

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**ФАКУЛЬТЕТ ІНОЗЕМНОЇ ФІЛОЛОГІЇ
КАФЕДРА АНГЛІЙСЬКОЇ ФІЛОЛОГІЇ ТА ЛІНГВОДИДАКТИКИ**

**Кваліфікаційна робота
магістра**

**на тему СТРУКТУРНО-СЕМАНТИЧНІ ПАРАМЕТРИ
АНГЛІЙСЬКОМОВНИХ НЕОЛОГІЗМІВ СФЕРИ КОМП'ЮТЕРНИХ
ЗЛОЧИНІВ**

Виконала: студентка 2 курсу,
групи 8.0352-2 а-з
спеціальності 035 Філологія
спеціалізації 035.041 Германські мови та
літератури (переклад включно)
освітньо-професійної програми
Мова і література (англійська)
Дедюкіна Ольга Костянтинівна

Керівник к.ф.н., доц. Шевчук О. В.
Рецензент д.ф.н., доц. Веремчук Е. О.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет іноземної філології

Кафедра англійської філології та лінгводидактики

Освітній рівень магістр

Спеціальність 035 Філологія

Спеціалізація 035.041 германські мови та літератури (переклад включно)

Освітньо-професійна програма Мова та література (англійська)

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри

Надточій Н. О.

« » 20 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА
ДЕДЮКІНІЙ ОЛЬЗІ КОСТЯНТИНІВНІ

1. Тема кваліфікаційної роботи магістра (проєкту) «Структурно-семантичні параметри англійськомовних неологізмів сфери комп'ютерних злочинів»

Керівник кваліфікаційної роботи (проєкту) Шевчук Оксана Василівна,

к.ф.н., доцент

затверджені наказом ЗНУ від «11» квітня 2023 року № 516-с

2. Строк подання студентом кваліфікаційної роботи (проєкту) 5 грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи (проєкту)

теоретичні засади дослідження розвитку словникового складу англійської мови сфери комп'ютерних злочинів у XXI столітті: аналіз шляхів і способів утворення нових номінативних одиниць сфери комп'ютерних злочинів, що виникли під впливом суспільного життя у XXI столітті та їх структурний аналіз.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити).

1) здійснити огляд теоретичних джерел; 2) розглянути основні шляхи і способи розвитку словникового складу англійської мови у XXI столітті; 3) визначити структурно-семантичні особливості творення нових номінативних одиниць; 4) проаналізувати основні види комп'ютерних злочинів, які найбільше вплинули на розвиток словникового складу англійської мови; 5) визначити особливості формування неологізмів утворених під впливом суспільно-політичних рухів XXI століття; 6) дослідити їх структурні особливості.

5. Консультанти розділів кваліфікаційної роботи (проєкту)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Вступ	Шевчук О. В., к.ф.н., доц.	19.09.2023	19.09.2023
Розділ 1	Шевчук О. В., к.ф.н., доц.	15.10.2023	15.10.2023
Розділ 2	Шевчук О. В., к.ф.н., доц.	01.11.2023	01.11.2023
Висновки	Шевчук О. В., к.ф.н., доц.	16.11.2023	16.11.2023

6. Дата видачі завдання 19.09.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи магістра	Строк виконання етапів роботи (проєкту)	Примітка
1.	Пошук наукових джерел з теми дослідження, їх аналіз	вересень 2023	виконано
2.	Добір фактичного матеріалу	вересень 2023	виконано
3.	Написання вступу	вересень 2023	виконано
4.	Написання теоретичного розділу	жовтень 2023	виконано
5.	Написання практичного розділу	жовтень 2023	виконано
6.	Формулювання висновків	листопад 2023	виконано
7.	Проходження нормоконтролю	грудень 2023	виконано
8.	Одержання відгуку та рецензії	грудень 2018	виконано
9.	Захист	грудень 2018	виконано

Автор роботи несе персональну відповідальність за відсутність в роботі несанкціонованих текстових запозичень (академічного плагіату)

Магістрант _____
(підпис)

О. К. Дедюкіна _____
(ініціали та прізвище)

Керівник роботи _____
(підпис)

О. В. Шевчук _____
(ініціали та прізвище)

Нормоконтроль пройдено
Нормоконтролер _____
(підпис)

Е. О. Веремчук _____
(ініціали та прізвище)

РЕФЕРАТ

Дипломна робота – 78 стор., 53 джерела

Об’єкт дослідження: англійськомовні неологізми сфери комп’ютерних злочинів XXI століття.

