, так і в нормативно-правовому тексті. Текстова практика - це сукупність анонімних, історичних, завжди детермінованих в часі і просторі правил, які в дану епоху і для даного соціального, економічного, географічного, лінгвістичного сектора визначили умови здійснення функції висловлювання/

Будь-який нормативно-правовий текст формується і транслюється в рамках цієї практики, і ось деякі її особливості.

1. Оповідальна структура нормативно-правового тексту як і будь-якого іншого – предикативна.

2. Оповідь нормативно-правового тексту підпорядковується вимогам правдивості, але ні в якому разі не правдоподібності.

3. Текст нормативно-правового акта завжди догматичний, оскільки складається зі стверджувальних речень.

4. Текст нормативно-правового акта абсолютно вільний від діалогу, при цьому, в основі будь-якого нормативно-правового тексту лежить відмінність, а саме відмінність інтересів.

5. Нормативно-правовий текст відрізняється специфічною і функціональної лексикою, він найсуворіше кодифікований.

6. Процес читання і сприйняття нормативно-правового тексту — це рух від загального до конкретного, від одного юридичного терміну до іншого (процес номінації), від принципу до його реалізації.

7. Важливість і значимість ясності мови нормативно-правового акта, як вимоги риторики, була позначена ще Гегелем і актуальна і донині. Наразі ясність юридичної мови, дискурсу є цінністю.

РОЗДІЛ 2
ЛІНГВОКОГНІТИВНА СПЕЦИФІКА РЕАЛІЗАЦІЇ КОНЦЕПТУ «CYBERSECURITY» У ТЕКСТАХ НОРМАТИВНО-ПРАВОВОЇ БАЗИ

2.1 Поняття, структура і способи репрезентації концептів у сучасній лінгвістиці

Термін «концепт» у лінгвістиці не новий. Він відноситься до епохи середньовічного концептуалізму, основоположниками якого були Т. Гобс, П. Абеляр, У. Окамі та інші. Концептуалізм розглядав концепти як універсалії, які узагальнюють ознаки речей і створені розумом для його внутрішнього вживання, фокусуючи у собі важливу і актуальну інформацію [1, с. 37].

С.С. Неретіна вважала концептом «сукупність понять, поєднання висловлювань у єдину точку зору на той чи інший предмет за умови визначальної сили розуму» [49, с. 12].

Звернемо увагу на те, що вживання терміна «концепт» актуально і пов'язано з розвитком когнітивного напряму в психології, у мовознавстві і появою спеціальних дисциплін:. когнітивної психології, психолінгвістики та когнітивної лінгвістики.

Прийнято вважати основною категорією когнітивної лінгвістики саме поняття «концепт». Категорія концепту фігурує у дослідженнях філософів, логіків і психологів, вона несе на собі сліди всіх цих позалінгвістичних інтерпретацій [14, с.403].

Період утвердження терміну в науці неодмінно пов'язаний з певною довільністю його вживання, розмитістю кордонів, змішуванням з близькими за значенням або мовними формами терміна.

Важливою є поява терміна концепт на початку XX ст. у науковій, літературі.

С. А. Аскольдов-Алексєєв у 1928 році у статті «Концепт і слово» дав наступне визначення поняття: «Концепт є уявним утворенням, яке замінює

нам у процесі думки невизначену безліч предметів одного і того ж роду» [5, с. 156].

Приблизно у той же час Д. С. Ліхачов використовував поняття концепт для позначення узагальненої розумової одиниці, яка відображає і інтерпретує явища в залежності від особистого досвіду, професійного і соціального досвіду носіїв мови і, будучи свого роду узагальненням різних значень слова в індивідуальній свідомості носіїв мови, дозволяє у спілкуванні долати існуючі індивідуальні відмінності у розумінні слів.

Концепт, за словами Д. С. Ліхачова, не виникає із значень слів, а є результатом зіткнення, засвоєння значення з особистим життєвим досвідом мовця. Концепт, на його думку, виконує замісну функцію в мовленнєвому спілкуванні [42, с.26].

У 80-х роках у зв'язку з перекладом робіт англомовних авторів терміни «концепт», «концептуалізація», «концептуальні сутності» тощо прижилися у слов'яністиці, хоча і сьогодні термін «концепт» не має однозначного тлумачення.

У сучасній когнітивній лінгвістиці стрижневим поняттям стає поняття «концепт», яке в якості терміна використовується дослідниками, що займаються проблемами мовного подання когніцій.

У найзагальнішому вигляді концепт, на думку Ю. С. Степанова, можна уявити, як «згусток культури у свідомості людини: те, у вигляді чого культура входить у ментальний світ людини» [60, с. 93].

Наразі можна виділити різні розуміння терміна «концепт».

Доречно звернути увагу на думку П. В. Чеснокова, який стверджував. що: «Концепт — це одиниця мислення, яка володіє окремим цілісним змістом і реально не розкладається на більш дрібні думки, тобто елементарна сторона внутрішнього шару» [69, с. 13].

Так, М. А. Холодна розкриває поняття «концепт» як «пізнавальну психічну структуру особливості організації якої забезпечують можливість відображення насправді в єдності різноякісних аспектів» [67, с. 201].

Поряд з цим К. С. Кубрякова подає наступне визначення поняття: «концепт — це одиниця ментальних або психічних ресурсів нашої свідомості і тієї інформаційної структури, яка відображає знання і досвід людини; оперативна змістовна одиниця пам'яті, ментального лексикону, концептуальної системи мови і мозку <...>, всієї картин світу, відображеної у людській психіці» [40, с. 4].

Наразі, слід визнати, що саме «концепт» є ключовим поняттям когнітивної лінгвістики. Проте, незважаючи на те, що поняття концепт можна вважати у сучасній когнітивістиці утвердилися, зміст цього поняття дуже істотно варіюється у різних концепціях наукових шкіл і окремих вчених.

Так, Н.В. Сиромятнікова стверджує, що смисли, якими оперує людина у своїй розумовій діяльності і які відображають її досвід і знання зберігаються у вигляді особливих ментальних структур, що отримали в когнітивній науці назву концептів. Інтерпретація концептів безпосередньо пов'язана з дисципліною, об'єктом якої він стає [58, с. 18].

В. І. Карасик, характеризує концепти як «ментальні утворення, які є значущими усвідомлюваними типовими фрагментами досвіду людини, що зберігаються у пам'яті» [27, с. 59], «багатовимірне ментальне утворення у складі якого виділяються образно-перцептивна, понятійна і ціннісна сторони», «фрагмент життєвого досвіду людини» [34, с. 23], «пережита інформація» [33, с.128], «квант пережитого знання» [34, с. 25].

А. Залевська визначає концепт як об'єктивно існуюче у свідомості людини перцептивно-когнітивно-афективне утворення динамічного характеру на відміну від понять і значень як продуктів наукового опису (конструктів) [29, с. 39].

Також А. А. Залевська характеризує нейронну основу концепту, як активізацію багатьох окремих нейронних ансамблів, розподілених по різним ділянкам мозку, що входять в єдиний набір. Доступ до всіх цих ділянок здійснюється одночасно завдяки словам або. якому-небудь іншому знаку [30, с. 53].

З психолінгвістичної точки зору А. А. Залевська підкреслює індивідуальну природу концепту. На її думку концепт «багатовимірна. симультанна структура. Концепт — це надбання індивіда» [30, с. 12].

С. Р. Воркачов визначає концепт як «операційну одиницю думки», як «одиницю колективного знання (що відправляє до вищих духовних сутностей), що має мовне вираження і відзначена етнокультурною специфікою» [17, с. 51-52]. Якщо ментальне утворення не має етнокультурної специфіки, то воно, на думку вченого, до концептів не відноситься.

М. В. Піменова зазначає: «Те що людина знає, вважає, уявляє про об'єкти зовнішнього і внутрішнього світу і є тим, що називається концептом. Концепт - це уявлення про фрагменти світу» [51, с. 51-52].

В.В. Красних дає наступне визначення: «концепт — максимально абстрагована ідея «культурного предмета», що не має візуального прототипічного образу, хоча і можливі візуально-образні асоціації з ним пов'язані» [38, с. 7].

Національний концепт В. В. Красних визначає як «саму загальну, максимально абстраговану, але конкретно репрезентовану (мовну) свідомість, що піддалася когнітивній обробці ідею «предмета», що став сукупністю всіх валентних зв'язків, позначених національно-культурним маркуванням» [38, с. 8]; «свого роду згорнутий глибинний «сенс» «предмета» [38, с. 9]. Таким чином, у розумінні В. В. Красних: «концепт може бути тільки одиницею високого ступеня абстракції, що має національно-культурну специфіку, що виражається словом і включає словесні асоціації на ім'я концепту» [38, с. 10].

У статті «Концепт «Життя»: понятійна і символічна складові» Н.В. Дєєва робить висновок, що концепт є одиницею свідомості людини, яка акумулює знання та досвід, отримані в процесі освоєння навколишньої дійсності [25, с.25].

Іншим джерелом відображення цих знань виступає будь-яка природна мова, що є звуковою книгою про світ. Протягом всієї історії існування людей у процесі пізнання об'єктивного світу створювався якийсь світ смислів, що відображають світ реальний у ідеальній формі. Цей світ смислів і є концепти —

ментальні утворення. Мова у своїх формах матеріалізує нашу свідомість, вона є основним джерелом отримання інформації щодо ментальної сутності. Через мовні одиниці (слова, фразеологізми, вільні словосполучення, речення, тексти) і об'єктивуються концепти [25, с.27].

Найбільш вдале визначення концепту, на думку Р. М. Фрумкіної [65], дала. А. Вежбицька, відзначаючи близькість її підходу до ідей Гумбольдта. Під концептом А. Вежбицька розуміє «об'єкт із світу «ідеальне», що має ім'я і відображає певні культурно-обумовлені уявлення людини про світ «дійсність». Сама дійсність дана нам у мисленні (не у сприйнятті!) саме через мову, а не безпосередньо» [14, с. 407].

Р. М. Фрумкіна ж зазначає, що концепт є об'єктом концептуального аналізу, сенс якого — «простежити шлях пізнання сенсу концепту і записати результат формалізованою семантичною мовою» [65, с. 58].

Варто відзначити, що у словнику М.В. Піменова термін «концепт» самостійною словниковою статтею не представлений, але його значення дається і розкривається у статті «поняття», а «концепт» виділений як синонім, який позначений. у дужках: «Поняття (концепт) — явище того ж порядку, що і значення слова, але розглянуте у дещо іншій системі зв'язків; значення — у системі мови, поняття в системі логічних. відносин і форм, досліджуваних як у мовознавстві, так і логіці» [76, с.15].

Л. О. Чернейко дає можливість зрозуміти «концепти як якісь розумові образи, що стоять за мовними знаками і позначають мовні знаки, які останнім часом стали предметом жвавої уваги лінгвістів. Поняття концепту, яке прийшло з когнітології, виявилося важливим і потрібним для вивчення мови і лягло в основу когнітивної лінгвістики. Із концептів складається семантичний простір конкретного мовлення, а за семантичним простором можна судити про структури знань в їх конкретно-національному переломленні» [68, с. 25].

А.Б. Бабушкін у монографії «Типи концептів у лексико-фразеологічній системі мови» розглядає концепти як структури подання знань. Він розуміє концепт «як будь-яку дискретну змістовну одиницю колективної свідомості, що

відображає предмет реального або ідеального світу та зберігається в національній пам'яті носіїв мови у вигляді пізнаного субстрату. Концепт. вербалізується, позначається словом, інакше його існування неможливе» [6, с. 21].

З.Д.Попова і І.А. Стернін визначають концепт як «дискретне ментальне утворення, що є базовою одиницею розумового коду людини, що володіє впорядкованою внутрішньою структурою та є результатом пізнавальної (когнітивної) діяльності особистості і суспільства і несе комплексну, енциклопедичну інформацію про те, що відображає предмет або явище, про інтерпретацію даної інформації суспільною свідомістю і відношення суспільної свідомості, до даного явища або предмету» [53, с. 7].

У сучасній лінгвістиці термін «концепт» використовується як позначення однією з форм репрезентації знань про світ з позицій когнітивної семантики.

Однак, як відзначають З.Д. Попова і І.А. Стернін у лінгвістичній науці зіткнулися різні інтерпретації терміна [53, с. 8].

Так, наприклад, визначення концепту, близьке розумінню, запропоноване М. В. Піменовою: «Концепт — це якесь уявлення про фрагмент світу чи частину такого фрагмента, що має складну структуру, виражену різними групами ознак, що реалізуються різноманітними мовними способами і засобами. Концептуальна ознака об’єктивується у закріпленій і вільній формах поєднань відповідних мовних одиниць - репрезентантів концепту. Концепт відображає категоріальні і ціннісні характеристики знань щодо деяких фрагментів світу. У структурі концепту відображаються ознаки, функціонально значущі для відповідної культури. Повний опис того чи іншого концепту, значущого для певної культури, можливий тільки при дослідженні найбільш повного набору засобів його вираження» [52, с. 10].

Концепт кодується у свідомості індивідуальним чуттєвим чином, що є чуттєвим компонентом змісту концепту, і є базовою одиницею універсального предметного коду людини [19, с. 158].

За визначенням В. І. Карасика [34, с. 79], «динаміка сенсу в інтервалі між вихідним і динамічним змістом концепту проявляється як еволюція та інволюція концепту, тобто смислове розширення і стиснення». Іншими словами, разом з розширенням (лат. evolution – розгортання) лінгвісти говорять і про «згортання» – інволюції, коли поняття втрачає частину своїх когнітивних ознак у процесі історичної зміни. У філософському трактуванні це відповідає уявленню про ускладнення або спрощення системи в ході еволюції, коли результатом самоорганізації нерівнозначних систем є їх прогресивна або регресивна зміна.

Еволюція / інволюція концепту проявляється у зміні його різних параметрів: номінативній щільності, оцінному знаку, образній характеристиці тощо, причому вона дещо відрізняється за своїми параметрами і напрямами для концептів різних типів.

Лексично представлені концепти прийнято розділяти на когнітивні і лінгвокультурні.

Перший тип – замісне поняття, це «натяк на можливе значення» і «відгук на попередній мовний досвід людини» [57, с. 182], він заснований на значенні слова, але враховує особистий і загальнонародний досвід (наприклад, КРИЗА, БУДИНОК тощо). Другий – лінгвокультурний концепт – є концентратом культури, це «згусток культури у свідомості людини» [60, с.40]; це багатовимірне смислове утворення, у якому виділяються ціннісна, образна і понятійна складові [57, с. 58] (наприклад, концепти етики і релігії типу БОГ, ДОБРО, ГРІХ, СКРОМНІСТЬ та ін). В їх аналізі використовують як загальні, так і різні параметри: когнітивний концепт, як правило, структурують у вигляді концептуальної мережі значення [45, с.26] або матриці доменів [48, с.11], а в лінгвокультурному концепті описують його понятійний, образний, ціннісний компоненти [36, с. 59].

Для концептів всіх типів виявляють їх когнітивні метафори і способи номінації метонімічної номінації.

Таким чином, можна з достатньою певністю сказати, що когнітивна лінгвістика з'ясовує, як пов'язані концепти з експлікуючими їх мовними

факторами. Відповідь на це питання надає інформацію про функціонування когнітивної системи.

Тож, у сучасній лінгвістиці немає єдності у розумінні концепту. На наш погляд, найбільш вдале визначення (що синтезує характер) дала М. В. Піменова: «Концепт — це якесь уявлення про фрагмент світу чи частину такого фрагмента, що має складну структуру, виражену різними групами ознак, що реалізуються різноманітними мовними способами і засобами» [50, с. 15].

Кожен концепт має певну структуру, яка є необхідною умовою існування концепту і його входження в концептосферу. Структура концепту має складну будову. З одного боку, до неї відноситься все, що належить до побудови поняття, з іншого боку, в структуру концепту входить те, що робить його фактом культури – вихідною формою (етимологія); стиснута до основних ознак змісту історія; сучасні асоціації; оцінки, конотації [35, с. 47]. У складній багатоплановій структурі концепту можна виділити як конкретне, так і абстрактне, як раціональне, так і емоційне, як універсальне, так й етнічне, як загальнонаціональне, так і індивідуально-особистісне. Цим і пояснюється відсутність єдиного визначення. Структуру концепту визначають як складну ментальну репрезентацію, утворену кількома каузально пов’язаними простими репрезентаціями, які, у свою чергу, формуються в результаті первинної взаємодії людини та середовища, яке її оточує [35, с. 50], тобто концепт народжується як образ, але, просуваючись щаблями абстракції, поступово перетворюється з чуттєвого образу у власне розумовий. Такий принцип формування ментальної репрезентації знань про світ дозволяє розглядати концепт як «поглинаючу польову структуру» [35, с.62], до якої входять різні аспекти знання і досвіду, у тому числі світоглядний, раціональний, емотивний, культурологічний.

На думку Г.Г.Слишкіна можна говорити про наявність трьох структурних типів концепту: однорівневих, багаторівневих та сегментних, де однорівневий концепт включає в себе тільки ядро, тобто чуттєвий образ. Таку структуру можуть мати концепти у свідомості дитини, а також концепти у свідомості інтелектуально нерозвиненій особистості. Багаторівневий концепт включає в

себе кілька когнітивних шарів, що розрізняються за рівнем абстракції, що відбивається ними. Сегментний концепт являє собою базовий чуттєвий шар, оточений кількома сегментами, «рівноправними за ступенем абстракції» [59, с.35].

Концепт втілюється у мові за допомогою різних можливостей цієї мови. Репрезентація знань у мовній формі є безліччю мовних засобів за допомогою яких передається думка. Таким чином, художні концепти моделюються та інтерпретуються з опорою на мовну репрезентацію [54, с.38].

Існує багато способів мовний апеляції до концепту. До одного і того ж концепту можна апелювати за допомогою одиниць різних рівнів: морфем, словоформ, лексем, фразеологізмів, вільних словосполучень. Структурні і позиційні схеми речень також є засобом репрезентації концептів у мові. «Вхід» в концепт може здійснюватися за допомогою пара лінгвістичних засобів [46, с.5].

Концепт вибірково втілюється у певних мовних одиницях, а також когнітивних моделях протягом тривалого періоду розвитку мови. Вивчення засобів і способів вербалізації концепту передбачає аналіз семантичної структури слів, що репрезентують концепт. Через аналіз способів репрезентації концепту виявляється певний елемент художньої картини світу письменника на матеріалі однієї з ділянок авторської картини світу, відображеної у змісті і структурі художніх творів. Таким чином, аналіз цих смислових одиниць важливий для визначення особливостей створеної автором картини світу, яка поглиблює інтерпретацію його творів і виявляє істотні особливості індивідуального стилю автора [37, с.10].

Концепт репрезентується у мові готовими лексемами і фразеосполученнями зі складу лексико-фразеологічної системи мови; вільними словосполученнями; структурними і позиційними схемами речень, що несуть типові речення (синтаксичні концепти); текстами і сукупностями текстів (при необхідності експлікації чи обговорення змісту складних, абстрактних чи індивідуально-авторських концептів) [21, с.125].

Культурний концепт у мовній свідомості поданий як багатовимірна мережа значень, яка виражається лексичними, фразеологічними, пареміологічними одиницями, прецедентними текстами, етикетними формулами, а також мовними поведінковими тактиками, що віображають повторювані фрагменти соціального життя [21, с.126].

Наявність мовного вираження концепту, його регулярна вербалізація підтримують концепт у стабільному, стійкому стані, роблять його загальновідомим (оскільки значення слів якими він передається, загальновідомі, вони тлумачаться носіями мови, відображаються у словниках). Науковці [2; 18; 24; 25; 28; 35; 39;41; 43; 44; 47; 61; 66; 71; 78] пропонують наступну модель концепту: ядром концепту є чуттєвий базовий образ, що виступає як кодуючий образ універсального предметного коду. Цей образ належить буттєвому шару свідомості і, як показують деякі спостереження, має операційний або предметний характер, базуючись на біодинамічній і чуттєвій тканині свідомості. Базовий образ оточений конкретно-чуттєвим за своїм походженням когнітивним шаром, що відбиває чуттєво — сприймані властивості ознак предмета [63, с.14].

Вербалізація у широкому сенсі означає вербальний (словесний) опис переживань, почуттів, думок, поведінки. Тож, вербалізація — це процес вираження через звукове позначення символів опису світу.

Одним з основних способів вербалізації концепту більшість вчених визнають фразеологізми.

Так, Н.Ф. Алефіренко у якості найбільш поширених засобів вербалізації концепту зазначає слово фразеологізм, словосполучення, структурну схему речення і, навіть, текст, якщо в ньому розкривається сутність якого-небудь концепту» [2, с. 42].

Таким чином, концепт — це, з одного боку, вихідний пункт породження значення мовного знака, а з іншого — завершальний етап смислового насичення слова. У мові концепт, по-перше, вербалізується, оскільки отримує своє ім'я, а по-друге, репрезентується різнорівневими засобами мови.