Мета роботи: розкриття структурно-семантичних параметрів англійськомовних неологізмів сфери комп’ютерних злочинів.

Теоретико-методологічні засади: аналіз неологізмів проведено в контексті теоретичних висновків (Л. М. Архіпенко, С. Г. Волкова, В. В. Громовенко, та ін.) та лексикографічних досліджень («Словник неологізмів. Іновації у словниковому складі англійської мови початку XXI століття», “Cambridge Dictionary Online”, “Meriam Webster Dictionary” та ін.).

Отримані результати: серед структурно-семантичних параметрів англійськомовних неологізмів у сфері комп’ютерних злочинів виокремлюється вплив афіксації, композиції та аббревіації для формування нових термінів. З урахуванням семантичних особливостей, багато неологізмів безпосередньо пов’язані з характеристиками комп’ютерних злочинів, такими як “phishing”, “ransomware”, або “cyberbullying”. Також виявлено групу неологізмів, які активно використовуються для опису аспектів комп’ютерних злочинів у великих масштабах та їхнього впливу на суспільство. Порівняльний аналіз з використанням різних словникових джерел, таких як “Cambridge Dictionary Online” та “Longman Dictionary of Contemporary English”, доповнює та підтверджує отримані результати.

Ключові слова: *неологізм, структурно-семантичні параметри, комп’ютерний злочин*

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ НЕОЛОГІЗМІВ НА ТЛІ РОЗВИТКУ СЛОВНИКОВОГО СКЛАДУ АНГЛІЙСЬКОЇ МОВИ У 20-21 СТОЛІТТІ	7
1.1 Вплив суспільства на еволюцію словникового складу сучасної англійської мови	7
1.2 Створення неологізмів, як один із шляхів розвитку словникового складу англійської мови.....	14
1.3 Аналіз структурно-семантичних особливостей творення нових номінативних одиниць	21
РОЗДІЛ 2 КОМП'ЮТЕРНІ ЗЛОЧИНИ ЯК СУСПІЛЬНО-ПОЛІТИЧНЕ ЯВИЩЕ 21 СТОЛІТТЯ	31
2.1 Різновиди комп'ютерних злочинів	31
2.2 Комп'ютерні злочини пов'язані з суспільством	38
2.3 Комп'ютерні злочини пов'язані з економікою	47
2.4 Комп'ютерні злочини пов'язані з політикою.....	54
ВИСНОВКИ	59
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	62

ВСТУП

Безперервні зміни в суспільному житті, в суспільних відносинах, а також розвиток науки, техніки, мистецтва і культури невідмінно відбиваються в лексичному багатстві мови. Деякі слова виходять з активного словника і поступово втрачають свою актуальність, але в той же час народжується велика кількість нових слів, що розширює словниковий запас.

Мова – це продукт довгого історичного розвитку, і вона постійно змінюється. Ця динаміка мови тісно пов'язана з різними зовнішніми чинниками, такими як зміни в політичному, економічному і культурному житті суспільства. Крім того, вплив мовних контактів також відображається на різних аспектах мови, особливо на лексичному складі.