2.2 Функціонування концепту «CYBERSECURITY» у текстах резолюційного жанру

У сучасному інтерактивному суспільному житті все частіше мають місце такі негативні наслідки інформатизації, як: кібератаки, кібервійна, кіберексплуатація, кіберпогрози, кіберконфлікт, кіберпіратство, кіберкрадій, кібертерроризм, кіберзлочин, кіберзнущання, кіберсаботаж,; а також відповідне протистояння з боку правового сектору – кіберворог, кіберкриміналістика, кіберзахист, кіберполіція, кіберправо тощо. У нормативних документах вони представлені такими лексикалізованими концептами, як: *CYBERATTACK, CYBERWAR, CYBERESPIONAGE, CYBER-AGREEMENT, CYBER-THEFT, CYBERPIRACY, CYBERTHIEF, CYBERLAW, CYBERCRIME, CYBER-SABOTAGE, CYBERBULLYING, CYBERSECURITY, CYBERACTIVITY, CYBERDETERRENCE, CYBEREXPLOITATION, CYBERCONFLICT, CYBEROFFENCE, CYBERENEMY, CYBERTERRORISM, CYBERPOLICE, CYBERCRIMINALISTICS*. Сьогодні у світі велика увага приділяється закріпленню концепту «CYBERSECURITY» на нормативно-правовому рівні. На особливий інтерес заслуговує Резолюція Генеральної Асамблеї ООН A/RES/57/239 від 20 грудня 2002 року “Створення глобальної культури кібербезпеки” (Creation of a global culture of cybersecurity) [85], в якій вперше чітко використовувалося поняття кібербезпека. У згаданій Резолюції конценцепт «CYBERSECURITY» було використано 17 разів, зокрема у преамбулі автори вжили його шість разів: (37) «*The General Assembly, Noting the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information, Recognizing that the need for cybersecurity increases as countries increase their participation in the information society, Noting also the work of relevant international and regional organizations on enhancing cybersecurity and the security of information technologies*;

1. *Takes note of the elements annexed to the present resolution, with a view to creating a global culture of cybersecurity;*

2. *Invites all relevant international organizations to consider, inter alia, these elements for the creation of such a culture in any future work on cybersecurity;*

3. *Invites Member States to take into account these elements, inter alia, in their efforts to develop throughout their societies a culture of cybersecurity in the application and use of information technologies;*

4. *Invites Member States and all relevant international organizations to take, inter alia, these elements and the need for a global culture of cybersecurity into account in their preparations for the World Summit on the Information Society, to be held at Geneva from 10 to 12 December 2003 and at Tunis in 2005; 5. Stresses the necessity to facilitate the transfer of information technology and capacity-building to developing countries, in order to help them to take measures in cybersecurity»* [85]. — *«Генеральна Асамблея, відзначаючи зростаючу залежність урядів, підприємств, інших організацій та окремих користувачів від інформаційних технологій для надання основних товарів та послуг, ведення бізнесу та обміну інформацією, визнаючи необхідність кібербезпеки зростає у міру збільшення участі країн в інформаційному суспільстві, відзначаючи також роботу відповідних міжнародних та регіональних організацій щодо підвищення кібербезпеки та безпеки інформаційних технологій;*

1. бере до уваги елементи, додані до цієї резолюції, з метою створення глобальної культури кібербезпеки;

2. Запрошує усі відповідні міжнародні організації, зокрема, розглянути ці елементи для створення такої культури в будь-якій майбутній роботі з кібербезпеки;

3. Запрошує держави-члени взяти до уваги ці елементи, зокрема, у своїх зусиллях розвивати в своїх суспільствах культуру кібербезпеки при застосуванні та використанні інформаційних технологій;

4. Запрошує держави-члени та всі відповідні міжнародні організації, зокрема, врахувати ці елементи та необхідність глобальної культури

кібербезпеки під час підготовки до Всесвітнього саміту з питань інформаційного суспільства, який відбудеться в Женеві з 10 до 12 Грудень 2003 р. І в Тунісі 2005 р .; 5. наголошує на необхідності сприяти передачі інформаційних технологій та розбудові потенціалу країнам, що розвиваються, щоб допомогти їм вжити заходів щодо кібербезпеки»[85].

Активно до теми кібербезпеки звертається Міжнародний союз електрозв'язкум (МСЕ), International Telecommunication Union (ITU), який ухвалив низку резолюцій і рекомендацій, які безпосередньо торкаються проблеми забезпечення безпекиу кіберпросторі. На особливу увагу заслуговує Рекомендація МСЕ-Т59 Х.1205 від 2008 року, яка надає визначення кібербезпеки, представляє у систематизованій формі загрози кібербезпеці та уразливості (включно з переліком найпоширеніших інструментів хакерських атак). У зазначеному документі наведене таке трактування дефініції «кібербезпека»: (38) «*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets* [88]. — *«Кібербезпека — це сукупність інструментів, політик, концепцій безпеки, гарантій безпеки, керівних принципів, підходів до управління ризиками, дій, тренінгів, найкращих практик, гарантій та технологій, які можуть бути використані для захисту кіберсередовища та організації та активів користувача* [88].

Також у Резолюції вербалізуються інші складові концептосфери «CYBERSECURITY», а саме: cyber environment, computing devices, personnel, infrastructure, applications, services, telecommunications systems, the totality of transmitted and/or stored information та ін. Продемонструємо лексикалізацію понять досліджуваної концептосфери прикладом із Рекомендації ITU -T59: (39) *«Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization*

and user's assets against relevant security risks in the cyber environment» [88]. — *«До активів організації та користувачів належать підключені обчислювальні пристрої, персонал, інфраструктура, додатки, послуги, телекомунікаційні системи та сукупність переданої та / або збереженої інформації в кіберсередовищі. Кібербезпека прагне забезпечити досягнення та підтримку властивостей безпеки організації та активів користувача проти відповідних ризиків безпеки в кіберсередовищі*»[88].

У 2009 р. Міжнародний союз електрозв'язку опублікував звіт «Розуміння кіберзлочинності. Керівництво для країн, що розвиваються» (Understanding Cybercraime: A Guaide for Developing Counries) [91], метою якого є сприяння країнам, що розвиваються в розумінні законодавчих аспектів кібербезпеки і допомога в гармонізації законодавчих основ.

У керівництві подано дуже детальний огляд багатьох важливих тем, пов'язаних з законодавчим регулюванням кіберзлочинності в глобальному світі. В ньому описані проблеми, включаючи міжнародну взаємодію і процедури обміну інформацією. Наведено стратегії боротьби з кіберзлочинцями, проаналізовано міжнародне законодавство, питання процесуального характеру і т.д.: *The term "cybercrime" is used to cover a wide variety of criminal conduct. As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime. One approach can be found in the Convention on Cybercrime, which distinguishes between four different types of offences*:

1. *offences against the confidentiality, integrity and availability of computer data and systems;*

2. *computer-related offences;*

3. *content-related offences;*

4. copyright-related offences» [91].

Досить поширеним різновидом кібернетичних злочинів стає *identity theft – «викрадення особистості».* Шахраям достатньо знати прізвище і номер картки соціального страхування особи, щоб, вдаючись до маніпуляцій з використанням

Інтернет, одержувати від імені цієї людини кредити, замовляти товари і послуги. Із крадіжками особистих даних пов'язано створення неологізмів identity theft, ID crook для позначення «комп'ютерних» шахраїв, а нове словосполучення identity theft industry підкреслює існування цілої індустрії комп'ютерного шахрайства. У звіті ITU «Understanding Cybercraime: *A Guaide for Developing Counries» термін identity theft трактується як «the fraudulent practice of using another person's name and personal information in order to obtain credit, loans,* etc.» [91].

Наприкінці XX ст. у лінгвістиці з'являється поняття *cyberterrorism – «кібертероризм»*. Це поняття у новому столітті було розширено, і тим самим було розширене значення лексеми cyberterrorism: спочатку воно позначало використання комп'ютерної техніки для терористичних актів, а сучасне тлумачення визначає його як навмисну, політично мотивовану атаку на інформаційні, комп'ютерні системи, програми і бази даних з метою їх руйнування або нанесення збитку мирним об'єктам і мешканцям. Практично повним синонімом слова cyberterrorism виступає і неологізм cyber-sabotage [10, с. 59]. Номінація *cyberterrorism* сьогодні є досить частотною у резолютивних документах. Так, у воно вжито більше 50 разів: «*In addition, some terms that are used to describe criminal acts (such as "cyberterrorism" or "phishing") cover acts that fall within several categories. Nonetheless, the four categories can serve as a useful basis for discussing the phenomena of cybercrime*» [91].

З кібертероризмом пов'язана і ціла низка інших понять і відповідних новотворів. Це такі поняття, як *cyberattack, cyberspace attack – кібератака, кібернапад, cyberdefence – кіберзахист, cybersecrecy – кіберсекретність, cybervulnerability – кібервразливість, cyberweapon – кіберзброя, cyberwarfare, Internet warfare, digital warfare – кібервійна (цифрова, інтернетівська війна).*

"Organizational structures" focuses on the prevention, detection, response to and crisis management of cyberattacks, including the protection of critical information infrastructure systems» [91].

«Cyberspace attack – cyberspace actions that create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains» [85].

Застосування методів і засобів «кібертероризму», вважають аналітики, може призвести до того, що терористи будуть мати доступ до систем контролю за енергетикою, міськими комунікаціями, атомними електростанціями, повітряним транспортом. Тому, з метою створення системи «кібербезпеки» проти кібертероризму у США було сформовано і окремий департамент, який очолює «цар кібербезнеки» *cybersecurity czar.*

Розглядаючи лексику і фразеологію, що входять до лексико-семантичного поля концепту «CYBERSECURITY», можна помітити певні специфічні лінгвальні явища. До них відносимо явище атракції синонімів навколо концепту «CYBERSECURITY», а також концентрація неологізмів навколо ключових центрів парадигм. До понять, навколо яких концентруються синоніми, слід віднести такі: *cyberaddict, chip-head, cyberhead, computer junkie, cyberjunkie, cyberbuff, datajunkie, digit-head, gearhead, nethead, technofreak, technophile, tekky, telephile («великий аматор комп'ютерної техніки»); computer nerd, cyberguru, cybernerd, geek, supernerd, techguru, technogeek, technoguru, techopundit, technonerd, technosavant, ubernerd («фахівець в галузі сучасної техніки»); computer hip, computerate, computent, com-puter-savvy, cybersavvy, it-savvy, technoliterate, techsavvy («такий, що добре знає комп'ютерну техніку»); cyber-citizen, cybersurfer, e-surfer, netter, internant, nethead, netizen, netsurfer («людина, яка активно користується мережею Інтернет»); lamer, end user, luser, novice, readonly twink, user, munchkin, weasel («недосвідчений користувач»); neoludite, Internot, leadite, shiftless («особа, відчужена від домену технічної сфери*»).

Однак такі синоніми переважно вживаються у розмовному чи художньому стилях. У нормативних документах вони мають відповідники, які традиційно вживаються у правовому дискурсі: *wizard, IT specialist, specialist in information technology, expert, computer supernerd.* Продемонструємо сказане прикладом з

«*Some experts suggest the only real solution in the fight against spam is to raise transmission costs for senders*» [91].

Наведемо інший приклад: «*One important requirement of an efficient education and information strategy is open communication of the latest cybercrime threats. Some states and/or private businesses refuse to emphasize that citizens and clients respectively are affected by cybercrime threats, in order to avoid them losing trust in online communication services. The United States Federal Bureau of Investigation has explicitly asked companies to overcome their aversion to negative publicity and report cybercrime. In order to determine threat levels, as well as to inform users, it is vital to improve the collection and publication of relevant information»* [91].

Як бачимо, у концептосфері «CYBERSECURITY» функціонує багато лексем на позначення суб'єктів кібербезпеки, які відзначаються багатою синонімією. Довший синонімічний ряд охоплює лексичні одиниці для позначення понять «торгівля» і «гроші»: *cybercommerce, cybertrade, cybershopping, ecommerce, d-commerce, electronic commerce, electronic shopping, e-shopping, Internet shopping, t-commerce, m-commerce, telesales, v-commerce («електронна торгівля»); beenz, cybercash, cybercurrency, cybermoney, e-cash, digital cash, egold, idollars,e-money, online bucks, flooz, virtual money («віртуальні гроші» для розрахунків через Інтернет*»).

Зокрема, Committee on National Security Systems наводить наступне визначення: «*Intellectual property – creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract "properties" has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered»* [85].

Наведені приклади свідчать, що динамічний розвиток інформаційних технологій активізує феномен «поліномінації», тобто коли одне поняття, одна річ набувають низку номінацій. У той же час, як можна прослідкувати із деяких

мовних одиниць, виникає особливий тип неологізмів – «ретроніми», під якими маються на увазі нові позначення вже відомих понять і предметів у зв'язку з уточненням даних понять, із появою нових різновидів існуючих предметів і необхідністю тим самим більш чіткого розмежування старого і нового поняття або предмета. Як приклади синонімії серед метафоричних номінантів англійської комп'ютерної лексики можна назвати й такі, як *bitty box – примітивний комп'ютер, big iron – застарілий великий комп'ютер, dinosaur – застарілий, великий комп'ютер, retroware – застаріла техніка, tired iron – застарілий пристрій, toaster-toy – застарілий маленький комп'ютер, steampowered iron – старий, але надійний пристрій.*

Наступним знаковим документом, опублікований останніми роками, є міжнародний стандарт ISO / IEC 27032 до: 2012 «Information technology. Security techniques. Guidelines for cybersecurity» (Інформаційні технології. Методи забезпечення безпеки. Настанови щодо кібербезпеки). Стандарт дає чітке розуміння зв'язку терміна cybersecurity (кібербезпека) з мережевою безпекою, прикладною безпекою, Інтернет-безпекою та безпекою критичних інформаційних інфраструктур з позиції західноєвропейських науковців. Документом визначається, що кібербезпека і інформаційна безпека не є взаємозамінними поняттями. Зокрема у документі зазначено: «*Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: - information security, - network security, - internet security, and - critical information infrastructure protection* (CIIP)» [87].

У зазначеному стандарті має місце група номінації наслідків створення кібернетичної загрози, зокрема лексема «CYBERCRIME». Документ наводить визначення поняття cybercrime: «*criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime»* [87]. У наведеному прикладі вербалізовано інший концепт із досліджуваної концептосфери *cyberspace.* Резолюційний характер носять окремі документи Комітету з питань національної безпеки (Committee on National Security Systems (CNSS)), який є міжурядовою

організацією США, що встановлює політику щодо функціонування систем безпеки США. Зокрема у CNSSI 4009 подається словник термінів, які відносяться до концептосфери “Cybersecurity“. Зокрема у документі автори трактують кібербезпеку як *«prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation»* [87]. У наведеній дефініції вжиті лексеми, семантика яких пов’язана з кібернетичною безпекою. Також процеси управління ризиками кібербезпеки описані в наступних документах: ISO 31000: 2009; ISO / IEC 27005: 2008; NIST Special Publication 800-39; Electricity Sector Cybersecurity Risk Management Process (RMP) Guideline Octave тощо.

Висновки до розділу 2

У розділі визначено, що у сучасному інтерактивному суспільному житті все частіше мають місце такі негативні наслідки інформатизації, як: кібератаки, кібервійна, кіберексплуатація, кіберпогрози, кіберконфлікт, кіберпіратство, кіберкрадій, кібертерроризм, кіберзлочин, кіберзнущання, кіберсаботаж,; а також відповідне протистояння з боку правового сектору – кіберворог, кіберкриміналістика, кіберзахист, кіберполіція, кіберправо тощо. У нормативних документах вони представлені концептом «CYBERSECURITY».

Визначено, що концепт — це якесь уявлення про фрагмент світу чи частину такого фрагмента, що має складну структуру, виражену різними групами ознак, що реалізуються різноманітними мовними способами і засобами. Культурний концепт у мовній свідомості поданий як багатовимірна мережа значень, яка виражається лексичними, фразеологічними, пареміологічними одиницями, прецедентними текстами, етикетними формулами, а також мовними поведінковими тактиками, що віображають повторювані фрагменти соціального життя.

З’ясовано, що концепт — це, з одного боку, вихідний пункт породження значення мовного знака, а з іншого — завершальний етап смислового насичення слова. У мові концепт, по-перше, вербалізується, оскільки отримує своє ім'я, а по-друге, репрезентується різнорівневими засобами мови.

Наявність мовного вираження концепту, його регулярна вербалізація підтримують концепт у стабільному, стійкому стані, роблять його загальновідомим (оскільки значення слів якими він передається, загальновідомі, вони тлумачаться носіями мови, відображаються у словниках).

Визначено наступні особливості нормативно-правового тексту. По-перше: він володіє диференціацією значущості текстів, висловлювань; по-

друге, сумісний з іншими видами текстів; по-третє, завжди має в якості об'єкта уваги правовідносини; по-четверте, нормативно-правовий текст знаходить своє вираження у мові, нормативно-правових текстах, комунікативних актах, більш того сама правосвідомість - текст; по-п'яте, атомом нормативно-правового тексту є висловлювання, при цьому висловлювання не тотожне акту висловлювання, реченню, судженню, синтагмі.

Нормативно-правовий текст характеризується особливостями дискурсивної практики, яка в рамках нормативно-правового акта відрізняється догматичністю, монологічністю (при цьому в ній присутня логіка «відповіді»), специфічною (кодифікованою) лексикою, предикативною оповідною структурою, заснованою на критерії правдивості.

РОЗДІЛ 3
СПОСОБИ ВЕРБАЛІЗАЦІЇ КОНЦЕПТУ «CYBERSECURITY» У СУЧАСНИХ АНГЛОМОВНИХ ТЕКСТАХ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ ТА ОСОБЛИВОСТІ ЇХ ПЕРЕКЛАДУ УКРАЇНСЬКО МОВОЮ

3.1 Засоби вербалізації концепту

Спробуємо встановити межі концептосфери “Cybersecurity“ в англійській мові і виділити категоріальні компоненти, складові обсягу досліджуваної концептосфери. Сьогодні концепт “Cybersecurity“ знаходить своє відображення у різних видах текстів (художніх, наукових, офіційно-ділових, публіцистичних) а також усному мовленні, що є відкриті у доступі для будь-якої аудиторії як експліцитне відображення поточного сприйняття концептосфери суспільством, з одного боку, та імпліцитний вплив на формування даної концептосфери, з іншого боку. Ключовими лексемами, що лежать в основі вербалізації аналізованої концептосфери в англійській мові, з'явилися «CYBERSAFETY» / «CYBERSECURITY» (кіберзахист, кібербезпека) в комбінаториці. Відповідно до словникових даних можна говорити про її базові компоненти. Визначимо обсяг концептосфери «CYBERSAFETY» / «CYBERSECURITY». У словнику is a property of cyberspace that is an ability to resist intentional and/or unintentional threats and respond and recover.

В англійській мові загальна семантика наведених одиниць, що об'єктивують досліджувану концептосферу в англійській мові, виявляє три загальні типові значення, згідно з аналізом словників: 1) safety, freedom from attack, harm, or damage, a state in which or a place where you are safe and not in danger or at risk (безпека, відсутність загрози нападу, шкоди, стан або місце, в якому немає загрози, небезпеки, або ризику); 2) protection of a person, building, organization or country against threats (захист людини, будівлі, організації або країни від різних видів загроз); 3) things done to keep people,

places, or things safe (заходи для забезпечення безпеки людей, місць, речей) [4; 7; 11; 16; 22; 31].

Таким чином, словникові дані формують ядро концептосфери «CYBERSAFETY» / «CYBERSECURITY» (кібербезпека) на ключовому параметрі концепту threat (загроза), опиняється в положенні дихотомії cyber threat presence — cyber threat absence («наявність кіберзагрози - відсутність кіберзагрози»), що тягне за собою неминучий розподіл розглянутої концептосфери на два взаємоспрямовані напрямки, що реалізуються шляхом взаємодії: threat presence (виникнення загрози) і cyber threat absence (відсутність загрози) як одночасно впливаючі на ментальне явище, що лежить в основі даної концептосфери. Структурно дана дихотомія організовується більш дрібно, об'єднуючи різні аспекти і способи забезпечення її провідних значень. Серед таких виявляються номінації безпосередньо дій, маркованих ситуації виникнення загрози інформаційній безпеці або її відсутності, комплекс заходів, який обслуговує зазначені дії, а також джерела забезпечення ситуативного прецеденту в основі кожного з контекстів. Концепт cyber threat (кіберзагроза) являє собою комплекс різноманітних репрезентують його одиниць із загальним значенням створення або виникнення загрози. Концепт реалізується в двох складових його фреймах: cyber threat presence (наявність кіберзагрози) і cyber threat absence (відсутність кіберзагрози).

Матеріал, який вербалізує концепт, утворює кілька семантичних груп - слотів кожного фрейму. Фрейм cyber threat presence (наявність кіберзагрози) структурно організується в наступні групи-слоти: Threatening activity (дії зі створення загроз) - номінація безпосередньо дії створення загрози з точки зору реалізації її основного значення «виникнення небезпеки, порушення стабільності»; Threat sources (джерела загроз) — номінація джерела виникнення загрози, Threat consequences (наслідки загроз) — номінація її наслідків; Threatening means (засоби створення загроз) — вербалізація засобів, які сприяють виникненню загрози.

Провідною семантичною групою в даному фреймі виявляються одиниці і словосполучення, які вербалізують загрозу як акт порушення стабільності інформаційної системи, а саме cybersecurity threats / threatening activity of cybersecurity (дії зі створення кіберзагроз): information interventions (інформаційна інтервенція), cybercrimes (кіберзлочини), cyberterrorism (кібертероризм), cyberattacks (кібератаки), cyber espionage (кібершпигунство), breaking personal data (злам персональних даних), criminal negligence in the cybersphere (злочинна недбалість у кіберсфері), cyberpanic (паніка), causing or risking a cybercrash / cybercatastrophe (провокувати кіберкатастрофу), committed a range of other offenses (здійснити ряд інших злочинів), cyberwarfare (кібервійни), Internet warfare (Інтернет-війни), digital warfare цифрові війни). Також суміжною є група sources of cyber threats / cyber threat sources (джерела кіберзагроз) — група одиниць, що номінують джерело загрози: cyber terrorist groups (кібертерористичні угруповання), hacker (хакер), cyber jihadists (кібер-джихадисти), cybercroocs (кіберплути). Серед лексичної репрезентації джерела кібернетичної загрози виділяються безпосередньо суб'єкти, що створюють кіберзагрозу, організовані об'єднання і організації, неживі суб'єкти природної і техногенної приналежності. До цієї групи примикає і частково з нею перетинається група cyber threatening means (засоби створення кіберзагроз) — група одиниць, номінують засоби створення загрози: cyberweapon (кіберзброя), smart missiles («розумні ракети»), smart bombs («розумні бомби»), the maximum-security prison (в'язниці особливо суворого режиму). Тут варто відзначити частковий перетин одиниць концепту кіберсфери з одиницями інших груп. Так, в'язниці спочатку мають на меті усунення кіберзагрози, проте можуть виступати її джерелом (в контексті недостатності умов для утримання ув'язнених, а також внаслідок загрозливого характеру її компонента — «в'язнів»). Група cyber threat consequences (наслідки кіберзагроз) — група номінації наслідків створення кібернетичної загрози — виявляється досить широкою за своїм семантичним наповненням і включає в себе різноманітні групові організації лексичног матеріалу в сукупності з номінацією явищ в процесі прийняття заходів щодо

усунення та подальшого протидії кібезагрозі та інших, пов'язаних з цим обставин, перетинаючись з областю значень концепту cyber threat absence (відсутність кіберзагрози). В якості одиниць, які репрезентують цю групу, можна навести такі: prison education program (програма освіти в тюрмах), history of cybercrime and punishment (історія кіберзлочинів і покарань), catastrophic scales of personal data breaks and massive cracking of password data (катастрофічні масштаби зломів персональних даних і масові вскриття паролів). Протилежним кадру cyber threat presence (наявність кіберзагрози) в дихотомії концепту cyber threat (кіберзагроза) виявляє фрейм cyber threat absence / no cyber threats (відсутність кіберзагрози), який, в свою чергу, являє собою комбінацію двох взаємопов'язаних слотів: cyber threat prevention (запобігання кіберзагрозі) та cyber threat response / cyber threat elimination (усунення кіберзагрози). Обидва цих фрейми виявляють кореляцію в загальному значенні, хоча і покликані впливати на створену кібернетичну загрозу з різних сторін. Незважаючи на їх семантичні та екстралінгвістичні відмінності, дані фрейми виявляють аналогічну репрезентацію засобами мови. Лексичний матеріал, який реалізує зазначені фрейми, організовується відповідно до загальних структурних параметрів і включає кілька категоріальних груп в кожному з них. Так, першою з них можна назвати номінацію безпосередньо дії щодо запобігання або усуненню кіберзагрози. Серед одиниць групи Prevention activity, вербалізуется дії із запобігання кіберзагрозі, представлені наступні: counteracting account hacking (протистояння зламу акаунтів), to protect your personal data (захистити персональні дані), closing a loop hole in cybersecurity laws (закрити «дірку» в законодавстві у сфері кібербезпеки), implored the police to increase cybersecurity efforts (спонукати поліцію посилити заходи кібербезпеки), placing security cameras (розмістити камери стеження). Одиниці групи Response activity, що репрезентують дії щодо усунення кіберзагрози, включають такі, як: to prosecute (залучати до відповідальності), to review the investigation cybercrime (аналізувати розслідування кіберзлочинів), find evidence of interference with a person's privacy (знайти докази втручання в приватне життя особи), Homeland Security's decision

(рішення Департаменту внутрішньої безпеки), to remove Kaspersky software from government systems (відмовитися від програмного забезпечення Касперського на урядових 36 комп'ютерах), mission to root out cybercrime (місія з викорінення кіберзлочинів), fought over cybercrime (боротися з кіберзлочинністю) (7/350). Також в рамках цих концептів реалізуються групи Agencies and Agents (служби та службовці), що включають одиниці, номінується служби та службовців, відповідальних за запобігання або усунення загрози: jails and prisons (тюремні і судові органи), Cybecrime and Correction Committee (комітет із запобігання кіберзлочинів і пенітенціарна система), attorney general (генеральний прокурор). Близькою виявляється група Regulatory documents, яка об'єднує одиниці, що номінують регулятивні документи, що забезпечують механізми реалізації вищеописаних дій щодо усунення або запобігання кіберзагрози. Ця група включає широкий спектр репрезентативних одиниць: state regulations (державні постанови), statutes protecting cyberpolice secrecy (закони, що захищають конфіденційність діяльності кіберполіції), Controlling the Assault of Non-solicited Pornography and Marketing (Закон «Про боротьбу зі спамом»), Wire and Electronic Communications in Terception and Interception of Oral Communications (Закон «Про перехоплення електронних повідомлень та прослуховування переговорів»), Federal Information Security Management Act (Закон «Про інформаційну безпеку»). Суміжними є групи Prevention means cybercrime (засоби запобігання кіберзлочинам) і Response means cybecrime (засоби усунення кіберзлочинності), об'єктивує засоби протидії загрозі при її усуненні або запобіганні: *$ 500 million to provide "cybecsecurity assistance" (500 мільйонів доларів на забезпечення кібербезпеки), cells 'fences (решітки в камерах), cordon tape (загороджувальна стрічка).*

Таким чином, концептосфера «CYBERSECURITY» (Кібербезпека) в англійській мові будується на базовому концепті «CYBERTHREAT» (кіберзагроза), обсяг якого формується сукупністю взаємопроникаючих значень двох антагоністичних фреймів: фрейма cyber threat presence (наявність кіберзагрози) і сукупністю обсягу фрейма cyber threat absence (відсутність

кіберзагрози), що включає обов'язкову дихотомію cyber threat prevention (запобігання кіберзагрози) і cyber threat response (усунення кіберзагрози). Семантика концептосфери заснована на семантиці категоріальних компонентів, які номінують її групи, характерні для кожного фрейма зазначеного концепту. Такими структурними параметрами для фрейма «cyber threat presence» (наявність кіберзагрози) є групи, що репрезентують безпосередню дію створення кібернетичної загрози, джерело кіберзагрози, наслідки та засоби створення загрози у інформаційній сфері. Фрейм «cyber threat absence» (відсутність кіберзагрози) розглядається в нерозривній дихотомії його слотівсценаріїв «cyber threat prevention» (запобігання кіберзагрози) і «cyber threat response» (усунення кіберзагрози), виявляючи загальні цільові, але семантично різні групи лексики: групи, що номінують безпосередньо дії щодо запобігання або усунення кіберзагрози, групи, що номінують органи і служби, які реалізують зазначені дії, групи, які вербалізують документи та інші регулятивні інструменти, які вказують порядок дій щодо запобігання / усунення кіберзагрози, а також засоби для здійснення даних дій. Також слід зауважити, що виникнення більшості лексикалізованих концептів, що належать до кнцептосфери «CYBERSECURITY», актуалізуються розвитком інтерактивної мережі. У свою чергу це призводить до закріплення морфологізованого концепту «cyber» – у центральній (ядерній) ділянці мережі англомовних морфологізованих концептів. За нашими спостереженнями, він має досить стійкі позиції щодо продукування інноваційних лінгво-ментальних одиниць шляхом включення у процеси концептуальної деривації за метакогнітивною моделлю афіксальної деривації, утворюючи при цьому похідну операційну модель із константним елементом W + CYBER– [20, с. 160].

Таким чином, концептосфера «CYBERSECURITY» (кібербезпека) в англійській мові реалізується шляхом спільного двостороннього впливу на сутність провідного значення концептосфери - загрози кібернетичній безпеці, при цьому кожен з двох структурних елементів виявляється неодмінною умовою

існування концептосфери, релевантної для представника англійської мовної спільності.

3.1.1 Концептуальні зв'язки

Концепт «CYBERSECURITY» / «КІБЕРБЕЗПЕКА», який номінується в англійській мові як «SAFETY» / «SECURITY», є одним із ключових концептів, що вербалізує одну з необхідних умов життя в соціумі - явище безпеки. Наразі явище безпеки в сучасному світі отримало широке висвітлення в наукових лінгвістичних та інших суміжних галузях, що дозволяє говорити про широку репрезентацію даного концепту мовними засобами у лінгвокультурологічній свідомості людини. Внаслідок різноманітності когнітивних установок, залучених у формування ментального образу концепту «SAFETY» / «SECURITY» (БЕЗПЕКА), можна стверджувати, що останній є компонентом структури концептосфери «SAFETY» / «SECURITY» (БЕЗПЕКА).

Матеріалом дослідження послужили тексти документів міжнародних організацій, що знаходяться у відкритому доступі для будь-якої аудиторії як експліцитне відображення поточного сприйняття концептосфери суспільством, з одного боку, і імпліцитний вплив на формування даної концептосфери, з іншого боку. Ключовими лексемами, що лежать в основі вербалізації аналізованої концептосфери в англійській мові, є safety / security (захист, безпека) у комбінаториці. Відповідно словниковим даним можна говорити про їх базові компоненти.

Визначимо обсяг концептосфери «SAFETY» / «SECURITY» (БЕЗПЕКА). В англійській мові загальна семантика наведених одиниць, що об'єктивують досліджувану концептосферу в англійській мові, виявляє три загальних типових значення, згідно з аналізом словників [81; 82: 1) *safety, freedom from attack, harm, or damage, a state in which or a place where you are safe and not in danger or at risk* (безпека, відсутність загрози нападу, шкоди, стан або місце, в якому немає загрози, небезпеки, або ризику); 2) *protection of a person, building, organization or*

country against threats (захист людини, будівлі, організації або країни від різних видів загроз); 3) *things done to keep people, places, or things safe* [74] (заходи щодо безпеки людей, місць, речей).

Таким чином, словникові дані формують ядро концептосфери «SAFETY» / «SECURITY» (БЕЗПЕКА) на ключовому параметрі концепту THREAT (ЗАГРОЗА), опиняється в положенні дихотомії *threat presence - threat absence («наявність загрози - відсутність загрози»),* що тягне за собою неминучий розподіл розглянутої концептосфери на два взаємоспрямованих напрямки, що реалізуються шляхом взаємодії: «THREAT PRESENCE» (ВИНИКНЕННЯ ЗАГРОЗИ) і «THREAT ABSENCE» (ВІДСУТНІСТЬ ЗАГРОЗИ) які одночасно впливають на ментальне явище, що лежить в основі даної концептосфери. Структурно дана дихотомія організовується більш дрібно, об'єднуючи різні аспекти і способи забезпечення її провідних значень. Серед таких виявляються номінації безпосередньо дій, що маркують ситуації виникнення загрози або її відсутності, комплекс заходів, який обслуговує зазначені дії, а також джерела забезпечення ситуативного прецеденту в основі кожного з контекстів.

Представлена нижче схема наочно представляє структурну організацію концептосфери «SAFETY» / «SECURITY» (БЕЗПЕКА) через концепт «THREAT» (ЗАГРОЗА), що реалізується у вигляді фреймів типових об'єктів і сценаріїв, які формують обсяг розглянутого концепту.

Концепт «THREAT» (ЗАГРОЗА) являє собою комплекс різноманітних репрезентуючих його одиниць із загальним значенням створення або виникнення загрози. Концепт реалізується в двох складових його фреймах: «THREAT PRESENCE» (НАЯВНІСТЬ ЗАГРОЗИ) і «THREAT ABSENCE» (ВІДСУТНІСТЬ ЗАГРОЗИ). Матеріал, що вербалізує концепт, утворює кілька семантичних груп — слотів кожного фрейму.

Фрейм «THREAT PRESENCE» (НАЯВНІСТЬ ЗАГРОЗИ) структурно організується в наступні групи-слоти: Threatening activity (дії зі створення загроз) — номінація безпосередньо дії створення загрози з точки зору реалізації її основного значення «виникнення небезпеки, порушення стабільності»; Threat

sources (джерела загроз) — номінація джерела виникнення загрози, Threat consequences (наслідки загроз) — номінація її наслідків; Threatening means (засоби створення загроз) — вербалізація засобів, що сприяють виникненню загрози.

Провідною семантичною групою у даному фреймі виявляються одиниці і словосполучення, що вербалізують загрозу як акт порушення стабільності системи, а саме Threatening activity (дії зі створення загроз): murder (вбивство), abuse of early inmates (насильство над первинними ув'язненими), drug crimes (злочини, пов'язані з наркотиками), the threat of Russian interference (загроза російського втручання, attacks (теракт 11 вересня), criminal negligence (злочинна недбалість), suicide bombing (вибух за участю смертника), the poor hygiene (низький рівень гігієни), panic (паніка), beating her in the stomach with a board (вдарити в живіт дошкою), causing or risking a catastrophe (провокувати катастрофу), plant a device (bomb) (встановити бомбу), fleeing from prison (втекти з в'язниці), kidnapping a lawyer (викрасти юриста), committed a range of other offenses [73] (здійснити ряд інших злочинів) тощо.

/ «SAFETY» / «SECURITY» \ / (БЕЗПЕКА) \ «THREAT» (ЗАГРОЗА}

Також суміжною є група «THREAT SOURCES» (джерела загроз) — група одиниць, що номінують джерело загрози: terrorist groups (терористичні угруповання), Guantânamo detainee (укладений Гуантанамо), suspicious-looking people (підозрілі люди), Hurricane Katrina (ураган Катріна), Russian military and intelligence (військові і розвідувальні сили Росії), Pokémon Go (гра «Покемон»), a stray bullet [Ibidem] (випадкова куля) (7/137).

Серед лексичної репрезентації джерела загрози виділяються безпосередньо суб'єкти, що створюють загрозу, організовані об'єднання і організації, неживі суб'єкти природної і техногенної приналежності.

До цієї групи примикає і частково з нею перетинається група Threatening means (засоби створення загроз) — група одиниць, що номінують засоби створення загрози: weapons (зброя), the stone incident that affected that passenger train (камінь, що потрапив у вікно пасажирського поїзда), a vehicular and knife

attack (напад за допомогою транспортного засобу і ножа), the maximum-security prison [Ibidem] (в'язниці особливо суворого режиму) (4/59).

Тут варто відзначити частковий перетин одиниць з одиницями інших груп. Так, в'язниці спочатку мають на меті усунення загрози, проте можуть виступати її джерелом (в контексті недостатності умов для утримання ув'язнених, а також внаслідок загрозливого характеру її компонента — «в'язнів»).

Група Threat consequences (наслідки загроз) — група номінації наслідків створення загрози — виявляється досить широкою за своїм семантичним наповненням і включає в себе різноманітні групові організації лексичного матеріалу в сукупності з номінацією явищ в процесі прийняття заходів щодо усунення та подальшої протидії загрозі та інших, пов'язаних з цим обставин, перетинаючись з цариною значень концепту «THREAT ABSENCE» (ВІДСУТНІСТЬ ЗАГРОЗИ). В якості одиниць, які репрезентують цю групу, можна подати такі: prison education program (програма освіти в тюрмах), history of crime and punishment (історія злочинів і покарань), catastrophic loss of life and mass destruction [Ibidem] (катастрофічних масштабів загибелі людей і масові руйнування) (3 / 98).

Протилежним фрейму «THREAT PRESENCE» (НАЯВНІСТЬ ЗАГРОЗИ) у дихотомії концепту «THREAT» (ЗАГРОЗА) виявляється фрейм «THREAT ABSENCE» (ВІДСУТНІСТЬ ЗАГРОЗИ), який, в свою чергу, являє собою комбінацію двох взаємопов'язаних слотів: «THREAT PREVENTION» (ЗАПОБІГАННЯ ЗАГРОЗИ) і «THREAT RESPONSE» (УСУНЕННЯ ЗАГРОЗИ). Обидва цих фрейми виявляють кореляцію у загальному значенні, хоча і покликані впливати на створену загрозу з різних сторін. Незважаючи на їх семантичні та екстралінгвістичні відмінності, дані фрейми виявляють аналогічну репрезентацію засобами мови. Лексичний матеріал, який реалізує зазначені фрейми, організовується відповідно до загальних структурних параметрів і включає кілька категоріальних груп в кожному з них. Так, першою з них можна назвати номінацію безпосередньо дії щодо запобігання або усунення загрози. Серед одиниць групи Prevention activity, що вербалізує дії із запобігання загрозі,

представлені наступні: opposed the invasion of Iraq (протистояти вторгненню в Ірак), to protect themselves (захистити себе), closing a loop hole in gun laws (закрити «дірку» в збройовому законодавстві), implored the police to increase security efforts in the neighborhood (спонукати поліцію посилити заходи безпеки в районі), placing security cameras and patrols (розмістити камери стеження і посилити патрулювання), life saving medical technology [Ibidem] (медична технологія, що дозволяє рятувати життя).

Одиниці групи Response activity, які репрезентують дії щодо усунення загрози, включають такі, як: to prosecute (залучати до відповідальності), to review the investigation (аналізувати розслідування), find evidence of political interference (знайти докази втручання поліції), to remove Kaspersky software from government systems (відмовитися від програмного забезпечення Касперського на урядових комп'ютерах), Homeland Security's decision (рішення Департаменту внутрішньої безпеки), mission to root out Islamic terrorism (місія з викорінення ісламського тероризму), fought over slavery [Ibidem] (боротися з рабством) (7 / 350).

Також в рамках цих концептів реалізуються групи Agencies and Agents (служби та службовці), що включають одиниці, які номінують служби та службовців, відповідальних за запобігання або усунення загрози: jails and prisons (тюремні і судові органи), Crime and Correction Committee (комітет із запобігання злочинам і пенітенціарна система), chairman of the California Public Defenders Association's legislative committee (голова законодавчого комітету Асоціації Громадських адвокатів Каліфорнії), critical care physician (реаніматолог), the president and executive director of Californians for Safety and Justice (президент і виконавчий директор Каліфорнійського товариства щодо забезпечення правопорядку і правосуддя), attorney general [Ibidem] (генеральний прокурор).

Близькою виявляється група Regulatory documents, яка об'єднує одиниці, що номінуютья регулятивні документи, які забезпечують механізми реалізації вищеописаних дій щодо усунення або запобігання загрози. Ця група включає широкий спектр репрезентуючих її одиниць: state regulations (державні постанови), statutes protecting police secrecy (закони, що захищають

конфіденційність діяльності поліції), a 1976 law enshrined in the state's civil rights code (закон від 1976, що входить до кодексу цивільних прав штату), A strict medical marijuana law (строгий закон про застосування марихуани в медичних цілях), Proposition 47 [Ibidem] (поправка 47) (5/98).

Суміжними є групи Prevention means (засоби запобігання) і Response means (засоби усунення), об'єктивує засоби протидії загрозі при її усунення або запобігання: $ 500 million to provide "security assistance" (500 мільйонів доларів на забезпечення безпеки, військова допомога), cells 'fences (решітки в камерах), cordon tape (загороджувальна стрічка), F-15 fighters (винищувач F-15), bullet proof vests [Ibidem] (куленепробивні жилети) (5/67).

Таким чином, концептосфера «SAFETY» / «SECURITY» (БЕЗПЕКА) в англійській мові будується на базовому концепті «THREAT» (ЗАГРОЗА), обсяг якого формується сукупністю взаємопроникаючих значень двох протилежноспрямованих фреймів: фрейма «THREAT PRESENCE» (НАЯВНІСТЬ ЗАГРОЗИ) і сукупністю обсягу фрейма «THREAT ABSENCE» (ВІДСУТНІСТЬ ЗАГРОЗИ), що включає обов'язкову дихотомію «THREAT PREVENTION» (ЗАПОБІГАННЯ ЗАГРОЗИ) і «THREAT RESPONSE» (УСУНЕННЯ ЗАГРОЗИ).

Семантика концептосфери заснована на семантиці категоріальних компонентів, номінуючих її груп, характерних для кожного фрейма зазначеного концепту. Такими структурними параметрами для фрейма «THREAT PRESENCE» (НАЯВНІСТЬ ЗАГРОЗИ) є групи, що репрезентують безпосередньо дію створення загрози, джерело загрози, наслідки та засоби створення загрози.

Фрейм «THREAT ABSENCE» (ВІДСУТНІСТЬ ЗАГРОЗИ) розглядається в нерозривній дихотомії його слотів-сценаріїв «THREAT PREVENTION» (ЗАПОБІГАННЯ ЗАГРОЗИ) і «THREAT RESPONSE» (УСУНЕННЯ ЗАГРОЗИ), виявляючи загальні цільові, але семантично різні групи лексики: групи, що номінують безпосередньо дії щодо запобігання або усунення загрози, групи, що номінують органи і служби, які реалізують зазначені дії, групи, шо вербалізують

документи та інші регулятивні інструменти, які вказують порядок дій щодо запобігання або усунення загрози, а також засоби для здійснення даних дій [70, с.45-46].

Концептосфера «CYBERSECURITY» / «SAFETY» / «SECURITY» (БЕЗПЕКА) в англійській мові реалізується шляхом спільного двостороннього впливу на сутність провідного значення концептосфери - загрози, при цьому кожен з двох структурних елементів виявляється неодмінною умовою існування концептосфери, релевантної для представника англійської мовної спільності.

3.1.2Лексична сполучуваність

Кожна національна культура в процесі розвитку формує притаманний їй образ безпеки та власне розуміння безпекових відносин. Мова стає одним із способів кодування різноманітних форм пізнання інформаційної безпеки: чуттєвого (відчуття, сприйняття, уявлення) і раціонального (поняття, судження, умовивід). Вивчення цього важливого елемента національної концептосфери англомовних носіїв лінгвістичними методами представляє, таким чином, науковий інтерес у зв'язку з підвищеною увагою до проблем кібербезпеки та її сутності в сучасній науці та правовій та юридичній практиці. В умовах соціально-економічних, політичних, культурних трансформацій сучасного суспільства, викликаних процесами інформатизації, глобалізації, що стрімко розвиваються останнім часом, руйнується традиційний набір стереотипів поведінки у динамічному кіберсередовищі, що ведуть у кінцевому підсумку до руйнування традиційних суспільних інститутів захисту інформаційної безпеки. Нові реалії народжують варіанти нових форм юридичного захисту, переосмислення традиційного поняття безпеки. Мова як чуйний барометр часу фіксує і відображає ці нові реалії. На думку С.Ю. Бакуліної, «концептосфера права – це система уявлень, значень, образів та асоціацій, що виникають в індивідуальній та масовій свідомості у процесі сприйняття і осмислення ключових морально-етичних категорій, що мають правове навантаження (закон,

відповідальність, свобода, обов'язок, вина, права людини, правопорядок, суд і т.д.)» [7, с. 4]. Тому в основі системи концептів текстів нормативно-правового типу лежить етична складова, в центрі якої знаходиться макроконцепт «моральність». Саме цей концепт в системі ієрархії концептів текстів нормативно-правових документів займає найбільш значиме місце. Одним з найсучасніших напрямів діяльності держави, який в останні роки набуває особливої актуальності і ваги, є кібербезпекова політика. Поява цього напряму завдячує динамічним технічним прогресом і проникненню інформаційних технологій у всі сфери людського життя. Правове регулювання кібернетично безпеки набуває надзвичайно важливого значення за умови зростання реальних загроз як окремим громадянам, так і організаціям, установам, закладам, державі в цілому. У свою чергу, процес нормотворчості має оперувати відповідним термінологічним апаратом, який в сфері кібернетичної безпеки сьогодні перебуває на етапі своєї розробки і потребує створення наукових засад номінації та застосування понять.