Детальним дослідженням неологізмів англійської мови займалися Л. М. Архіпенко, С. Г. Волкова, В. В. Громовенко, Ю. А. Зацний, О. І. Дзюбіна, Н. С. Демченко, М. О. Жулінська, Л. В. Клименко, К. Ю. Ладоня, Є. Б. Новікова, О. Д. Остафійчук, Н. В. Торнолог, О. І. Зіборова, Т. А. Пріт. Англійськомовні неологізми опрацьовані і лексикографічно, насамперед у таких словниках як «Словник неологізмів. Іновації у словниковому складі англійської мови початку XXI століття: англо-український», «Словник англійськомовних неологізмів XXI століття», “Cambridge Dictionary Online”, “Longman Dictionary of Contemporary English”, “Meriam Webster Dictionary”, “Oxford English Dictionary”, “Urban Dictionary Online”, “WordSense Dictionary Online”.

Попри значний інтерес до проблематики неологізмів та велику кількість присвячених їм наукових праць, у лінгвістиці досі є дискусійні положення, щодо їх структурно-семантичних параметрів та функціонування в сучасній англійській мові. Зокрема, не остаточно вирішеним є питання про визначення неологізмів у мові, принципи їх класифікування, основні функції, структурні характеристики та семантичні особливості.

Актуальність роботи полягає в необхідності опрацювання та аналізу структурно-семантичних параметрів англійськомовних неологізмів та з'ясування особливостей їх функціонування як складного лінгвістичного явища, спираючись на сучасний мовний матеріал.

Наукова новизна полягає у спробі власного дослідження структурно-семантичних параметрів англійськомовних неологізмів сфери комп'ютерних злочинів.

Об'єктом дослідження є англійськомовні неологізми сфери комп'ютерних злочинів ХХІ століття.

Предметом дослідження є структурно-семантичні параметри англійськомовних неологізмів сфери комп'ютерних злочинів.

Метою дослідження є розкриття структурно-семантичних параметрів англійськомовних неологізмів сфери комп'ютерних злочинів.

Для дослідження поставленої мети необхідно вирішити наступні **завдання**:

- 1) з'ясувати теоретичні засади дослідження на тлі розвитку словникового складу англійської мови у 20-21 століття;
- 2) виявити вплив суспільства на еволюцію словникового складу сучасної англійської мови;
- 3) розглянути створення неологізмів, як один із шляхів розвитку словникового складу англійської мови;
- 4) здійснити аналіз структурно-семантичних особливостей творення нових номінативних одиниць;
- 5) дослідити комп'ютерні злочини як суспільно-політичне явище 21 століття;
- 6) надати класифікацію комп'ютерних злочинів;
- 7) проаналізувати структурно-семантичні параметри неологізмів сфери комп'ютерних злочинів пов'язаних з суспільством, економікою, політикою.

Матеріалом матеріалом дослідження слугували словники англійськомовних неологізмів сфери комп'ютерних злочинів.

Методи дослідження. Дослідження здійснювалось на основі використання таких методів та прийомів: лінгвістичного спостереження та аналізу – для з'ясування теоретичних засад дослідження на тлі розвитку словникового складу англійської мови у 20-21 столітті, створення неологізмів, як один із шляхів розвитку словникового складу англійської мови, описового і компонентного методів – для аналізу структурно-семантичних особливостей творення нових номінативних одиниць та комп'ютерних злочинів як суспільно-політичного явища 21 століття, методу аналізу словникових дефініцій – для визначення структурно-семантичних параметрів неологізмів сфери комп'ютерних злочинів пов'язаних з суспільством, економікою, політикою.

Практична значущість дослідження полягає у можливості використання його результатів під час проведення семінарських занять з лексикології, стилістики, теоретичної граматики та практичних занять з англійської мови.

Робота пройшла **апробацію** на XV Міжнародній науковій конференції «Іноземна філологія у XXI столітті». Результати дослідження представлено у публікації:

1. Шевчук О. В., Дедюкіна О. К. Дослідження неологізмів у сфері комп'ютерних злочинів в політиці. *«Іноземна філологія у XXI столітті»* : збірник тез доповідей XV Міжнародній науковій конференції (24 листопада 2023 року). Запоріжжя : Запорізький національний університет, 2023. С. 31– 35.

Структура роботи: дослідження складається зі вступу, двох розділів, висновків, додатку та списку використаної літератури.