Головними тенденціями розвитку загроз в кіберпросторі є наступні:

- зростання числа атак, багато з яких ведуть до великих втрат;

- зростання складності атак, які можуть включати кілька етапів і застосовувати спеціальні методи захисту від можливих методів протидії;

- вплив практично на всі електронні (цифрові) пристрої, в числі яких останнім часом все більшої значущості набувають мобільні пристрої, а вони найбільшою мірою схильні до ризиків в сфері інформаційної безпеки;

- все частішими є випадки нападу на інформаційну інфраструктуру великих корпорацій, найважливіших промислових об'єктів і навіть державних структур;

- застосування найбільш розвиненими в сфері комп'ютерних технологій країнами коштів і методів кібернападів на інші держави.

Це підтверджується практично щоденними зведеннями новин, в яких повідомляється про нові атаки злочинців в інформаційній сфері. Число шкідливих об'єктів, які виявляються в мережі щорічно, обчислюється

мільярдами, їх поширення ведеться більш ніж 100 мільйонів інтернет адрес. Щороку це число збільшується на 40%. Атаки в інформаційному просторі завдають шкоди, яка оцінюється в 100 мілрд. дол. [63, с. 78]. Особливу небезпеку становлять загрози мобільних пристроїв, які раніше рідко піддавалися атакам. Динамічність розвитку інформаційної сфери призводить до необхідності мовної номінації нових об'єктів і предметів, які виникають в результаті наукової діяльності. Концепти, як ментально-логічні одиниці, з'являються внаслідок теоретико-пізнавальної, практичної чи експериментальної діяльності людини, матеріалізуються або залишаються абстрактами. На рівні когнітивної науки виникає потреба у знаходженні відповідної назви для досліджуваних об'єктів, конкретизується семантичне поле певної одиниці мови. Через специфічні особливості індивідуального світосприйняття й картини світу, формування системи знань людини про певні наукові концепції і методологічні засади ускладнюється об'єктивація новітніх предметів та явищ. З оглягу на сказане не припиняються наукові дискусії щодо сутності понять «інформаційний простір», «кібернетичний простір», «кібернетична безпека», «кібербезпекова політика» тощо. Навіть при первинній усталеності оснвних понять їхнє тлумачення, в тому числі й на нормативно-правовому рівні, не перестає бути об'єктом суперечок. Однак до текстів нормативних актів мають потрапляти найбільш точні значення термінів. Інтернаціоналізація клонцептосфери кібербезпеки зумловлена, в першу чергу, глобальним характером явища, переважанням англомовної термінології через дію екстралінгвістичних чинників (глобалізаційні процеси, пріоритетність окремих держав в галузі наукових досліджень, наявність досвіду у сфері державного управління певними явищами, широке поширення як світової мови тощо). Зазначене пояснює причину вжитку різних лексикотематичних груп номінацій концепту «CYBERSECURITY» у сфері інформаційної безпеки, починаючи із самого елементу «кібер», який став дуже продуктивним у словотворенні. Природа ретермінізації мовних одиниць сфери, що досліджуються, також є на поверхні. Техногенний характер кібербезпеки призводить до виникнення соціальних явищ, а це, у свою чергу, зумовлює

необхідність вироблення урядами країн політики та її закріплення у нормативно-правових актах. Відповідно до стилістичних норм вжиття термінології обмежується науковим стилем та його підстилями. Проте застосування юридичної термінології поза текстами наукових досліджень, а саме – в мові нормативно-правових документів – дещо розмиває саме наукові властивості терміну, надає йому нових якостей і функцій, тобто має місце детермінологізація. Має місце процес репрезентації термінології у нормативно-правових текстах. Терміни проходять шлях від складової концептосфери як методологічної основи явища кіберзагрози до наукового втілення ідеї про кібербезпеку, а потім – і виходу за межі науки з перетинанням у сферу правотворчості. Через легалізацію (законодавче закріплення терміну) він отримує принципово інший статус, фактично стає складовою норм права, частиною механізму правового регулювання у сфері протидії кіберзагрозам. Здійснимо аналіз репрезентації концепту «CYBERSECURITY» на основі таких важливих нормативно-правових актів як «Convention on cybercrime, opening of the treaty» та Congressional Bills 113th Congress from the U.S. Government Publishing Office [83]. Концепт «CYBERSECURITY» репрезентований у Конвенції Ради Європи про кіберзлочинність, прийнятій 23 листопада 2001 року, відому також як Будапештська конвенція (Convention on cybercrime, opening of the treaty). Наразі це єдиний глобальний документ міжнародного рівня, який є обов'язковим для держав-учасниць, який регулює дії по боротьбі з кіберзлочинністю. У 2017 році число сторін Конвенції збільшилася до 56, ще 14 держав підписали її або були запрошені приєднатися. Також концепт «CYBERSECURITY» широко представлений у Кодексі Сполучених Штатів. Хоча нові реалії вимагають численних змін у законодавство, про що свідчить проаналізований нами Законопроект 113-го Конгресу США (C. 2521 Представлено в Сенаті (IS)) (Congressional Bills 113th Congress From the U.S. Government Publishing Office [S. 2521 Introduced in Senate (IS)]. S. 2521. У преамбулі документу зазначено: «to amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security». Розподіл

представлених у згаданих законодавчих документах термінів за принципами фасетної класифікації дозволяє виділити наступні лексикосемантичні групи концептосфери «CYBERSECURITY» за номінаціями:

1. Суб'єкти кібербезпеки (cybersecurity entities – суб'єкти забезпечення кібербезпеки, critical infrastructure owners and managers – власники і розпорядники об'єктів критичної інфраструктур, Federal agency information security – Федеральне агентство інформаційної безпеки, the Chief Information Officers Council – Рада головних інформаційних служб та ін.); У текстах законодавчих актів зазначені номінації вжиті у наступному контексті: «…*provide a mechanism for improved oversight of Federal agency information security programs* [83]; *recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products* [83]; *coordinating Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council established under section 3603* [83].

2. Об'єкти кібербезпеки (*cyberspace - кіберпростір, critical information infrastructure – критична інформаційна інфраструктура, об'єкти критичної інфраструктури, objects of cyber defense - об'єкти кіберзахисту, national cybersecurity system - національна система кібербезпеки, sphere of electronic communications - сфера електронних комунікацій, external and internal security environment - зовнішнє та внутрішнє безпекове середовище, information and web resources - інформаційні та веб- ресурси, website - веб-сайт, blog platform - блог-платформа, video hosting - відеохостинги та ін.*); *«The term `national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency-- ``(i) the function, operation, or use of which-- ``(I) involves intelligence activities; ``(II) involves cryptologic activities related to national security; ``(III) involves command and control of military forces;* ``(IV) *involves equipment that is an integral part of a weapon or weapons system; or ``(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or ``(ii) is*

protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy» [83]; *«A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system»* [84]; *«Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed»* [84]; *«Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks»* [84].

3. Відомості, предмети і явища у кібернетичному просторі (*cybersecurity incident information – інформація про інцидент кібербезпеки, indicators of cyber threats - індикатори кіберзагроз, cybercrime – кіберзлочинність*).

Лексеми, які номінують названі відомості, предмети і явища у сфері кібернетичної безпеки, репрезентовані у текстах законів наступним чином: *«requirements for reporting security incidents to the Federal information security incident center established under section 3556»* [83]; «*Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies»* [83]; «*Cybersecurity research and development act. Section 8(d)(1) of the Cybersecurity Research and Development Act (15 U.S.C. 7406) is amended by striking «section 35342 and inserting «section 3554»* [83].

4. Дії та заходи, діяльність управлінсько-правового характеру *(state cybersecurity policy - державна політика у сфері кібербезпеки, criminal policy aimed at the protection of society against cybercrime – кримінальна політика, спрямована на захист суспільства від кіберзлочинності; providing cybersecurity – забезпечення кібербезпеки; coordination of cybersecurity activities – координація*

діяльності у сфері кібербезпеки; ensuring protection of the rights of users of communication systems – забезпечення захисту прав користувачів комунікаційних систем, timely detection, prevention and neutralization of real and potential threats to the national security in cyberspace – своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці у кіберпросторі, cyber defense – кібероборона, prevention of cyber incidents – запобігання кіберінцидентів, protection of national information resources – захист національних інформаційних ресурсів; public-private engagement in cybersecurity – державно-приватна взаємодія у сфері кібербезпеки; control over the legality of cyber security measures – контроль за законністю заходів із забезпечення кібербезпеки).

Номінації зазначеної лексико-семантичної групи функціонують в обох документах, про що свідчать наступні приклади: *«Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation»* [84]; «*This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system*» [84]; *«Protection of Information. Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations»* [84].

5. Технологічні процеси, процедури, засоби, які забезпечують безпеку у кіберпросторі (*detection and response to cyber threats – виявлення та реагування на кіберзагрози, ensuring that information security management processes – забезпечення процесів управління інформаційною безпекою, cyber defense tools – засоби кіберзахисту, process control system – система управління технологічними процесами, information security – захист інформації; implementation of*

organizational and technical model of cyber defense – впровадження організаційно-технічної моделі кіберзахисту). Зокрема, у законодавчих текстах ми зустрічаємо наступні приклади вживання номінацій даної лексико-семантичної групи: *«…ensuring that information security management processes are integrated with agency strategic and operational planning processes»* [84]; «*provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets*» [83]; *Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation* [84].

6. Юридично значущі події (*cyber security incident – інцидент кібербезпеки, cyberattack – кібератака, cyber threat – кіберзагроза, security threat to electronic communications systems – загроза безпеці систем електронних комунікацій*). Ця лексико-семантична група також широко представлена у досліджуваному законодавстві: «*perating the Federal information security incident center established under section 3556*»; «*Provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b)»* [83].

7. Правопорушення / злочини *(cybercrime (computer crime) – кіберзлочин (комп'ютерний злочин), cyberterrorism – кібертероризм; cyber espionage – кібершпигунство; breach of privacy/privacy breach – порушення конфіденційності; breach of confidentiality, integrity, accessibility of electronic information resources – порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів; disruption and / or blocking of the system and / or unauthorized management of its resources – зрив та/або блокування роботи системи, та/або несанкціоноване управління її ресурсами).* Наведемо приклади

репрезентації номінації даної лексико-семантичної групи у законодавстві у сфері регулювання кібербезпеки: *«Sec. 3559. Privacy breach requirements» (a) Policies and Procedures.--The Director, in consultation with the Secretary, shall establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information, including requirements for…»* [83]; *«The term `information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide»* [83]

Проведений аналіз дає підстави стверджувати, що законодавець чітко розмежовує об'єкти кібербезпеки (Cybersecurity) та об'єкти кіберзахисту (Cyber Defense). До першої групи він відносить такі глобальні категорії, як *person, human being, individual, rights and freedoms of man and citizen, user of information technology; society, sustainable development of cybernetic society and information communication environment; state, national security, including cybersecurity; national interests in all spheres of life of the individual, society and the state; information technology and telecommunications (electronic communications) as critical infrastructure.* На цьому рівні простежується поєднання абстрактних категорій з матеріальними об'єктами. До другої групи (objects of cyber defense) належать номінації, що позначають реальні об'єкти: *communication systems, cyberspace, cybersystems, objects of critical information infrastructure.* Варто звернути увагу на те, що об'єкти критичної інфраструктури у законі віднесені до категорії кібербезпеки, а об'єкти критичної інформаційної інфраструктури – до кіберзахисту [28, с. 105].

У зв'язку з цим виникає потреба у порівняльному аналізі нормативного тлумачення понять «кібербезпека» і «кіберзахист». Законодавець, надаючи дефініцію першого поняття, спирається на денотат «захищеність»: *«Cybersecurity is organized capabilities to protect against, mitigate from and rapidly recover from the effects of cyber attack»* [83]. *Що ж до спорідненого поняття, то воно тлумачиться так: «Cyber Defense is a computer network defense mechanism which includes response to actions and critical infrastructure protection and*

information assurance for organizations, government entities and other possible networks» [83].

Тож чітко відстежується одночасне вживання в межах одного нормативно-правового акту двох близьких за семантикою лексем «protection» і «security». Подальший розвиток діяльності держави у сфері кібернетичної безпеки, концептуальне вироблення засад політики у цій галузі можливо лише за умови комплексного поєднання науково виважених засад різних інтегративних наук і відтворення провідних концепцій у текстах відповідних нормативно-правових актів.

3.2 Специфіка перекладу мовних засобів репрезентації концепту «CYBERSECURITY» в українській мові

Переклад дипломатичних документів різного типу залишається актуальним питанням протягом довгого часу і вимагає особливої уваги у зв'язку зі специфікою дипломатичних текстів. В умовах постійно зростаючої міжнародного взаємодії, перекладач у цій царині має враховувати не тільки офіційно-діловий стиль спілкування, а й характерні риси різних дипломатичних документів.

У виконанні перекладу текстів подібного роду велике значення має перекладацька еквівалентність. Англійська перекладознавець Дж. Кетфорд визначає переклад як «заміну текстового матеріалу однієї мови еквівалентним матеріалом іншої мови» [71, с. 17]

Перекладацька еквівалентність — це схожість текстів оригіналу і перекладу за змістом, яка досягається перекладачем у процесі перекладу [3, с. 51] Однак, в рамках даної роботи, еквівалентність перекладу може бути визначена не тільки як смислова близькість двох текстів, а й максимальне збереження граматичної структури і специфіки стилю тексту. Крім того, необхідно також брати до уваги особливості (синтаксичні та лексичні) такого типу тексту як текст резолюції.

3.2.1 Аналіз лексичних трансформацій

Для перекладу резолюцій перекладачеві необхідно орієнтуватися на досягнення еквівалентності на рівні граматики, лексики і структури документа. Виділяють також три види можливих дій перекладачів, які мають місце і у перекладі тексту даної Резолюції [3, с. 59]:

- Використання перекладачем готових відповідностей (однозначна еквівалентність). Прикладами служать: (40) *General Assembly - Генеральна Асамблея;* (41) *multilingualism - багатомовність;* (42) *United Nations - Організація Об'єднаних Націй;* (43) *Secretary-General - Генеральний Секретар.*

- Вибір перекладачем з декількох варіантів (варіантні відповідності): (44) *Core value - головна цінність / ключова цінність / основна цінність;*

(45) *Comprehensive report - всеосяжна доповідь / комплексна доповідь / вичерпна доповідь; recalls - нагадує / посилається*.

- Перетворення тексту перекладачем (перекладацькі трансформації), що включають:

- заміну лексичної одиниці словосполученням:

(46)*... protecting and preserving diversity of languages and cultures globally ...* [3, с.68].

... захисту і збереження мов і культур в глобальному масштабі ... [3, с.68].

-заміну порядку слів:

(47) *Recognizing the contribution of multilingualism in promoting international peace and security, development and human rights, through the work of the United Nations departments and offices.* [3, с.69].

Визнаючи внесок, який багатомовність вносить, завдяки роботі департаментів і управлінь Організації Об'єднаних Націй, в забезпечення міжнародного миру і безпеки, розвитку і дотримання прав людини. [3, с.68].

На основі вивченого теоретичного матеріалу і вивчених офіційно-ділових документів міжнародних організацій та їх офіційних перекладів українською мовою, виділили перекладацькі трансформації, до яких найчастіше вдаються

перекладачі для досягнення адекватного перекладу концепту «CYBERSECURITY».

Відповідно до класифікації В.М. Комісарова, це лексичні та лексико-граматичні трансформації. Таким чином, можна зробити висновок, що перекладачі, у перекладі концептів у офіційно-ділових документах міжнародних організацій, більше уваги звертають на лексичну складову, ніж на граматичну. Це пояснюється тим, що у перекладі концепту «CYBERSECURITY» в офіційно-ділових текстах акцент робиться на досягнення еквівалентності перекладу, тобто існує необхідність передати точну, зрозумілу інформацію для досягнення головної мети офіційно-ділового стилю загалом - досягнення домовленості між двома сторонами.

Відповідно до аналізу, калькування, транскрипція і транслітерація – це перекладацькі трансформації, які найбільш часто використовуються для перекладу концепту «CYBERSECURITY» в англомовній офіційно-діловій документації міжнародних організацій українською мовою, наприклад:

(48) *«Concerned about the continued promulgation and application by Member States of laws and regulations, such as that promulgated on 12 March 1996 known as" the Helms-Burton Act ", the extraterritorial effects of which affect the sovereignty of other States, their* ***cybersecurity****, the legitimate interests of entities or persons under their jurisdiction and the freedom of trade and navigation»* [83, с.8].

«Будучи стурбованими тривалим прийняттям і застосуванням державами-членами законів і положень, таких як прийнятий 12 березня 1996 року Закон, відомий як« закон Хелмса-Бертона », екстериторіальні наслідки яких зачіпають суверенітет інших держав, їх ***кібербезпеку****, законні інтереси юридичних чи фізичних осіб, які підпадають під їх юрисдикцію, а також свободу торгівлі і судноплавства»* [50, с.16].

У цьому прикладі концепт cybersecurity перекладено за допомогою прийому калькування.

(49) *«We will also undertake appropriate measures for access to justice and protections for victims in criminal justice processes, including measures to ensure that identified victims are not penalized for having been trafficked and that they do not suffer from victimization as a result of actions taken by Government authorities,* ***cyberterrorists»*** [83, с.12].

«Будемо також вживати належних заходів для того, щоб жертви отримували доступ до правосуддя і були захищені в ході кримінального судочинства, в тому числі заходи, покликані не допустити, щоб виявлені жертви каралися за те, що стали об'єктами такої торгівлі, і не піддавалися віктимізації внаслідок дій державної влади та ***кібертерористів»*** [50, с.14]**.**

У наведеному вище прикладі концепт *cyberterrorists* був відтворений за допомогою транскрипції і транслітерації, так як в українській мові немає терміна-еквівалента. Цей термін є запозиченням, а за допомогою транскрипції і транслітерації вдалося зберегти його форму, звучання, а також саму прагматичну складову.

(50) *«Requirements for reporting security incidents to the Federal* ***information security*** *incident center established under section 3556»* [83, с.17];

«Вимоги щодо повідомлення інцидентів безпеки у Федеральному центрі інцидентів ***інформаційної безпеки****, створеному відповідно до розділу 3556»* [50, с.18].

У наведеному вище прикладі концепт *information security* був відтворений за допомогою транслітерації і калькування.

(51) *«Recognising the need for co-operation between States and private industry in combating* ***cybercrime*** *and the need to protect legitimate interests in the use and development of information technologies»* [84, с.7];

«Визнаючи необхідність співпраці між державами та приватною промисловістю у боротьбі з ***кіберзлочинністю*** *та необхідність захисту законних інтересів у використанні та розвитку інформаційних технологій»* [50, с.10].

У цьому прикладі концепт *cybercrime* був відтворений за допомогою транслітерації і калькування - *кіберзлочинністю*.

(52) ***«Cybersecurity** research and development act. Section 8(d)(1) of the Cybersecurity Research and Development Act (15 U.S.C. 7406) is amended by striking «section 35342 and inserting «section 3554»* [88, с.6].

*«Акт досліджень і розробок **кібербезпеки.** Розділ 8 (d) (1) Закону про дослідження та розвиток кібербезпеки (15 США 7406) доповнено виправленням "розділу 35342 та вставкою" розділу 3554».* [50, с.9].

У цьому прикладі концепт *cybersecurity* був відтворений за допомогою транслітерації і калькування – *кібербезпеки.*

(53) *«Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against **cybercrime**, inter alia, by adopting appropriate legislation and fostering international co-operation»* [84, с.17].

*«Переконаний у необхідності в першочерговому порядку проводити спільну кримінальну політику, спрямовану на захист суспільства від **кіберзлочинності,** зокрема, шляхом прийняття відповідного законодавства та сприяння міжнародному співробітництву»* [50, с.20].

У цьому прикладі концепт *cybersecurity* був відтворений за допомогою транслітерації і калькування – *кіберзлочинності.*

(54) *«This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or **protection of a computer system**»* [84, с.7].

«Ця стаття не повинна тлумачитися як накладення кримінальної відповідальності, коли виробництво, продаж, закупівля для використання, ввезення, розповсюдження чи іншим наданням у розпорядження чи володіння, зазначеним у пункті 1 цієї статті, не є метою вчинення злочину, встановленого відповідно до зі статтями 2 - 5 цієї Конвенції, наприклад,

*щодо дозволеного тестування або **захисту комп'ютерної системи** »* [50, с.20].

У цьому прикладі концепт *protection of a computer system* був відтворений за допомогою транслітерації і калькування – *захисту комп'ютерної системи.*

(55) *«Protection of Information. Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect **information security.** Such protections shall be commensurate with the risk and comply with all applicable laws and regulations* »[83, с.6].

«Захист інформації. Агентства та оцінювачі вживають відповідних заходів для забезпечення захисту інформації, яка, якщо буде розкрита, може негативно вплинути на інформаційну безпеку. Такі засоби захисту повинні відповідати ризику та відповідати усім чинним законам та нормам » [50, с.10].

У цьому прикладі концепт *information security* був відтворений за допомогою транслітерації і калькування – *інформаційну безпеку.*

(56) *«**Cybersecurity** is organized capabilities to protect against, mitigate from and rapidly recover from the effects of cyber attack»* [83, с.7].

*«**Кібербезпека** - це організована спроможність захищати від наслідків кібератаки та швидко їх відновлювати»* [50, с.9].

У цьому прикладі концепт *cybersecurity* був відтворений за допомогою транслітерації і калькування – *кібербезпека.*

(57) *«**Cyber Defense** is a computer network defense mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks»* [83, с.12].

***«Кіберзахист** - це механізм захисту комп'ютерної мережі, який включає реагування на дії та захист критичної інфраструктури та забезпечення інформації для організацій, державних структур та інших можливих мереж»* [50, с.15].

У цьому прикладі концепт *cyber defense* був відтворений за допомогою транслітерації і калькування – *кіберзахист.*

(58) *«3559. Privacy breach requirements» (a) Policies and Procedures.--The Director, in consultation with the Secretary, shall establish and oversee policies and*

procedures for agencies to follow in the event of a breach of ***information security*** *involving the disclosure of personally identifiable information, including requirements for…»* [83, с.11].

«3559. Вимоги щодо порушення конфіденційності»(а) Політика та процедури. - Директор, консультуючись із Секретарем, встановлює та контролює політику та процедури, якими слід скерувати агенції у разі порушення ***інформаційної безпеки****, що передбачає розкриття особистої ідентифікації. інформація, включаючи вимоги щодо… »* [50, с.13].

У цьому прикладі концепт *information security* був відтворений за допомогою транслітерації і калькування – *інформаційної безпеки.*

(59) *«The term* ***`information security'*** *means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide»* [83, с.11]

"*Термін"* ***інформаційна безпека*** *"означає захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, зриву, модифікації чи знищення з метою надання"* [50, с.14].

У цьому прикладі концепт *information security* був відтворений за допомогою транслітерації і калькування – *інформаційна безпека.*

(60) «*Perating the Federal* ***information security*** *incident center established under section 3556*». [83, с.20].

«Перевірка Федерального центру інцидентів ***інформаційної безпеки,*** *створеного відповідно до розділу 3556»;* [50, с.21].

У цьому прикладі концепт *information security* був відтворений за допомогою транслітерації і калькування – *інформаційної безпеки.*

(61) «*Provide, as appropriate, intelligence and other information about* ***cyber threats****, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b)»* [83, с.16].

«Зробити, відповідно, розвідувальну та іншу інформацію щодо ***кіберзагрози****, вразливості та інцидентів для агентств для надання допомоги в оцінках ризику, проведених відповідно до розділу 3554 (b)»* [50, с.20].

У цьому прикладі концепт *cyber threats* був відтворений за допомогою калькування – *кіберзагрози.*

(62) *«…ensuring* ***information security*** *management processes are integrated with agency strategic and operational planning processes»* [83, с.8].

«… забезпечення інтеграції процесів ***управління інформаційною безпекою*** *з процесами стратегічного та оперативного планування агентства»* [50, с.10].

У цьому прикладі концепт *information security* був відтворений за допомогою транслітерації і калькування – *інформаційною безпекою.*

(63) «…*provide a comprehensive framework for ensuring the effectiveness of* ***information security controls*** *over information resources that support Federal operations and assets»* [83, с.5].

«…забезпечити комплексну основу для забезпечення ефективності ***контролю інформаційної безпеки*** *інформаційних ресурсів, що підтримують федеральні операції та активи»* [50, с.7].

У цьому прикладі концепт *information security controls* був відтворений за допомогою транслітерації і калькування – *контролю інформаційної безпеки.*

(64) *Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of* ***computer systems, networks and computer data*** *as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation* [84, с.7].

«Переконаний, що ця Конвенція необхідна для стримування дій, спрямованих на конфіденційність, цілісність та ***доступність комп'ютерних систем, мереж та комп'ютерних даних****, а також на неправильне використання таких систем, мереж та даних шляхом забезпечення криміналізації такої поведінки, як описано в цій Конвенції, та прийняття повноважень, достатніх для ефективної боротьби з такими кримінальними*

правопорушеннями, шляхом сприяння їх виявленню, розслідуванню та кримінальному переслідуванню як на внутрішньому, так і на міжнародному рівнях, а також шляхом забезпечення швидкого та надійного міжнародного співробітництва [50, с.22].

У цьому прикладі концепт *computer systems, networks and computer data* був відтворений за допомогою транслітерації і калькування – *доступність комп'ютерних систем, мереж та комп'ютерних даних.*

(65) «*…provide a mechanism for improved oversight of Federal agency* ***information security*** *programs»* [83, с.3].

«… забезпечити механізм удосконалення контролю за програмами ***інформаційної безпеки*** *Федерального агентства»* [50, с.5].

У цьому прикладі концепт *information security* був відтворений за допомогою транслітерації і калькування – *інформаційної безпеки.*

(66) «*…recognize that the selection of specific technical hardware and software* ***information security*** *solutions should be left to individual agencies from among commercially developed products* [83, с.4].

«…визнають, що вибір конкретних технічних апаратних та програмних рішень щодо ***захисту інформації*** *повинен залишатися окремим агенціям з числа комерційно розроблених продуктів* [50, с.5].

У цьому прикладі концепт *information security* був відтворений за допомогою транслітерації і калькування – *захисту інформації.*

(67) «*coordinating Government-wide efforts on* ***information security*** *policies and practices, including consultation with the Chief Information Officers Council established under section 3603* [83, с.3].

«координація зусиль уряду щодо політики та практики ***інформаційної безпеки,*** *включаючи консультації з Радою головних інформаційних служб, створеною відповідно до розділу 3603* [50, с.6].

У цьому прикладі концепт *information security* був відтворений за допомогою транслітерації і калькування – *інформаційної безпеки.*

(68) *«The term* ***`national security system'*** *means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency-- ``(i) the function, operation, or use of which-- ``(I) involves intelligence activities; ``(II) involves cryptologic activities related to national security; ``(III) involves command and control of military forces*; ``(IV) *involves equipment that is an integral part of a weapon or weapons system; or ``(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or ``(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of* ***national defense*** *or foreign policy»* [83, с.2].

«*Термін* ***«система національної безпеки»*** *"означає будь-яку інформаційну систему (включаючи будь-яку телекомунікаційну систему), що використовується або керується агентством або підрядником агентства або іншою організацією від імені агентства--` `(i) функція, функціонування або використання яких-- `` (I) передбачає розвідувальні дії; `` (II) передбачає криптологічні дії, пов'язані з національною безпекою; `` (III) передбачає командування та контроль військових сил; `` (IV) передбачає обладнання, яке є невід'ємною частиною зброї або системи озброєння; або `` (V), що підпадає під підпункт (B), має вирішальне значення для безпосереднього виконання військових або розвідувальних місій; або `(ii) захищений у будь-який час процедурами, встановленими для інформації, спеціально дозволеної відповідно до критеріїв, встановлених Виконавчим розпорядженням або Актом Конгресу, що класифікуються в інтересах* ***національної оборони*** *чи зовнішньої політики"* [50, с.20].

У цьому прикладі концепти *`national security system'* та *national defense* були відтворений за допомогою транслітерації і калькування *–система національної безпеки* та *національної оборони.*

(69) *«A Party may require that the offence be committed by* ***infringing security measures****, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system»* [84, с.7].

«Сторона може вимагати, що правопорушення було вчинено із ***порушенням заходів безпеки****, з наміром отримати комп'ютерні дані чи інший нечесний намір, або стосовно комп'ютерної системи, підключеної до іншої комп'ютерної системи»* [50, с.23].

У цьому прикладі концепт *infringing security measures* був відтворений за допомогою калькування – *порушенням заходів безпеки.*

(70) *«Where the requested Party believes that preservation will not ensure the future availability of the data or will* ***threaten the confidentiality*** *of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed»* [84, с.8].

«Якщо запитувана Сторона вважає, що охорона не забезпечить майбутню доступність даних або загрожує конфіденційності або іншим чином завдасть шкоди розслідуванню запитуючої Сторони, вона негайно повідомляє про це Сторону, яка запитує, яка визначає, чи буде запит виконано» [50, с.23].

У цьому прикладі концепт *threaten the confidentiality* був відтворений за допомогою транслітерації та калькування – *загрожує конфіденційності.*

(71) *«Concerned by the risk that* ***computer networks and electronic information may also be used for committing criminal offences*** *and that evidence relating to such offences may be stored and transferred by these networks»* [84, с.7].

«Стурбований ризиком того, що ***комп'ютерні мережі та електронна інформація також можуть використовуватися для вчинення кримінальних злочинів,*** *і що ці мережі можуть зберігати та передавати ці мережі»* [50, с.23].

У цьому прикладі концепт *комп'ютерні мережі та електронна інформація також можуть використовуватися для вчинення кримінальних злочинів* був відтворений за допомогою транслітерації та калькування –

комп'ютерні мережі та електронна інформація також можуть використовуватися для вчинення кримінальних злочинів.

(72) «*One important requirement of an efficient education and information strategy is open communication of the* ***latest cybercrime threats****. Some states and/or private businesses refuse to emphasize that citizens and clients respectively are affected by* ***cybercrime threats****, in order to avoid them losing trust in online communication services. The United States Federal Bureau of Investigation has explicitly asked companies to overcome their aversion to negative publicity and report* ***cybercrime****. In order to determine threat levels, as well as to inform users, it is vital to improve the collection and publication of relevant information»* [91, с.4].

«Однією з важливих вимог ефективної освітньої та інформаційної стратегії є відкрите повідомлення про новітні ***загрози кіберзлочинності.*** *Деякі держави та / або приватний бізнес відмовляються підкреслювати, що громадяни та клієнти відповідно зазнають* ***загрози кіберзлочинності****, щоб уникнути втрати довіри до Інтернет-служб зв'язку. Федеральне бюро розслідувань США чітко просило компанії подолати свою неприязнь до негативної реклами та повідомити про* ***кіберзлочинність.*** *Для визначення* ***рівнів загрози****, а також для інформування користувачів важливо вдосконалити збір та публікацію відповідної інформації »* [50, с.25].

У цьому прикладі концепт *latest cybercrime threats* був відтворений за допомогою транслітерації та калькування – *загрози кіберзлочинності.*

(73) **«*Intellectual property*** *– creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract "properties" has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered»* [85, с.2].

«Інтелектуальна власність *- такі твори, як музичні, літературні та художні твори; винаходи; і символи, імена, зображення та конструкції, що використовуються в комерції, включаючи авторські права, торгові марки,*

патенти та суміжні права. Відповідно до законодавства щодо інтелектуальної власності, власник однієї з цих абстрактних «властивостей» має певні ексклюзивні права на твір, комерційний символ чи винахід, якими він охоплюється » [50, с.12].

У цьому прикладі концепт *intellectual property* був відтворений за допомогою транслітерації та калькування – *«інтелектуальна власність.*

(74) «*criminal activity where services or applications in the* ***Cyberspace*** *are used for or are the target of a crime, or where the* ***Cyberspace*** *is the source, tool, target, or place of a crime»* [87, с.2].

«злочинна діяльність, коли послуги чи програми в ***Кіберпросторі*** *використовуються для/ або є об'єктом злочину, або де* ***Кіберпростір*** *є джерелом, інструментом, ціллю або місцем злочину»* [50, с.10].

У цьому прикладі концепт *cyberspace* був відтворений за допомогою транслітерації та калькування – *кіберпростір.*

(75) *$ 500 million to provide "****cybecsecurity assistance"***

500 мільйонів доларів на ***забезпечення кібербезпеки.***

У цьому прикладі концепт *cybecsecurity assistance* був відтворений за допомогою транслітерації та калькування – *забезпечення кібербезпеки.*

(76) *«Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the* ***cyber environment****.* ***Cybersecurity*** *strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the* ***cyber environment****»* [88, с.3].

«До активів організації та користувачів належать підключені обчислювальні пристрої, персонал, інфраструктура, додатки, послуги, телекомунікаційні системи та сукупність переданої інформації в ***кібер-середовищі. Кібербезпека*** *прагне забезпечити досягнення та підтримку властивостей безпеки організації та активів користувача проти відповідних ризиків безпеки в* ***кібер-середовищі****»* [50, с.24].

У цьому прикладі концепти *cyber environment* та *cybersecurity* були відтворені за допомогою транслітерації та калькування – *кібер-середовище, кібербезпека.*

(77) *The term **“cybercrime**” is used to cover a wide variety of criminal conduct. As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime.* [91].

*Термін **"кіберзлочинність"** використовується для охоплення найрізноманітніших злочинних дій. Оскільки визнані злочини включають широкий спектр різних злочинів, складно розробити типологію або систему класифікації кіберзлочинності.* [50, с.24].

У цьому прикладі концепт *cybercrime* був відтворений за допомогою транслітерації та калькування – *кіберзлочинність.*

(78) «*...for Developing Counries» термін identity theft interpreted as **«the fraudulent practice of using another person's** name and personal information in order to obtain credit, loans,* etc.» [91, с.3].

*«…для країн, що розвиваються термін «**крадіжки особистих даних»** трактується як« шахрайська практика використання імені та особистої інформації іншої особи для отримання кредиту, позики тощо».* [50, с.24].

У цьому прикладі концепт *«the fraudulent practice of using another person'* був відтворений за допомогою калькування – *крадіжки особистих даних.*

(79) «*In addition, some terms that are used to describe criminal acts (such as “**cyberterrorism**” or “**phishing**”) cover acts that fall within several categories. Nonetheless, the four categories can serve as a useful basis for discussing the phenomena of **cybercrime***» [91, с.3].

«*Крім того, деякі терміни, які використовуються для опису злочинних діянь (наприклад, «**кібертероризм**» чи «**фішинг**»), охоплюють діяння, що належать до кількох категорій. Тим не менше, чотири категорії можуть слугувати корисною основою для обговорення явищ **кіберзлочинності**»* [50, с.24].

У цьому прикладі концепти *cyberterrorism, phishing, cybercrime* були відтворені за допомогою транслітерації та калькування – *кібертероризм, фітинг, кіберзлочинність.*

(80) *"Organizational structures" focuses on the prevention, detection, response to and crisis management of* ***cyberattacks,*** *including the protection of critical information infrastructure systems»* [91, с.4].

"Організаційні структури" зосереджуються на запобіганні, виявленні, реагуванні на ***кібератаки*** *та протидії кризам, включаючи захист критичних систем інформаційної інфраструктури "* [50, с.25].

У цьому прикладі концепт *cyberattacks* був відтворений за допомогою калькування – *кібератаки.*

(81) *«****Cyberspace attack*** *– cyberspace actions that create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains»* [85, с.3].

*«****Атака на кіберпростір*** *- дії на кіберпростір, які створюють різні ефекти прямого заперечення (тобто деградація, зрив чи руйнування) та маніпуляції, що призводять до приховування, того, що є прихованим або проявляється у фізичних царинах»* [50, с.11].

У цьому прикладі концепт *cyberspace attack* був відтворений за допомогою калькування – *атака на кіберпростір.*

(82) *«The General Assembly, Noting the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information, Recognizing that the need for* ***cybersecurity*** *increases as countries increase their participation in the information society, Noting also the work of relevant international and regional organizations on enhancing* ***cybersecurity and the security of information technologies.*** [88, с.2].

«Генеральна Асамблея, відзначаючи зростаючу залежність урядів, підприємств, інших організацій та окремих користувачів від інформаційних технологій для надання основних товарів і послуг, ведення бізнесу та обміну

інформацією, визнаючи необхідність зростання ***кібербезпеки****, оскільки країни збільшують свою участь у інформаційному суспільстві, відзначаючи також роботу відповідних міжнародних та регіональних організацій щодо підвищення* ***кібербезпеки та безпеки інформаційних технологій***. [50, с.18].

У цьому прикладі концепт *cybersecurity and the security of information technologies* був відтворений за допомогою транслітерації та калькування – *кібербезпеки та безпеки інформаційних технологій.*

(83) *«****Cybersecurity*** *is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the* ***cyber environment*** *and organization and user's assets* [88, с.3].

*«****Кібербезпека*** *- це сукупність інструментів, політики, концепцій безпеки, гарантій безпеки, настанов, підходів до управління ризиками, дій, навчання, кращих практик, забезпечення та технологій, які можна використовувати для захисту* ***кіберсередовища*** *організації та активів користувача* [50, с.18]. У цьому прикладі концепти *cybersecurity та cyber environment* були відтворені за допомогою транслітерації та калькування – *кібербезпека та кіберсередовища.*

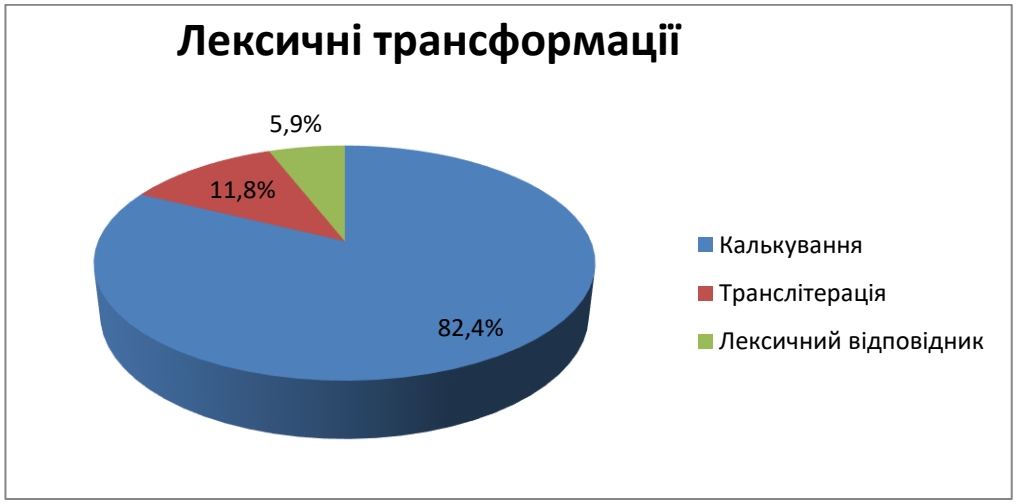

Рис. 3.1. Лексичні трансформації

Тож, можна зробити висновки, що основними прийомами перекладу концептів групи CYBERSECURITY є транслітерація, калькування та лексичні відповідники.

3.2.2 Специфіка лексико-граматичних трансформацій

Розглянемо приклади лексико-граматичних трансформацій у перекладі концептів групи CYBERSECURITY на матеріалі текстів міжнародних документів.

Заміна лексичної одиниці словосполученням відноситься до лексико-граматичним трансформаціям, наприклад:

(84)*... this requires protection and conservation on a global scale from* ***cyber espionage ...*** [87, с.2].

.. це вимагає захисту і збереження в глобальному масштабі від ***інформаційного шпіонажу ...*** [50, с.2].

У цьому прикладі концепт *cyber espionage* замінено словосполученням *інформаційного шпіонажу.*

(85) *...recognizing also that the United Nations has recognized criminal negligence in the* ***cyberspace…*** [92, с.2].

...визнаючи також, що Організація Об'єднаних Націй визнала злочинну недбалість ***у сфері інформаційної безпеки….*** [50, с.18].

У цьому прикладі концепт *cyberspace* замінено словосполученням *у сфері інформаційної безпеки.*

(86)*... encourages the Secretary General to continue his efforts towards ending the* ***Internet warfare.*** [87, с.2].

.. рекомендує Генеральному секретарю продовжувати докладати зусилля в напрямку ***припинення війни в інформаційному просторі.*** [50, с.2].

У цьому прикладі концепт *Internet warfar* замінено словосполученням *припинення війни в інформаційному просторі.*

(87) *«According to the president, the United States sought de-escalation in Syria. He noted that the actions of the "criminal" regime of Assad, including the use of chemical weapons, shocked the world. It is for these reasons that the United States*

attacked the Syrian air base, causing destruction, casualties and new ***cyber threats».*** [87, с.2].

«За словами президента, Сполучені Штати прагнули до деескалації в Сирії. Він зазначив, що дії «злочинного» режиму Асада, в тому числі використання ним хімічної зброї, потрясли світ. Саме з цих причин Сполучені Штати здійснили напад на сирійську авіабазу, що спричинило руйнації, жертви та ***нові загрози в інформаційному світі».*** [50, с.2].

У цьому прикладі концепт *cyber threats* замінено словосполученням *нові загрози в інформаційному світі.*

(88) «*Recalling that the United Nations Millennium Declaration includes a call for adherence to the "Olympic Truce" and tolerance on the* ***cyber environment*** *now and in the future and to support the International Olympic Committee in its efforts to promote peace and understanding between people through sport and the embodiment of Olympic ideals. "* [90, с.3].

«Нагадуючи про те, що в Декларацію тисячоліття Організації Об'єднаних Націй включений заклик дотримуватися «олімпійського перемир'я» та ***толерантності на теренах інтернету*** *наразі і в майбутньому і підтримувати Міжнародний олімпійський комітет в його*
зусиллях щодо заохочення миру і взаєморозуміння між людьми за допомогою спорту та втілення олімпійських ідеалів». [50, с.13].

У цьому прикладі концепт *cyber environment* замінено словосполученням *толерантності на теренах інтернету*.

(89) *«Taking note of declarations and resolutions of different intergovernmental forums, bodies and Governments that express the rejection by the international community and public opinion of the promulgation and application of measures of the kind referred to above on* ***cybersecurity».*** [87, с.3].

«Беручи до уваги заяви і резолюції різних міжурядових форумів, органів і урядів, в яких виражається незгода міжнародної спільноти та громадськості з прийняттям і застосуванням заходів, подібних вищезазначеним щодо ***кібернетичної безпеки».*** [50, с.3].

Цей приклад так само ілюструє чітку передачу морфемного складу англомовного терміна *cybersecurity* – модуляцію значення.

(90) «*Request the Conference on Disarmament to commence negotiations on the item "Prevention of nuclear war" of its agenda and to consider, inter alia the elaboration of an international instrument of a legally binding character laying down the obligation not to be the first to use nuclear weapons and* ***information security issues».*** [87, с.3].

«Просить Конференцію із роззброєння розпочати переговори по пункту її порядку денного« Запобігання ядерної війни »і розглянути, зокрема розробку міжнародного документа юридично обов'язкового характеру, в якому було б сформульовано зобов'язання не застосовувати першим ядерну зброю і питання ***кібербезпеки».*** [50, с.3].

Даний приклад так само ілюструє чітку передачу англомовного концепта *information security issues* модуляцією значення - *кібербезпеки*.

(91) *«In documents of the International Telecommunication Union under* ***Cyberspace****, means "an environment with connected computer devices,users, infrastructure, applications, services, telecommunication systems, as well as the totality of transmittedand / or information stored in this environment».* [83, с.2].

«У документах Міжнародного союзу електрозв'язку під ***кіберпростором****, розуміється «середовище з підключеними комп'ютерними пристроями,користувачами, інфраструктурою, додатками, сервісами, телекомунікаційними системами, а також сукупність переданої або збереженої в цьому середовищі інформації».* [50, с.9].

У цьому прикладі концепт *Cyberspace* був відтворений за допомогою транслітерації та калькування – *кіберпростором.*.

У документах міжнародних організацій, зокрема Організації Об'єднаних Націй, використовується словосполучення *Information and Telecommunication Technologies*, яке українською мовою перекладається по-різному: *«інформаційно-комунікаційні технології», «інформаційні та комунікаційні технології».* Вживання в цьому словосполученні дефіса або використання

сполучника «і», безсумнівно, змінює смислові характеристики і контекст їх застосування. Так, використання дефіса в українському перекладі терміна «*інформаційно-комунікаційні технології*» дає можливість віднести міжнародно-правове регулювання телекомунікацій до сфери діяльності Міжнародного союзу електрозв'язку та виділяти при цьому інформаційні технології як окрему сферу міжнародно-правового регулювання, що в значній мірі збігається зі сферою «транскордонного управління» інтернетом.