У вступі подано загальні відомості про дану наукову працю, починаючи від умотивування теми, мети, завдань, актуальності дослідження, визначення об'єкту, предмету та структурування роботи.

У першому розділі подаються теоретичні засади на тлі розвитку словникового складу англійської мови у 20-21 столітті, особлива увага приділяється впливу суспільства на еволюцію словникового складу сучасної англійської мови та створенню неологізмів як одному із шляхів розвитку словникового складу англійської мови, структурно-семантичним особливостям творення нових номінативних одиниць.

Другий розділ містить власний аналіз класифікації неологізмів комп'ютерних злочинів та дослідження структурно-семантичних параметрів неологізмів сфери комп'ютерних злочинів пов'язаних з суспільством, економікою, політикою.

У висновках подано узагальнені результати проведеної роботи.

Загальна кількість сторінок 78, кількість використаних джерел 53.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ НЕОЛОГІЗМІВ НА ТЛІ РОЗВИТКУ СЛОВНИКОВОГО СКЛАДУ АНГЛІЙСЬКОЇ МОВИ У 20-21 СТОЛІТТІ

1.1 Вплив суспільства на еволюцію словникового складу сучасної англійської мови

Безперервні зміни в суспільному житті, в суспільних відносинах, а також розвиток науки, техніки, мистецтва і культури невідмінно відбиваються в лексичному багатстві мови. Деякі слова виходять з активного словника і поступово втрачають свою актуальність, але в той же час народжується велика кількість нових слів, що розширює словниковий запас.

Мова – це продукт довгого історичного розвитку, і вона постійно змінюється [Торнолог 2016]. Ця динаміка мови тісно пов'язана з різними зовнішніми чинниками, такими як зміни в політичному, економічному і культурному житті суспільства. Крім того, вплив мовних контактів також відображається на різних аспектах мови, особливо на лексичному складі.

Оскільки мова є неотдільним аспектом суспільства, існує взаємозв'язок між ними. Цей взаємозв'язок виявляється взаємно. З одного боку, мова формується та розвивається завдяки впливу суспільства, а з іншого боку, існування суспільства без мови було б неможливим. Мова служить усім сферам соціуму як функціональний організм, і навіть трудова діяльність не може обійтися без неї.

Розвиток та функціонування мови в значній мірі залежать від стану суспільства. Наприклад, у мові відображається соціальна диференціація суспільства, така як класова, професійна та статеві. На мовний стан впливають демографічні процеси, такі як зміни в чисельності населення, співвідношення

між містом та селом, міграційні процеси, а також рівень загальної освіти та розвиток науки. Створення державності також має велике значення.

Суспільство може свідомо впливати на розвиток мови, і цей свідомий вплив відомий як мовна політика. Мовна ситуація в багатомовному суспільстві залежить від цілеспрямованих заходів, які вживає суспільство через мовну політику [Сухенко 2016, с. 734].

У світі мови неминуче відбуваються зміни, а сучасна англійська мова не виняток. Важливо відзначити, що англійська мова справді активно запозичує слова, і ця тенденція відображається у її словнику. Але варто відзначити, що, порівняно з іншими мовами, особливо французькою, кількість запозичень зазвичай є значною більше.

Сучасна англійська мова набуває все більшого словникового багатства, і це проявляється в швидкому зростанні кількості неологізмів. Різні галузі людської діяльності постійно збагачують словник англійської мови за рахунок нових слів, і цей процес стежить вже давно [Мурко 2012, с. 20].

Англійська мова продовжує розширюватися завдяки запозиченням, хоча це відбувається менш інтенсивно, ніж в минулому. З мови, яка запозичує, вона перетворюється на мову, яка в свою чергу вносить свій внесок у інші мови. Це пов'язано з тим, що англійська мова стала мовою міжнародного спілкування у XX столітті.

На сучасному етапі розвитку англійської мови також важливо зазначити роль внутрішніх запозичень. Це вже не тільки запозичення з інших мов, але й взаємодія національних варіантів англійської мови, а також стилістичних підсистем. Цей процес відбувається в контексті тенденції до демократизації мови і зближення писемно-літературної та усно-розмовної мови [Зацний 2016, с. 28].