(92)*... recommends that the Secretary-General continue his efforts in the field* ***of information and communication security…*** [89, с.2].

… рекомендує Генеральному секретарю продовжувати докладати зусилля в напрямку ***безпеки у царині інформаційно-комунікаційних технологій…*** [50, с.12].

Переклад концепту *of information and communication security* здійснено способом додавання - *безпеки у царині інформаційно-комунікаційних технологій*.

Заміна порядку слів у реченні є граматичною трансформацією, наприклад:

(93) *Recognizing the contribution of multilingualism in promoting international peace and* ***security,*** *development and human rights, through the work of the United Nations departments and offices.* [87, с.3].

Визнаючи внесок, який багатомовність вносить, завдяки роботі департаментів і управлінь Організації Об'єднаних Націй, в забезпечення міжнародного миру і ***безпеки****, розвитку і дотримання прав людини.* [50, с.3].

(94) *US Supreme Court in 2005 made a decision on the difference in classifications "****information services" and "telecommunications****", which influenced the differences in their legal regulation and use in US law enforcement practice.* [87, с.3].

*Верховний суд США в 2005 р. виніс рішення про відмінність класифікацій «****інформаційні послуги»*** *і* ***«телевізійні комунікації»****, що вплинуло на відмінності в їх правовому регулюванні і використанні в правозастосовчій практиці США.* [50, с.3].

Переклад концептів *"**information services**"* та *"**telecommunications**"*, здійснено способами калькування, транслітерації та модуляції.

(95) *In a comprehensive discussion, the WGIG (Working Group on Internet Governance) has defined the concept of "Internet governance": Internet governance is the introduction and application by governments, the private sector and civil society, in their respective roles, of general principles, norms, rules, decision-making procedures and programs. regulate the evolution and use of the Internet* ***within information security.*** [86, с.3].

Робоча група WGIG (Робоча група з управління інтернетом) з урахуванням всебічного обговорення виробила визначення поняття «управління інтернетом»: управління інтернетом є запровадження та застосування урядами, приватним сектором і громадянським суспільством, при виконанні ними своєї відповідної ролі, загальних принципів, норм, правил, процедур прийняття рішень і програм, що регулюють еволюцію і застосування інтернету в межах ***інформаційної безпеки.*** [50, с.13].

(96) *In Internet governance, Stakeholders play their "respective roles" in* ***information security.***

В управлінні інтернетом зацікавлені сторони виконують свої «відповідні ролі» з ***інформаційної безпеки.***

(97) *The role and responsibilities of governments are related to such aspects*

activities such as the development, coordination and implementation of public policy at the national level, policy coordination at the regional and international levels; creating favorable conditions for the development of ***information and communication.*** [88, с.2].

Роль і обов'язки урядів пов'язані з такими аспектами діяльності, як розробка, координація та здійснення державної політики на національному рівні, координація політики на регіональному та міжнародному рівнях; створення сприятливих умов для розвитку ***інформаційних і комунікаційних технологій (ІКТ).*** [50, с.6].

За допомогою генералізації можна слово з вужчим значенням *перекласти словом з більш широким значенням, наприклад:*

(98) *«Urges all Member States requesting exemption under Article 19 of the Charter to submit as much information as possible in support of their requests and to consider submitting such information in advance of the deadline specified in resolution 54/237 C so as to enable the collation of any additional detailed information that may be necessary 9 ».* [87, с.3].

«Настійно закликає всі держави-члени, які звертаються з проханням про застосування вилучення, передбаченого в статті 19 Статуту, представляти якомога більше інформації в обгрунтування своїх прохань і прагнути подавати таку інформацію завчасно до граничного терміну, встановленого в резолюції 54/237 з тим, щоб мати можливість отримувати і аналізувати будь-яку додаткову детальну інформацію, яка може знадобитися». [50, с.3].

Цей приклад демонструє як термін, що складається з одного компонента, переклали поєднанням слів для більш точного і детального опису того, що потрібно, згідно зі статтею 19 Статуту, від держав-членів організації.

Описовий переклад - не настільки часто використовувана перекладацька трансформація як, наприклад, модуляція, але теж необхідна, коли в мові, на який здійснюється переклад, немає подібного поняття, терміна, феномена. У такому випадку застосовується описовий переклад, за допомогою якого детально описується вихідний термін, наприклад:

(99) *«Recalling that the United Nations was founded in the aftermath of two world wars to help shape a better future, he said the United States had developed the Marshall* ***Plan to help restore Europe****, guided by the pillars of sovereignty,* ***security*** *and prosperity10».* [84, с.2].

«Нагадуючи, що Організація Об'єднаних Націй була створена після двох світових воєн, з метою допомогти сформувати краще майбутнє. Сполучені Штати розробили ***Програму відновлення Європи у царині кібербезпеки****, щоб допомогти відновити Європу, керуючись засадами суверенітету,* ***безпеки*** *і процвітання».* [50, с.12].

Тут перекладач використовував описовий переклад, так як для нашої культури цей термін, назва даного плану, не несе ніякого сенсу.

(100) *Calls upon the Secretary-General to continue to develop the network of focal points that supports the Coordinator for* ***cybersecurity.*** [84, с.3].

Закликає Генерального секретаря продовжувати розвивати мережу кураторів, що сприяють Координатору з питань ***кібербезпеки.*** [50, с.12].

У цьому прикладі здійснена заміна підрядно-означального речення на підрядно-з'ясувальне, до складу якого входить концепт *cybersecurity/ кібербезпеки.*

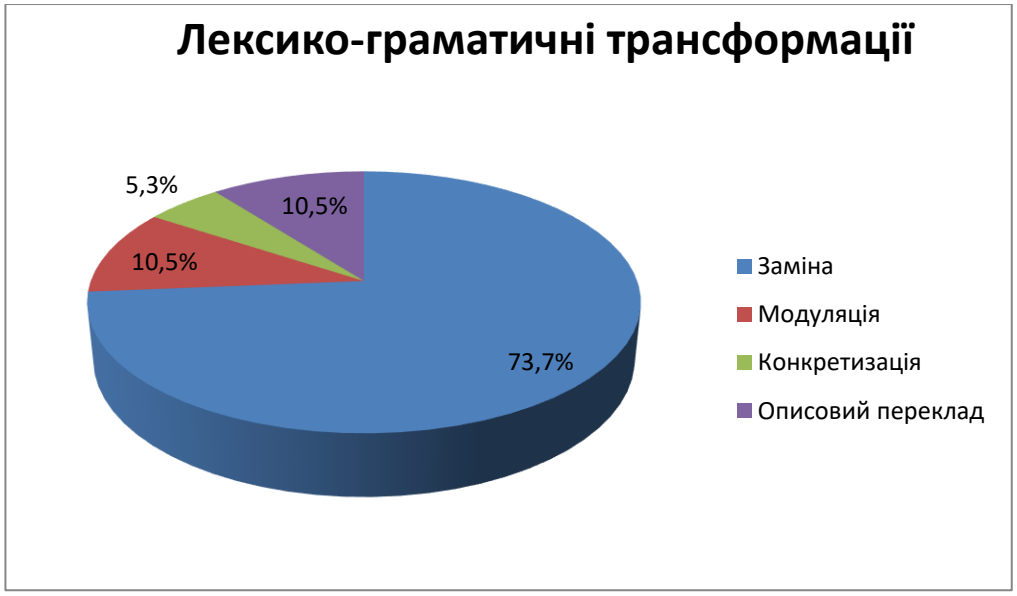

Рис. 3.2. Лексико-гаматичні трансформації

Тож, найпоширенішими лексико-граматичними трансформаціями у перекладі концепту «CYBERSECURITY» є заміни, модуляція, конкретизація, описовий переклад. Лексичні та лексико-граматичні трансформації перекладу концепту «CYBERSECURITY» подано у додатку (Додаток Б).

Таким чином, для успішного перекладу правозахисної лексики в ООН перекладачеві необхідно не тільки володіти великими загальними знаннями, розуміти особливості діяльності організації, бути в курсі актуальної інформації, але також і орієнтуватися у всіх супутніх тематиках - знати загальну термінологію ООН та інших міжнародних організацій, протокольну і процесуальну лексику.

Висновки до розділу 3

Законодавчий підстиль відрізняється більшою стилістичною і мовною однорідністю, ніж документи інших підстилів. У цих текстах можна відзначити широке використання юридичної термінології. У законодавчому підстилі використовується абстрактна лексика і практично відсутні експресивно-емоційні мовні засоби, оцінна лексика. Тут багато антонімів, оскільки законодавча мова відображає протилежні інтереси, протиставляє і зіставляє поняття. Розподіл термінів, які вжиті у нормативно-правових текстах, за принципами фасетної класифікації дає підстави виділити сім основні лексико-семантичні групи концептосфери «CYBERSECURITY» за номінаціями:

- суб'єкти кібербезпеки;
- об'єкти кібербезпеки;
- відомості, предмети і явища у кібернетичному просторі;
- дії та заходи, діяльність управлінсько-правового характеру;
- технологічні процеси, процедури, засоби, які забезпечують безпеку у кіберпросторі;
- юридично значущі події;
- правопорушення / злочини.

Лексеми, що наповнюють концептосферу «CYBERSECURITY» нормативноправових актів, носять колективний характер і мають інваріантне ядро (security), закріплене у дефініціях законів та підзаконних актів. Однак не можна не відзначити незначну варіативну складову їх змісту, яка визначається областю застосування: власне офіційно-діловий стиль, наукова публіцистика.

У ході практичної частини роботи було проведено аналіз офіційних англомовних документів міжнародних організацій, таких як ООН, а також їх офіційні переклади українською мовою.

В обраних документах висвітлювалися такі теми:

-проблеми кібербезпеки;

- спорт на благо миру та розвитку; Олімпійські ідеали;

- призупинення санкцій США проти Куби;
- незастосування ядерної зброї і запобігання ядерній війні;
- глобальний план ООН щодо боротьби торгівлею людьми;
- розподіл витрат ООН;
- війна в Сирії;
- боротьба з ісламською державою;
- ситуація в Північній Кореї.

З перерахованих вище джерел за допомогою методу суцільної вибірки було виділено концепти із сфери *CYBERSECURITY,* які представляють інтерес для аналізу їх перекладу.

Таким чином, було виявлено, що більшість концептів перекладаються за допомогою калькування, транслітерації і транскрибування, лексико-граматичних замін, конкретизації та описового перекладу.

Було виявлено, що наразі існує тенденція використання модуляції для перекладу термінів в концептів в офіційно-ділових текстах. Це означає, що терміни-концепти в офіційно-ділових текстах втрачають свою однозначність, так як для досягнення їх еквівалентного перекладу використовується прийом смислового розвитку на основі причинно-наслідкового зв'язку.

ВИСНОВКИ

У роботі розглянуто загальні жанрові особливості текстів нормативно-правової бази міжнародних організацій та визначено, що правовий текст є одним з найбільш затребуваних, актуальних і складних сучасних текстів, головним концептом якого є право, а ключовою складовою — мова права. Правовий текст орієнтований на всі верстви суспільства і об'єднує велику кількість учасників: державу, представлену органами правосуддя, офіційними і правоохоронними органами, а також юридичні та фізичні особи: компанії, громадяни, які виступають у різних якостях. Визначено, що тексти нормативно-правового типу поєднують в собі риси двох функціональних стилів: офіційно-ділового та науково-технічного, який представлений термінологією різної тематики і способів функціонування.

Визначена семантична специфіка лексики документів Організації Об'єднаних Націй та Міжнародного союзу електрозв’язку. З’ясовано, що Резолюції ООН і МСЕ розглядають як частину дипломатичних текстів. Дипломатична мова має свої семантичні та стилістичні особливості. Дипломатичний текст є одним з видів інституціонального дискурсу. Загалом, дипломатична мова поєднує в собі риси відразу декількох елементів різних дискурсів, що передбачає міждисциплінарний характер дослідження.

Розглянуто особливості текстів резолюційного жанру. Визначено, що особливість нормативно-правового тексту в тому, що сукупності висловлювань, які знаходяться в різному часі, спрямовані на певну сферу суспільних відносин – правовідносин. Крім того, йому притаманний певний стиль, характер висловлювань, єдиний словник, що дозволяє формувати нормативно-правові тексти (юридична мова), дескриптивні висловлювання (акти). Будь-який нормативно-правовий текст формується і транслюється в рамках юридичної практики, і має певні особливості:

По-перше, оповідальна структура нормативно-правового тексту як і будь-якого іншого є предикативною. Оповідальна синтагма тексту нормативно-правового акта має імплікативний вид;

По-друге, оповідь нормативно-правового тексту підпорядковується вимогам правдивості, але ні в якому разі не правдоподібності. Так, нормативно-правове встановлення будь-якого нормативно-правового акта несе в собі завдання — введення певних правил поведінки, і при цьому у встановленні імпліцитно закладений критерій власної валідності реальним потребам держави і суспільства.

З’ясовано поняття, структуру і способи репрезентації концептів у сучасній лінгвістиці. Визначено, що основною категорією когнітивної лінгвістики є саме поняття «концепт», як об'єктивно існуюче у свідомості людини перцептивно-когнітивно-афективне утворення динамічного характеру на відміну від понять і значень як продуктів наукового опису.

Визначено особливості функціонування концепту «CYBERSECURITY» у текстах резолюційного жанру. Зазначено, що у сучасному інтерактивному суспільному житті все частіше мають місце такі негативні наслідки інформатизації, як: кібератаки, кібервійни, кіберексплуатація тощо, які у нормативних документах представлені такими лексикалізованими концептами, як: CYBERATTACK, CYBERWAR, CYBERESPIONAGE, CYBER-AGREEMENT, CYBER-THEFT, CYBERPIRACY, CYBERTHIEF, CYBERLAW, CYBERCRIME, CYBER-SABOTAGE, CYBERBULLYING, CYBERSECURITY тощо. Сьогодні у світі велика увага приділяється закріпленню концепту «CYBERSECURITY» на нормативно-правовому рівні у документах міжнародних організацій.

Розглянуті засоби вербалізації концепту «CYBERSECURITY». Визначено, що ключовими лексемами, що лежать в основі вербалізації аналізованої концептосфери в англійській мові, з'явилися CYBERSAFETY / CYBERSECURITY (кіберзахист, кібербезпека) в комбінаториці.

З’ясовані концептуальні зв'язки «CYBERSECURITY». Внаслідок різноманітності когнітивних установок, залучених у формування ментального образу концепту safety / security (безпека), можна стверджувати, що останній є компонентом структури концептосфери safety / security (безпека).

Визначено особливості лексичної сполучуваності. Зазначено, що інтернаціоналізація клонцептосфери кібербезпеки зумловлена, в першу чергу, глобальним характером явища, переважанням англомовної термінології через дію екстралінгвістичних чинників (глобалізаційні процеси, пріоритетність окремих держав в галузі наукових досліджень, наявність досвіду у сфері державного управління певними явищами, широке поширення як світової мови тощо). Зазначене пояснює причину вжитку різних лексикотематичних груп номінацій концепту «CYBERSECURITY» у сфері інформаційної безпеки, починаючи із самого елементу «кібер», який став дуже продуктивним у словотворенні.

Аналіз лексичних трансформацій у перекладі концепту «CYBERSECURITY» визначив, що у виконанні перекладу текстів подібного роду велике значення має перекладацька еквівалентність. Визначено, що основними прийомами перекладу концептів групи CYBERSECURITY є транслітерація, калькування та лексичні відповідники.

Розглянута специфіка лексико-граматичних трансформацій. Виявлено, що найпоширенішими лексико-граматичними трансформаціями у перекладі концепту CYBERSECURITY є заміни, модуляція, конкретизація, описовий переклад.

Таким чином, для успішного перекладу правозахисної лексики в ООН перекладачеві необхідно не тільки володіти великими загальними знаннями, розуміти особливості діяльності організації, бути в курсі актуальної інформації, але також і орієнтуватися у всіх супутніх тематиках - знати загальну термінологію ООН та інших міжнародних організацій, протокольну і процесуальну лексику.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Агаркова Н.Е. Понятие «деньги» как фрагмент англоязычной картины мира (по материалам американской версии английского языка): Дис. канд. филол. наук: 10.02. Иркутск: Иркут. гос. ун-та, 2001. 171 с.
2. Алефиренко Н.Ф. Проблемы вербализации понятия: теоретическое исследование. Волгоград: Смена, 2003. 112 с.
3. Алимов В. В. Теория перевода. Перевод в сфере профессиональной коммуникации : учебное пособие. Москва, 2004. 306 с.
4. Апресян Ю.Д. Образ человека по данным языка: попытка описания системы // Вопросы языкознания. Москва. 2010. № 1. С. 29 - 67.
5. Аскольдов С. А. Понятие и слово // Русская литература: от теории литературы к структуре текста: Антология. Москва: Гнозис, 1997. 269 с.
6. Бабушкин А. П. Типы понятий в лексико-фразеологической семантике языка: монография. Воронеж: Воронежский государственный университет. 2011. 330 с.
7. Бакулина С. С. Концептосфера права как фактор гуманизации культуры : автореф. ... дисс. канд. Культурологии. СПб. 2012. 23 с.
8. Барт Р. Эффективность реальности. Избранные работы: Семиотика: Поэтика. Москва: Прогресс, 2006. С. 392 - 400.
9. Безкоровайный М. М. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1(2). С. 22-27.
10. Болдырев Н. Н. Когнитивная семантика: курс лекций по английской филологии. Тамбов, 2002. 124 с.
11. Болотнова Н. С. Поэтическая картина мира и ее изучение в коммуникативном стиле текста // Сибирский филологический журнал. Новосибирск. 2003, № 3-4. С. 55-59.
12. Вайсбербер Л. Родной язык и формирование духа. Москва. 2008. 193 с.
13. Веденеев Ю.А. Юридическая картина мира: между должным и сущим // Lex Russica. 2014. № 6. С. 641-654.

14. Вежбицкая А. Метатекст в тексте: Новое в зарубежной лингвистике. Том 8. Текстовая лингвистика. Москва, 2009. С. 402–412. URL: http://destructioen.narod.ru/vegbicka_metatekst.htm
15. Верещагин Е.М. Об относительности мирской этической нормы // Логический анализ языка. Языки этики. Москва: Языки русской культуры, 2000. С. 235-245.
16. Виноградов В. В. Русский язык. Москва.: Высшая школа, 2002. 615с.
17. Воркачев С. Г. Лингвокультурная концепция: типология и регион существования: монография.Волгоград, Волга, 2007. 254 с.
18. Гак В.Г. Актантная структура грехов и добродетелей // Логический анализ языка. Языки этики. М.: Языки русской культуры, 2000. С. 90-96.
19. Гальперин И. Р. Текст как объект лингвистического исследования. Москва: Наука, 2003. 140 с.
20. Гармаш О. Л. Вербалізація англомовних техноцентричних лексикалізованих концептів, утворених за метакогнітивним механізмом афіксації // Наукові записки НДУ ім. М. Гоголя. Філологічні науки. 2016. Книга 1. С. 158-162.
21. Гончаров В. Концепт в контексте традиционной теории толкования смыслов // «Международный круглый стол». Львов: Край, 2012. С. 120-131.
22. Горшков А. И. Русский стиль. Москва: ООО "Издательство Астрель": ООО "Издательский дом АСТ", 2001. 367 с.
23. Гринев С.В. Введение в терминоведение. Москва, 2015. 406 с.
24. ГумбольдтВ. фон. Избранные труды по лингвистике. Москва: Прогресс, 1984. 397 с.
25. Деева Н.В. Концепт «Жизнь»: понятийная и символическая составляющие. Москва, 2017. С.24-29.
26. Деррида Ж. Эссе об имени. Москва: Ин-т эксперим. социологии; Спб.: Алетейя, 2012. 190 с.
27. Евтушок Ю. Г. Языковая репрезентация концепта CRIME: автореф. дисс. … канд. филол. наук. Иркутск, 2004. 15 с.

28. Ефремова М. П. Концепт threat (угроза) как объективатор концептосферы safety/security (безопасность) в английском языке // Грамота. 2018. № 1(79). Ч. 1. С. 104-108.
29. Залевская А. А. Психолингвистический подход к проблеме концепта // Методологические проблемы когнитивной лингвистики: учебное пособие. Воронеж: Изд-во Воронежского государственного университета, 2001. 398 с.
30. Залевская А. А. Концепт как собственность личности: монография. Москва: Слово, 2005. 244 с.
31. Змийова И.В. Лингвокогнитивные характеристики средств вербализации концепта ДОБРО в английском языке. Дис. канд. филол. наук. Харьков. 2006. 228 с.
32. Калюжная В. В. Стиль англоязычных документов Международных организаций. Киев: Наукова Думка, 2010. 113 с.
33. Карасик В. И. Языковые ключи: монография. Москва: Гнозис, 2009. 406 с.
34. Карасик В.И. Языковой круг: личность, концепт, дискурс.: монография. Волгоград: Смена, 2002. 477 с.
35. Колесов В.В. Язык и менталитет. СПб .: Петербургские востоковеды, 2004. 237 с.
36. Кошелев А. Д. О языковом концепте ДОЛГ // Логический анализ языка: Языки этики: учебное пособие. Москва, 2000 . 156 с.
37. Кравченко А.Б. Проблема языкового значения как проблема представления знаний // Когнитивные аспекты языкового значения: межвузовский. сб. науч. трудов. Иркутск: ИГЛУ, 2017. С. 3-16.
38. Красных В. В. «Свой» среди «чужаков»: миф или реальность?: монография. Москва.: ИТДГК Гносис, 2003. 375 с.
39. Кубрякова Е. С. Об установках когнитивной лингвистики и актуальных проблемах когнитивной лингвистики // Вопросы когнитивной лингвистики. 2004. № 1. С. 6-9.

40. Кубрякова Е. С. О современном понимании термина «концепт» в лингвистике и культурологии // Реальность, язык и сознание: межвузовский. сб науч. тр. Вып.2. Тамбов: Издательство ТГУ им. Г.Р.Державина, 2002. С. 3-12.
41. Лакофф Дж. Лингвистические гештальты: новое в зарубежной лингвистике. Москва: Прогресс, 1980. С. 87-155.
42. Лихачев, Д. С. Концептосфера русского языка. Москва: Изв. РАН – СКВ. 2006. № 1. 96 с.
43. Лыткина О. И. О типологии понятий в современной лингвистике. URL: http://cyberleninka.ru/article/n/k-voprosu-o-tipologii-kontseptov-v-sovremennoy-lingvistike
44. Лотман Ю. М. Культура и взрыв / Полуосфера. СПб, 2000 . 464 с.
45. Ляпин С.Х. Концептология: к формированию подхода // Концепции. Том И. Архангельск, 1997. 344 с.
46. Майоренко И. А. Концептуализация понятия «деньги» в лексической системе и фонде устойчивых единиц русского, английского и французского языков. Краснодар, 2005. 198 с.
47. МаксимовЛ. В. Об определениях добра: логико-методологический анализ // Логический анализ языка: Языки этики / под редакцией: Н. Д. Арутюнов, Т. Е. Янко, Н. Т. Рябцева. Москва: Языки русской культуры, 2000. 448 с.
48. Маслова В. А. Когнитивная лингвистика: учеб. Пособие. Минск: Тетрацы-стебли, 2005. 256 с.
49. Неретина С. С. Слово и текст в средневековой культуре. Концептуализм Абеляра: учебное пособие. Москва: Гнозис, 2008. 216 с.
50. Официальная документация ООН: обзор // Организация Объединенных Наций URL: http://research.un.org/ru/docs/resolutions
51. Пименова М. В. Душа и дух: особенности концептуализации: монография. Кемерово: IPC Graphics, 2004. 386 с.
52. Пименова М. В. Концепция сердца: образ, понятие, символ: монография. Кемерово: Кемеровский государственный университет, 2007. 500 с.

53. Попова З. Д., Стернин И. А. Понятие «концепт» в лингвистических исследованиях. Воронеж: Издательство Воронежского гос. университет, 2009. 30 с.
54. Прохоров Ю. Е. В поисках концепции: учебное пособие. Москва: Флинт, 2009. 176 с.
55. Самедова И. А. Функционально-стилистический анализ англоязычных текстов Резолюций Совета Безопасности ООН (на примере Резолюций 853, 874 и 884) // Филологические науки. Вопросы теории и практики. 2013. №4(22), Ч.2. С. 166–170.
56. Серебренников Б.А. Отражает ли язык реальность или выражает ее символически? Как отражается картина мира на языке? // Роль человеческого фактора в языке: язык и картина мира. Москва: Наука, 1988. 212с.
57. Сидоренков В. А. От слова - к изображению, от словаря - к литературному тексту // Слово и грамматические законы языка: глагол. Москва: Наука, 1989. 222 с.
58. Сыромятникова Н. В. Понятие концепта в когнитивной лингвистике. Белгород: Белгородский государственный национальный исследовательский университет. http: URL: //tp.uss.dvfu.ru/conferences/aktualnye-problemy - inoiazychnogo-obrazov / section1 / poniatie-koncepta-v-kognitivnoi-lingvist.html
59. Слышкин Г. Г. Лингвокультурные понятия и метаконцепции: учебное пособие. Волгоград: Смена. 2017. 206 с.
60. Степанов Ю. А. Концепции. Тонкая пленка цивилизации: монография. Москвва.: Изд-во ЛКИ, 2007. 248 с.
61. Телия В. Н. Русская фразеология. Семантический, прагматический и лингвокультурологический аспекты. Москва, 1996. 286 с.
62. Харитонов В. И. Концептуальный анализ народного словаря, характеризующего нравственный мир русского человека: Автореф. дис. канд. филол. наук. Белгород. 17с.
63. Хижняк С.П. Новое в исследовании терминологических систем (на примере юридической терминологии 2012. 377 с.

64. Филимонова О. Е. Язык эмоций в английском тексте. Когнитивный и коммуникативный аспекты. СПб.: Издательство Герценского государственного педагогического университета им. А. И. Герцена, 2001. С. 239-242.
65. Фрумкина Р. М. Психолингвистика: учебник. Москва: Академия, 2008. 320 с.
66. Фуко М. Археология знания. СПб. : Гуманитарная академия, 2012. 416 с.
67. Холодная М. А. Психология концептуального мышления: от концептуальных структур к концептуальным способностям: монография. Москва: Издательство "Институт психологии РАН", 2012. 288 с.
68. Чернейко Л. О. Лингвофилософский анализ абстрактного имени. 2-изд. Переработанное. Москва: ЛИБРОКОМ, 2010. 272 с.
69. Чесноков И. И. Эмоциональная концепция как объект культурной лингвистики // Наследие академика В. И. Борковского и проблемы современного языкознания: статьи, исследования, материалы. Волгоград: Издательство Волга, 2006. 236 с.
70. Шишка Р. Б. Концепт безпеки в сучасній правовій доктрині // Безпека як правовий концепт: виступи учасників Всеукраїнської науково-практичної конференції (Київ, 20 квітня 2018 р.). Київ: Видавництво Ліра-К. 2018. С. 43-46.
71. Catford J. A Linguistic Theory of Translation: an essay on Applied Linguistics. London: Oxford University Press, 1995. 103 p.

СПИСОК ДОВІДНИКОВИХ ДЖЕРЕЛ

72. Большой юридический энциклопедический словарь / под ред. А. Б. Барихина. Москва, 2004. 680 с.
73. Электронный Британский корпус английского языка. URL: www // natcorp.ox.as.uk
74. Электронный толковый словарь английского языка: URL: http: // engood. com

75. Караулов Ю. Н. Русский ассоциативный словарь: URL: http: // tesaurus .ru / dict / dict.php
76. Пименов М. В. Методология концептуального исследования // Антология понятий: словарь / под ред. В.И. Карасик и И.А. Стернина. Москва: Гнозис, 2007.С. 14-16.
77. Русско-американский словарь терминов и определений в сфере информационной безопасности. URL: https://digital.report/cybersecurity-terminology/
78. Степанов Ю. С. Концепты. Словарь русской культуры. Исследовательский опыт. Москва, 1997. 216 с.
79. Языковая картина мира. URL: en.wikipedia.org/wiki/Language
80. Ярцева В. Н. Лингвистический энциклопедический словарь. URL: http: //tapemark.narod.ru/les/
81. English-Russian Comprehensive Law Dictionary / под ред. А. С. Мамуляна. Москва, 2003. 688 с.
82. Longman Dictionary of English Language and Culture. England, 2005. 688 p.

СПИСОК ІЛЮСТРАТИВНИХ ДЖЕРЕЛ

83. Congressional Bills 113th Congress [From the U.S. Government Publishing Office] [S. 2521 Introduced in Senate (IS)]
URL: https://www.govinfo.gov/content/pkg/BILLS113s2521is/html/BILLS113s2521is.html
84. Convention on cybercrime, opening of the treaty: Budapest, 23/11/2001. URL: https://www.coe.int/en/web/cybercrime/the-budapestconvention.
85. Cyber Security Research and Development Act Pub. L. 107-305, Nov. 27, 2002.
86. Federal Information Security Modernization Act of 2014 (Public Law 113-283; December 18, 2014).
URL: https://www.govinfo.gov/content/pkg/PLAW113publ283/html/PLAW-113publ283.html
87. Information technology. Security techniques. Guidelines for cybersecurity. URL: https://www.iso.org/standard/44375.html

88. ITU: Committed to connecting the world. URL: https://www.itu.int/en/Pages/default.aspx
89. Tsakanyan V.T. (2017). The role of cybersecurity in world politics. Vestnik RUDN. International Relations, 17(2), 339-348.
90. 2018 Cybercrime Report Europe Deepdive. URL: https://www.threatmetrix.com/info/2018-cybercrime-europe/
91. Understanding Cybercraime: A Guaide for Developing Counries. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CybcrimeE.pdf.
92. White House Cyberspace Policy Review, May 2009 // U.S. Department of Homeland Security.
URL: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf.

ДОДАТКИ

Додаток А

Словник термінів, що наповнюють концептосферу «CYBERSECURITY»

English term	Term definition	Commentary
Cyber Entity	— any distinct thing or actor that exists within the cyber infrastructure	A thing can be a person, network, etc. Known definitions were consulted during this process
Cyberspace	is an electronic medium through which information is created, transmitted, received, stored, processed and deleted.	Cyber has roots in the Greek word κυβερνητικός G meaning skilled in steering or governing. The term "cybernetics" is widely recognized as being coined in the book Cybernetics or Control and Communication in the Animal and the Machine (MIT Press, 1948). The author, Norbert Wiener, applied the term in the context of the control of complex systems in the animal world and in mechanical networks. The term would later be used in the medical community in reference to the integration of humans or animals with machinery. However, since cyber has been introduced it has taken on several meanings. The term is used effectively in business, law and policy. The term currently has highly useful application in that it can readily provide a reference to the other than physical, virtual world created by the Internet and other electronic communications. On the other hand, cyberspace does not exist without the physical ingredients from which it is composed. The compound word s inclusion of the word "space" implies that it should have dimension. That is, cyberspace must occupy an expanse. In addition, cyberspace is considered by some as a new domain like land, sea, air and space. However, as these four are natural, cyber is artificial, being created by man.

		Known definitions were consulted during this process. The U.S. Department of Defense has a documented definition as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." See Dictionary of Military and Associated Terms, U.S. Department of Defense, 31 January 2011, 92G93. (CJCS CMG0363G08)
Cyber Crime	is the use of cyberspace for criminal purposes as defined by national or international law.	Important considerations for this term include the following: Given the established laws that define criminal activity, the cyber crime term is deliberately designed to immediately reference existing legal structures. It is understood that jurisdictional considerations have an integral role in application of this term. Complexities arise when activities are performed by an individual in one country, utilizing cyber resources in another (second) country, and affecting someone, organization or other entity in the third country. Cyber criminals are increasingly being categorized as significant non state actors. The Convention on Cybercrime (2001) is the first international treaty seeking to harmonize cyber crime legislations across countries. It was drawn up by the Council of Europe with the United States participating as an observer. The U.S. has ratified the treaty, whereas Russia has not. Known definitions were consulted during this process.
Cyber Conflict	is a tense situation between and/or among nation-states and/or organized groups	where unwelcome cyber attacks result in retaliation. Important considerations for this term include the following: Cyber attacks could include physical attacks on cyber infrastructure.

		The attack retaliation methods may be asymmetrical (i.e. cyber, physical). Thus the response does not have to be cyber. Nor does the attack need to be cyber in order to have a cyber response. Cyber conflict can be a precursor to an escalated situation. Known definitions were consulted during this process.
Cybersecurity	is a property of cyberspace that is an ability to resist intentional and/or unintentional threats and respond and recover.	Important considerations are included in the "Discussion Disagreements: Information and Cyber" discussion presented in Section 1. The Russian word for "security" connotes protection. No additional meanings, such as the means to provide this protection, are implied by the Russian word for "security," whereas the English term "security" includes such means. Known definitions were consulted during this process. Of interest is research that underscores the original concept of being secure is most oriented around a sense of being safe.
Cyber Operation	organized activities in cyberspace to gather, prepare, disseminate, restrict or process information to achieve a goal.	Known definitions were consulted during this process.
Cyber	is organized capabilities to protect against, mitigate from and rapidly recover from the effects of cyber attack.	Important considerations for this term include the following: Cyber defense refers to actions taken by a party to protect its interests in anticipation of an attack. The inclusion of this term in this initial taxonomy related to defense is important because it helps explain the legitimate interest of nation states to invest in the development of capabilities that may be needed to protect their interests. Effective defense in electronic systems is typically based on detection, isolation, reporting, recovery and neutralization.

		The ability to absorb an attack may be an effective defensive strategy. An attack is only effective if it exercises an intrinsic vulnerability. Known definitions were consulted during this process.
Information Security	is property of information space that is an ability to resist threats and respond and frecover.	This also applies to all of its subspaces as well. Known definitions were consulted during this process.
Cyber Weapon	software, firmware or hardware designed or applied to cause damage through the cyber domain.	Consequential harm can be caused to the physical domain as well. Also see the quad chart of physical and cyber attributes (see page 13). Known definitions were consulted during this process.
Cyber Vulnerability	property of a cyber entity that is susceptible to exploitation.	Cyber intelligence can be military, political, economic, industrial, environmental, diplomatic, etc. Known definitions were consulted during this process.

Додаток Б

Способи перекладу концептосфери «CYBERSECURITY»

№з/п	Приклад	Переклад	Спосіб перекладу
1.	(1) on behalf and instructions [91].	від імені та за дорученням;	Калькування
2.	(2)I beg to inform you[91].	маю честь повідомити	Калькування

3.	(3) the ambassador presents his compliments [91].	Посол висловлює свою повагу	Калькування
4.	4)international understanding [91].	міжнародне взаєморозуміння;	Калькування
5.	(5)strict observance of the resolutions	суворе дотримання резолюцій	Калькування
6.	(6)International Mother Language Day [91].	Міжнародний День Рідної Мови	Калькування
7.	(7) on an equitable basis [91].	на справедливій основі	Калькування
8.	(8) Coordinator for Multilingualism [91].	координатор з питань багатомовності	Калькування
9.	(9) linguistic diversity [91].	лінгвістичне розмаїття	Калькування
10.	(10) United Nations (UN) [91].	Організація Об'єднаних Націй (ООН)	Калькування + транслітерація
11.	(11) Security Council (SC) [91].	Рада Безпеки (РБ)	Калькування
12.	(12) General Assembly (GA) [91].	Генеральна Асамблея	Калькування
13.	(13)status quo [91].	статус-кво	Калькування
14.	(14)veto [91].	право вето	Калькування
15.	(15)Secretariat [91].	Секретаріат	Транслітерація
16.	(16)international peace and security [91].	міжнародний мир і безпека	Калькування
17.	(17) human rights [91].	права людини,	Калькування
18.	(18)official languages / non-official languages [91].	офіційні мови / неофіційні мови	Калькування
19.	(19)working languages [91].	робочі мови	Калькування

20.	(20) headquarter [91].	штаб-квартира	Калькування
21.	(21) member states [91].	держави-члени	Калькування
22.	(22) recognizing	визнаючи	Калькування
23.	(23) stressing	підкреслюючи	Калькування
24.	(24) recalling	нагадуючи	Калькування
25.	(25) emphasizing	особливо відзначаючи	Калькування
26.	(26) reaffirming	підтверджуючи	Калькування
27.	(27) notes;	зазначає	Калькування
28.	(28) affirms;	підтверджує	Калькування
29.	(29) calls upon;	закликає	Калькування
30.	(30) underlines;	підкреслює	Калькування
31.	(31) welcomes	вітає	Калькування
32.	(32) - endorses	стверджує	Калькування
33.	(33) ncourages	рекомендує	Калькування
34.	(34) requests;	просить	Калькування
35.	(35) recalls;	посилається	Калькування
36.	(36) urges [72, с.297].	настійно рекомендує	Калькування
37.	(37) «The General Assembly, Noting the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information,	— «Генеральна Асамблея, відзначаючи зростаючу залежність урядів, підприємств, інших організацій та окремих користувачів від інформаційних технологій для надання основних товарів та послуг, ведення бізнесу та обміну інформацією, визнаючи необхідність кібербезпеки зростає у міру збільшення участі країн в	Калькування

	Recognizing that the need for cybersecurity increases as countries increase their participation in the information society, Noting also the work of relevant international and regional organizations on enhancing cybersecurity and the security of information technologies; 1. Takes note of the elements annexed to the present resolution, with a view to creating a global culture of cybersecurity; 2. Invites all relevant international organizations to consider, inter alia, these elements for the creation of such a culture in any future work on cybersecurity; 3. Invites Member States to take into account these elements, inter alia, in their efforts to develop throughout their societies a culture of cybersecurity in the application and use of information technologies; 4. Invites Member States and all relevant international organizations to take, inter alia, these elements and the need for a global	інформаційному суспільстві, відзначаючи також роботу відповідних міжнародних та регіональних організацій щодо підвищення кібербезпеки та безпеки інформаційних технологій; 1. бере до уваги елементи, додані до цієї резолюції, з метою створення глобальної культури кібербезпеки; 2. Запрошує усі відповідні міжнародні організації, зокрема, розглянути ці елементи для створення такої культури в будь-якій майбутній роботі з кібербезпеки; 3. Запрошує держави-члени взяти до уваги ці елементи, зокрема, у своїх зусиллях розвивати в своїх суспільствах культуру кібербезпеки при застосуванні та використанні інформаційних технологій; 4. Запрошує держави-члени та всі відповідні міжнародні організації, зокрема, врахувати ці елементи та необхідність глобальної культури кібербезпеки під час підготовки до Всесвітнього саміту з питань інформаційного суспільства, який відбудеться в Женеві з 10 до 12 Грудень 2003 р. І в Тунісі 2005 р .; 5. наголошує на необхідності сприяти передачі інформаційних технологій та розбудові потенціалу країнам, що	

	culture of cybersecurity into account in their preparations for the World Summit on the Information Society, to be held at Geneva from 10 to 12 December 2003 and at Tunis in 2005; 5. Stresses the necessity to facilitate the transfer of information technology and capacity-building to developing countries, in order to help them to take measures in cybersecurity» [85].	розвиваються, щоб допомогти їм вжити заходів щодо кібербезпеки»[85].	
38.	(38) «Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets [88].	— «Кібербезпека — це сукупність інструментів, політик, концепцій безпеки, гарантій безпеки, керівних принципів, підходів до управління ризиками, дій, тренінгів, найкращих практик, гарантій та технологій, які можуть бути використані для захисту кіберсередовища та організації та активів користувача [88].	Калькування_ транслітерація
39.	(39) «Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment	«До активів організації та користувачів належать підключені обчислювальні пристрої, персонал, інфраструктура, додатки, послуги, телекомунікаційні системи та сукупність переданої та / або збереженої інформації в кіберсередовищі. Кібербезпека прагне забезпечити досягнення та підтримку властивостей безпеки організації та	Калькування

	and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment» [88].	активів користувача проти відповідних ризиків безпеки в кіберсередовищі»[88].	
40.	(40) General Assembly	Генеральна Асамблея	Транслітерація
41.	(41) multilingualism	багатомовність	Калькування
42.	(42) United Nations	Організація Об'єднаних Націй	Калькування+ транслітерація
43.	(43) SecretaryGeneral	Генеральний Секретар.	Транслітерація
44.	44) Core value	головна цінність / ключова цінність / основна цінність;	Калькування
45.	(45) Comprehensive report	всеосяжна доповідь / комплексна доповідь / вичерпна доповідь	Калькування
46.	(46)... protecting and preserving diversity of languages and cultures globally ... [3, с.68].	... захисту і збереження мов і культур в глобальному масштабі ... [3, с.68].	Калькування+ транслітерація
47.	(47) Recognizing the contribution of multilingualism in promoting international peace and security, development and human rights, through the work of the United Nations departments and offices. [3, с.69].	Визнаючи внесок, який багатомовність вносить, завдяки роботі департаментів і управлінь Організації Об'єднаних Націй, в забезпечення міжнародного миру і безпеки, розвитку і дотримання прав людини. [3, с.68].	Калькування
48.	(48) «Concerned about the continued promulgation and application by Member	«Будучи стурбованими тривалим прийняттям і застосуванням державами-членами законів	Калькування+ транслітерація

	States of laws and regulations, such as that promulgated on 12 March 1996 known as" the Helms-Burton Act ", the extraterritorial effects of which affect the sovereignty of other States, their **cybersecurity**, the legitimate interests of entities or persons under their jurisdiction and the freedom of trade and navigation» [83, с.8].	і положень, таких як прийнятий 12 березня 1996 року Закон, відомий як« закон Хелмса-Бертона », екстериторіальні наслідки яких зачіпають суверенітет інших держав, їх **кібербезпеку**, законні інтереси юридичних чи фізичних осіб, які підпадають під їх юрисдикцію, а також свободу торгівлі і судноплавства» [50, с.16].	
49.	(49) «We will also undertake appropriate measures for access to justice and protections for victims in criminal justice processes, including measures to ensure that identified victims are not penalized for having been trafficked and that they do not suffer from victimization as a result of actions taken by Government authorities, **cyberterrorists»** [83, с.12].	«Будемо також вживати належних заходів для того, щоб жертви отримували доступ до правосуддя і були захищені в ході кримінального судочинства, в тому числі заходи, покликані не допустити, щоб виявлені жертви каралися за те, що стали об'єктами такої торгівлі, і не піддавалися віктимізації внаслідок дій державної влади та **кібертерористів»** [50, с.14]**.**	Транслітерація
50.	(50) «Requirements for reporting security incidents to the Federal **information security** incident center established under section 3556» [83, с.17];	«Вимоги щодо повідомлення інцидентів безпеки у Федеральному центрі інцидентів **інформаційної безпеки**, створеному відповідно до розділу 3556» [50, с.18].	Калькування+ транслітерація

51.	(51) «Recognising the need for co-operation between States and private industry in combating **cybercrime** and the need to protect legitimate interests in the use and development of information technologies» [84, c.7];	«Визнаючи необхідність співпраці між державами та приватною промисловістю у боротьбі з **кіберзлочинністю** та необхідність захисту законних інтересів у використанні та розвитку інформаційних технологій» [50, с.10].	Калькування+ транслітерація
52.	(52) **«Cybersecurity** research and development act. Section 8(d)(1) of the Cybersecurity Research and Development Act (15 U.S.C. 7406) is amended by striking «section 35342 and inserting «section 3554» [88, c.6].	«Акт досліджень і розробок **кібербезпеки.** Розділ 8 (d) (1) Закону про дослідження та розвиток кібербезпеки (15 США 7406) доповнено виправленням "розділу 35342 та вставкою" розділу 3554». [50, с.9].	Калькування+ транслітерація
53.	(53) «Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against **cybercrime**, inter alia, by adopting appropriate legislation and fostering international co-operation» [84, c.17].	«Переконаний у необхідності в першочерговому порядку проводити спільну кримінальну політику, спрямовану на захист суспільства від **кіберзлочинності,** зокрема, шляхом прийняття відповідного законодавства та сприяння міжнародному співробітництву» [50, с.20].	Калькування+ транслітерація
54.	(54) «This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use,	«Ця стаття не повинна тлумачитися як накладення кримінальної відповідальності, коли виробництво, продаж, закупівля для використання,	Калькування+ транслітерація

	import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or **protection of a computer system»** [84, с.7].	ввезення, розповсюдження чи іншим наданням у розпорядження чи володіння, зазначеним у пункті 1 цієї статті, не є метою вчинення злочину, встановленого відповідно до зі статтями 2 - 5 цієї Конвенції, наприклад, щодо дозволеного тестування або **захисту комп'ютерної системи** » [50, с.20].	
55.	(55) «Protection of Information. Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect **information security.** Such protections shall be commensurate with the risk and comply with all applicable laws and regulations »[83, с.6].	«Захист інформації. Агентства та оцінювачі вживають відповідних заходів для забезпечення захисту інформації, яка, якщо буде розкрита, може негативно вплинути на інформаційну безпеку. Такі засоби захисту повинні відповідати ризику та відповідати усім чинним законам та нормам » [50, с.10].	Калькування+ транслітерація
56.	(56) «**Cybersecurity** is organized capabilities to protect against, mitigate from and rapidly recover from the effects of cyber attack» [83, с.7].	«**Кібербезпека** - це організована спроможність захищати від наслідків кібератаки та швидко їх відновлювати» [50, с.9].	Калькування + транслітерація
57.	(57) «**Cyber Defense** is a computer network defense mechanism which includes response to	**«Кіберзахист** - це механізм захисту комп'ютерної мережі, який включає реагування на дії та захист критичної	Калькування + транслітерація

	actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks» [83, с.12].	інфраструктури та забезпечення інформації для організацій, державних структур та інших можливих мереж» [50, с.15].	
58.	(58) «3559. Privacy breach requirements» (a) Policies and Procedures.--The Director, in consultation with the Secretary, shall establish and oversee policies and procedures for agencies to follow in the event of a breach of **information security** involving the disclosure of personally identifiable information, including requirements for…» [83, с.11].	«3559. Вимоги щодо порушення конфіденційності»(a) Політика та процедури. - Директор, консультуючись із Секретарем, встановлює та контролює політику та процедури, якими слід скерувати агенції у разі порушення **інформаційної безпеки**, що передбачає розкриття особистої ідентифікації. інформація, включаючи вимоги щодо… » [50, с.13].	Калькування + транслітерація
59.	(59) «The term `**information security**' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide» [83, с.11]	"Термін" **інформаційна безпека** "означає захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, зриву, модифікації чи знищення з метою надання" [50, с.14].	Калькування + транслітерація
60.	(60) «Perating the Federal **information security** incident center established under section 3556». [83, с.20].	«Перевірка Федерального центру інцидентів **інформаційної безпеки,** створеного відповідно до розділу 3556»; [50, с.21].	Калькування + транслітерація

61.	(61) «Provide, as appropriate, intelligence and other information about **cyber threats**, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b)» [83, с.16].	«Зробити, відповідно, розвідувальну та іншу інформацію щодо **кіберзагрози**, вразливості та інцидентів для агентств для надання допомоги в оцінках ризику, проведених відповідно до розділу 3554 (b)» [50, с.20].	Калькування
62.	(62) «…ensuring **information security** management processes are integrated with agency strategic and operational planning processes» [83, с.8].	«… забезпечення інтеграції процесів **управління інформаційною безпекою** з процесами стратегічного та оперативного планування агентства» [50, с.10].	Калькування + транслітерація
63.	(63) «…provide a comprehensive framework for ensuring the effectiveness of **information security controls** over information resources that support Federal operations and assets» [83, с.5].	«…забезпечити комплексну основу для забезпечення ефективності **контролю інформаційної безпеки** інформаційних ресурсів, що підтримують федеральні операції та активи» [50, с.7].	Калькування + транслітерація
64.	(64) Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of **computer systems, networks and computer data** as well as the misuse of such systems, networks and data by providing for the criminalisation of such	«Переконаний, що ця Конвенція необхідна для стримування дій, спрямованих на конфіденційність, цілісність та **доступність комп'ютерних систем, мереж та комп'ютерних даних**, а також на неправильне використання таких систем, мереж та даних шляхом забезпечення криміналізації такої поведінки, як описано в цій	Транслітерація і калькування

	conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation [84, с.7].	Конвенції, та прийняття повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями, шляхом сприяння їх виявленню, розслідуванню та кримінальному переслідуванню як на внутрішньому, так і на міжнародному рівнях, а також шляхом забезпечення швидкого та надійного міжнародного співробітництва [50, с.22].	
65.	(65) «…provide a mechanism for improved oversight of Federal agency **information security** programs» [83, с.3].	«… забезпечити механізм удосконалення контролю за програмами **інформаційної безпеки** Федерального агентства» [50, с.5].	Транслітерація і калькування
66.	(66) «…recognize that the selection of specific technical hardware and software **information security** solutions should be left to individual agencies from among commercially developed products [83, с.4].	«…визнають, що вибір конкретних технічних апаратних та програмних рішень щодо **захисту інформації** повинен залишатися окремим агенціям з числа комерційно розроблених продуктів [50, с.5].	Транслітерація і калькування
67.	(67) «coordinating Government-wide efforts on **information security** policies and practices, including consultation with the	«координація зусиль уряду щодо політики та практики **інформаційної безпеки,** включаючи консультації з Радою головних інформаційних служб, створеною	Транслітерація і калькування

	Chief Information Officers Council established under section 3603 [83, c.3].	відповідно до розділу 3603 [50, с.6].	
68.	(68) «The term **`national security system'** means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency-- ``(i) the function, operation, or use of which-- ``(I) involves intelligence activities; ``(II) involves cryptologic activities related to national security; ``(III) involves command and control of military forces; ``(IV) involves equipment that is an integral part of a weapon or weapons system; or ``(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or ``(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of **national**	«Термін **«система національної безпеки»** "означає будь-яку інформаційну систему (включаючи будь-яку телекомунікаційну систему), що використовується або керується агентством або підрядником агентства або іншою організацією від імені агентства--` `(i) функція, функціонування або використання яких-- `` (I) передбачає розвідувальні дії; `` (II) передбачає криптологічні дії, пов'язані з національною безпекою; `` (III) передбачає командування та контроль військових сил; `` (IV) передбачає обладнання, яке є невід'ємною частиною зброї або системи озброєння; або `` (V), що підпадає під підпункт (B), має вирішальне значення для безпосереднього виконання військових або розвідувальних місій; або `(ii) захищений у будь-який час процедурами, встановленими для інформації, спеціально дозволеної відповідно до критеріїв, встановлених Виконавчим розпорядженням або Актом Конгресу, що класифікуються в інтересах	Транслітерація і калькування

	defense or foreign policy» [83, с.2].	**національної оборони** чи зовнішньої політики" [50, с.20].	
69.	(69) «A Party may require that the offence be committed by **infringing security measures**, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system» [84, с.7].	«Сторона може вимагати, що правопорушення було вчинено із **порушенням заходів безпеки**, з наміром отримати комп'ютерні дані чи інший нечесний намір, або стосовно комп'ютерної системи, підключеної до іншої комп'ютерної системи» [50, с.23].	Калькування
70.	(70) «Where the requested Party believes that preservation will not ensure the future availability of the data or will **threaten the confidentiality** of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed» [84, с.8].	«Якщо запитувана Сторона вважає, що охорона не забезпечить майбутню доступність даних або загрожує конфіденційності або іншим чином завдасть шкоди розслідуванню запитуючої Сторони, вона негайно повідомляє про це Сторону, яка запитує, яка визначає, чи буде запит виконано» [50, с.23].	Транслітерація і калькування
71.	(71) «Concerned by the risk that **computer networks and electronic information may also be used for committing criminal offences** and that evidence relating to such offences may be stored and transferred	«Стурбований ризиком того, що **комп'ютерні мережі та електронна інформація також можуть використовуватися для вчинення кримінальних злочинів,** і що ці мережі можуть зберігати та передавати ці мережі» [50, с.23].	Транслітерація і калькування

	by these networks» [84, с.7].		
72.	(72) «One important requirement of an efficient education and information strategy is open communication of the **latest cybercrime threats**. Some states and/or private businesses refuse to emphasize that citizens and clients respectively are affected by **cybercrime threats**, in order to avoid them losing trust in online communication services. The United States Federal Bureau of Investigation has explicitly asked companies to overcome their aversion to negative publicity and report **cybercrime**. In order to determine threat levels, as well as to inform users, it is vital to improve the collection and publication of relevant information» [91, с.4].	«Однією з важливих вимог ефективної освітньої та інформаційної стратегії є відкрите повідомлення про новітні **загрози кіберзлочинності.** Деякі держави та / або приватний бізнес відмовляються підкреслювати, що громадяни та клієнти відповідно зазнають **загрози кіберзлочинності**, щоб уникнути втрати довіри до Інтернет-служб зв'язку. Федеральне бюро розслідувань США чітко просило компанії подолати свою неприязнь до негативної реклами та повідомити про **кіберзлочинність.** Для визначення **рівнів загрози**, а також для інформування користувачів важливо вдосконалити збір та публікацію відповідної інформації » [50, с.25].	Транслітерація і калькування
73.	(73) **«Intellectual property** – creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights,	**«Інтелектуальна власність** - такі твори, як музичні, літературні та художні твори; винаходи; і символи, імена, зображення та конструкції, що використовуються в комерції, включаючи авторські права, торгові марки, патенти та суміжні	Транслітерація і калькування

	trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract “properties” has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered» [85, c.2].	права. Відповідно до законодавства щодо інтелектуальної власності, власник однієї з цих абстрактних «властивостей» має певні ексклюзивні права на твір, комерційний символ чи винахід, якими він охоплюється » [50, с.12].	
74.	(74) «criminal activity where services or applications in the **Cyberspace** are used for or are the target of a crime, or where the **Cyberspace** is the source, tool, target, or place of a crime» [87, c.2].	«злочинна діяльність, коли послуги чи програми в **Кіберпросторі** використовуються для/ або є об’єктом злочину, або де **Кіберпростір** є джерелом, інструментом, ціллю або місцем злочину» [50, с.10].	Транслітерація і калькування
75.	(75) $ 500 million to provide "**cybecsecurity assistance"**	500 мільйонів доларів на **забезпечення кібербезпеки.**	Транслітерація і калькування
76.	(76) «Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the **cyber environment**. **Cybersecurity** strives to ensure the attainment and maintenance of the security properties of the organization and	«До активів організації та користувачів належать підключені обчислювальні пристрої, персонал, інфраструктура, додатки, послуги, телекомунікаційні системи та сукупність переданої інформації в **кібер-середовищі.** **Кібербезпека** прагне забезпечити досягнення та підтримку властивостей безпеки організації та активів користувача проти відповідних ризиків безпеки в **кібер-середовищі**» [50, с.24].	Транслітерація і калькування

	user's assets against relevant security risks in the **cyber environment**» [88, c.3].		
77.	(77) The term **"cybercrime**" is used to cover a wide variety of criminal conduct. As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime. [91].	Термін **"кіберзлочинність**" використовується для охоплення найрізноманітніших злочинних дій. Оскільки визнані злочини включають широкий спектр різних злочинів, складно розробити типологію або систему класифікації кіберзлочинності. [50, с.24]	Транслітерація і калькування
78.	(78) «...for Developing Counries» термін identity theft interpreted as **«the fraudulent practice of using another person's** name and personal information in order to obtain credit, loans, etc.» [91, с.3].	«…для країн, що розвиваються термін «**крадіжки особистих даних»** трактується як« шахрайська практика використання імені та особистої інформації іншої особи для отримання кредиту, позики тощо». [50, с.24].	Калькування
79.	(79) «In addition, some terms that are used to describe criminal acts (such as "**cyberterrorism**" or "**phishing**") cover acts that fall within several categories. Nonetheless, the four categories can serve as a useful basis for discussing the phenomena of **cybercrime»** [91, с.3].	«Крім того, деякі терміни, які використовуються для опису злочинних діянь (наприклад, «**кібертероризм**» чи «**фішинг**»), охоплюють діяння, що належать до кількох категорій. Тим не менше, чотири категорії можуть слугувати корисною основою для обговорення явищ **кіберзлочинності**» [50, с.24].	Транслітерація і калькування
80.	(80) "Organizational structures" focuses on	"Організаційні структури" зосереджуються на запобіганні, виявленні,	Калькування

	the prevention, detection, response to and crisis management of **cyberattacks,** including the protection of critical information infrastructure systems» [91, с.4].	реагуванні на **кібератаки** та протидії кризам, включаючи захист критичних систем інформаційної інфраструктури " [50, с.25].	
81.	(81) «**Cyberspace attack** – cyberspace actions that create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains» [85, с.3].	«**Атака на кіберпростір** - дії на кіберпростір, які створюють різні ефекти прямого заперечення (тобто деградація, зрив чи руйнування) та маніпуляції, що призводять до приховування, того, що є прихованим або проявляється у фізичних царинах» [50, с.11].	Транслітерація і калькування
82.	(82) «The General Assembly, Noting the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information, Recognizing that the need for **cybersecurity** increases as countries increase their participation in the information society, Noting also the work of relevant international	«Генеральна Асамблея, відзначаючи зростаючу залежність урядів, підприємств, інших організацій та окремих користувачів від інформаційних технологій для надання основних товарів і послуг, ведення бізнесу та обміну інформацією, визнаючи необхідність зростання **кібербезпеки**, оскільки країни збільшують свою участь у інформаційному суспільстві, відзначаючи також роботу відповідних міжнародних та регіональних організацій щодо підвищення **кібербезпеки та безпеки інформаційних технологій**. [50, с.18].	Транслітерація і калькування

	and regional organizations on enhancing **cybersecurity and the security of information technologies.** [88, c.2].		
83.	(82) «The General Assembly, Noting the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information, Recognizing that the need for **cybersecurity** increases as countries increase their participation in the information society, Noting also the work of relevant international and regional organizations on enhancing **cybersecurity and the security of information technologies.** [88, c.2].	«Генеральна Асамблея, відзначаючи зростаючу залежність урядів, підприємств, інших організацій та окремих користувачів від інформаційних технологій для надання основних товарів і послуг, ведення бізнесу та обміну інформацією, визнаючи необхідність зростання **кібербезпеки**, оскільки країни збільшують свою участь у інформаційному суспільстві, відзначаючи також роботу відповідних міжнародних та регіональних організацій щодо підвищення **кібербезпеки та безпеки інформаційних технологій**. [50, с.18].	
84.	(84)... this requires protection and conservation on a global scale from **cyber espionage ...** [87, c.2].	.. це вимагає захисту і збереження в глобальному масштабі від **інформаційного шпіонажу ...** [50, с.2].	Граматична заміна
85.	(85) …recognizing also that	…визнаючи також, що Організація Об'єднаних	Граматична заміна

	the United Nations has recognized criminal negligence in the **cyberspace…** [92, с.2].	Націй визнала злочинну недбалість **у сфері інформаційної безпеки….** [50, с.18].	
86.	(86)... encourages the Secretary General to continue his efforts towards ending the **Internet warfare.** [87, с.2].	.. рекомендує Генеральному секретарю продовжувати докладати зусилля в напрямку **припинення війни в інформаційному просторі.** [50, с.2].	Граматична заміна
87.	(87) «According to the president, the United States sought de-escalation in Syria. He noted that the actions of the "criminal" regime of Assad, including the use of chemical weapons, shocked the world. It is for these reasons that the United States attacked the Syrian air base, causing destruction, casualties and new **cyber threats».** [87, с.2].	«За словами президента, Сполучені Штати прагнули до деескалації в Сирії. Він зазначив, що дії «злочинного» режиму Асада, в тому числі використання ним хімічної зброї, потрясли світ. Саме з цих причин Сполучені Штати здійснили напад на сирійську авіабазу, що спричинило руйнації, жертви та **нові загрози в інформаційному світі».** [50, с.2].	Граматична заміна
88.	(88) «Recalling that the United Nations Millennium Declaration includes a call for adherence to the "Olympic Truce" and tolerance on the **cyber environment** now and in the future and to support the International Olympic Committee in its efforts to promote peace and understanding between people through sport	«Нагадуючи про те, що в Декларацію тисячоліття Організації Об'єднаних Націй включений заклик дотримуватися «олімпійського перемир'я» та **толерантності на теренах інтернету** наразі і в майбутньому і підтримувати Міжнародний олімпійський комітет в його зусиллях щодо заохочення миру і взаєморозуміння між	Граматична заміна

	and the embodiment of Olympic ideals. " [90, с.3].	людьми за допомогою спорту та втілення олімпійських ідеалів». [50, с.13].	
89.	(89) «Taking note of declarations and resolutions of different intergovernmental forums, bodies and Governments that express the rejection by the international community and public opinion of the promulgation and application of measures of the kind referred to above on **cybersecurity».** [87, с.3].	«Беручи до уваги заяви і резолюції різних міжурядових форумів, органів і урядів, в яких виражається незгода міжнародної спільноти та громадськості з прийняттям і застосуванням заходів, подібних вищезазначеним щодо **кібернетичної безпеки».** [50, с.3].	Модуляція значення
90.	(90) «Request the Conference on Disarmament to commence negotiations on the item “Prevention of nuclear war” of its agenda and to consider, inter alia the elaboration of an international instrument of a legally binding character laying down the obligation not to be the first to use nuclear weapons and **information security issues».** [87, с.3].	«Просить Конференцію із роззброєння розпочати переговори по пункту її порядку денного« Запобігання ядерної війни »і розглянути, зокрема розробку міжнародного документа юридично обов'язкового характеру, в якому було б сформульовано зобов'язання не застосовувати першим ядерну зброю і питання **кібербезпеки».** [50, с.3].	Модуляція значення
91.	(91) «In documents of the International Telecommunication Union under **Cyberspace**, means “an	«У документах Міжнародного союзу електрозв'язку під **кіберпростором**, розуміється «середовище з підключеними	Калькування та транслітерація

	environment with connected computer devices,users, infrastructure, applications, services, telecommunication systems, as well as the totality of transmittedand / or information stored in this environment». [83, c.2].	комп'ютерними пристроями,користувачами, інфраструктурою, додатками, сервісами, телекомунікаційними системами, а також сукупність переданої або збереженої в цьому середовищі інформації». [50, с.9].	
92.	(92)... recommends that the Secretary-General continue his efforts in the field **of information and communication security…** [89, c.2].	. .. рекомендує Генеральному секретарю продовжувати докладати зусилля в напрямку **безпеки у царині інформаційно-комунікаційних технологій…** [50, с.12].	Додавання
93.	(93) Recognizing the contribution of multilingualism in promoting international peace and **security,** development and human rights, through the work of the United Nations departments and offices. [87, c.3].	Визнаючи внесок, який багатомовність вносить, завдяки роботі департаментів і управлінь Організації Об'єднаних Націй, в забезпечення міжнародного миру і **безпеки**, розвитку і дотримання прав людини. [50, с.3].	
94.	(94) US Supreme Court in 2005 made a decision on the difference in classifications "**information services" and "telecommunications**", which influenced the differences in their legal regulation and use in US law enforcement practice. [87, c.3].	Верховний суд США в 2005 р. виніс рішення про відмінність класифікацій «**інформаційні послуги»** і **«телевізійні комунікації**», що вплинуло на відмінності в їх правовому регулюванні і використанні в правозастосовчій практиці США. [50, с.3].	Калькування, модуляція

95.	(95) In a comprehensive discussion, the WGIG (Working Group on Internet Governance) has defined the concept of "Internet governance": Internet governance is the introduction and application by governments, the private sector and civil society, in their respective roles, of general principles, norms, rules, decision-making procedures and programs. regulate the evolution and use of the Internet **within information security.** [86, c.3].	Робоча група WGIG (Робоча група з управління інтернетом) з урахуванням всебічного обговорення виробила визначення поняття «управління інтернетом»: управління інтернетом є запровадження та застосування урядами, приватним сектором і громадянським суспільством, при виконанні ними своєї відповідної ролі, загальних принципів, норм, правил, процедур прийняття рішень і програм, що регулюють еволюцію і застосування інтернету в межах **інформаційної безпеки.** [50, с.13].	Калькування, модуляція
96.	(96) In Internet governance, Stakeholders play their "respective roles" in **information security.**	В управлінні інтернетом зацікавлені сторони виконують свої «відповідні ролі» з **інформаційної безпеки.**	Калькування, модуляція
97.	(97) The role and responsibilities of governments are related to such aspects activities such as the development, coordination and implementation of public policy at the national level, policy coordination at the regional and international levels; creating favorable conditions for the development of	Роль і обов'язки урядів пов'язані з такими аспектами діяльності, як розробка, координація та здійснення державної політики на національному рівні, координація політики на регіональному та міжнародному рівнях; створення сприятливих умов для розвитку **інформаційних і комунікаційних технологій (ІКТ).** [50, с.6].	Генералізація

	information and communication. [88, с.2].		
98.	(98) «Urges all Member States requesting exemption under Article 19 of the Charter to submit as much information as possible in support of their requests and to consider submitting such information in advance of the deadline specified in resolution 54/237 C so as to enable the collation of any additional detailed information that may be necessary 9 ». [87, с.3].	«Настійно закликає всі держави-члени, які звертаються з проханням про застосування вилучення, передбаченого в статті 19 Статуту, представляти якомога більше інформації в обгрунтування своїх прохань і прагнути подавати таку інформацію завчасно до граничного терміну, встановленого в резолюції 54/237 з тим, щоб мати можливість отримувати і аналізувати будь-яку додаткову детальну інформацію, яка може знадобитися». [50, с.3].	Описовий переклад
99.	(99) «Recalling that the United Nations was founded in the aftermath of two world wars to help shape a better future, he said the United States had developed the Marshall **Plan to help restore Europe**, guided by the pillars of sovereignty, **security** and prosperity10». [84, с.2].	«Нагадуючи, що Організація Об'єднаних Націй була створена після двох світових воєн, з метою допомогти сформувати краще майбутнє. Сполучені Штати розробили **Програму відновлення Європи у царині кібербезпеки**, щоб допомогти відновити Європу, керуючись засадами суверенітету, **безпеки** і процвітання». [50, с.12].	Описовий переклад
100.	(100) Calls upon the Secretary-General to continue to develop the network of focal points that supports the Coordinator for **cybersecurity.** [84, с.3].	Закликає Генерального секретаря продовжувати розвивати мережу кураторів, що сприяють Координатору з питань **кібербезпеки.** [50, с.12].	Граматична заміна