Наприклад, у Сполучених Штатах англійська мова інтегрується з мовами місцевих національних груп, і це призводить до семантичного розвитку слів. Слова можуть змінювати своє значення або зберігати первісне, створюючи нові лексично-семантичні варіанти.

Зміни в суспільстві, нові досягнення в науці, технології та культурні особливості призводять до появи нових слів в мові. Культура, як невід'ємна складова життя людей, також впливає на словниковий склад мови. Американські субкультури також мають великий вплив на розвиток словникового складу англійської мови.

Сучасна англійська мова продовжує еволюціонувати, і це відбувається через різноманітні чинники, включаючи запозичення, внутрішні зміни і вплив культури. Це робить мову живою і динамічною, і нові слова відображають зміни в суспільстві та світогляді.

Еволюція словникового складу сучасної англійської мови є складним процесом, який в значній мірі визначається впливом суспільства. Суспільство, як складова частина соціокультурного середовища, надає значний вплив на формування, збагачення та зміну лексичного фонду мови через низку факторів.

Цей вплив проявляється через широкий спектр соціокультурних, технологічних, економічних та політичних факторів. Відображенням цього впливу є постійні зміни, додавання нових слів, фраз, або змінення значень існуючих слів у словнику англійської мови [Зацний 2015, с. 67]. Дослідження цього явища вимагає комплексного підходу, що враховує різні аспекти взаємодії мови та суспільства.

Попередні дослідження [Клименко 2021, с. 56] підтверджують, що суспільні зміни, такі як технологічний прогрес, соціокультурні трансформації, міграційні процеси та глобалізація, безпосередньо впливають на словниковий склад англійської мови.

Можна визначити такі напрямки впливу суспільства на розвиток сучасної англійської лексики.

- створення нових технічних засобів призводить до одночасної появи нових слів. Наприклад: *device, smartphone*;
- прагнення до збереження місця, до скорочення, що можна побачити на прикладі сучасного онлайн-спілкування: *FONO (fear of normal), FORO (fear of running out), HOGO (hassle of going out)*. Нові слова, які з'являються внаслідок

дії закону збереження мовних засобів, значно ускладнюють розуміння спілкування, особливо коли йдеться про людину, яка не належить до певної групи;

- нові політичні тенденції також призводять до неологізмів;
- різноманітні соціальні явища теж призводять до появи нових слів.

наприклад: *cardening*, утворено від слів *car+gardening*; *digi-dog*, утворено від слів *digit+dog*; *docuality*, утворено від слів *documentary+reality*; *emoticonomy*, утворено від слів *emotion+ecomony*; *flurona*, утворено від слів *flu+corona*; *hortpreneur*, утворено від слів *horticulture+entrepreneur*;

- екологічні проблеми також призводять до неологізмів. Наприклад, з'явилося слово *locavores* 'споживачі, які вважають за краще купувати місцеві продукти;

- популярність соціальних мереж вимагає нових слів, наприклад, *defollow* і *unfriend*;

- існування різних субкультур теж впливає на лексику. Наприклад: *wish-cycling*, утворено від слів *wish+recycling*; *zoomer*, утворено від слів *Generation Z+boomer* [Дзюбіна 2016; Ладоня 2021, с. 234; Новікова 2017, с. 99].

Завершення ХХ і початок ХХІ століття супроводилися раптовим розвитком комп'ютерних та цифрових технологій, що вплинули не лише на конкретні предмети і явища, але й на суспільне життя в цілому. Ці зміни миттєво відобразилися в англійській мові, оскільки мова змінюється нарізі з розвитком суспільства. Серед найзначущих суспільних явищ, що спричинили появу нових слів у ХХІ столітті, можна виділити створення комп'ютерних та цифрових технологій, глобалізацію Інтернету, зміни в навколишньому середовищі, а також розвиток нових форм проведення часу та розваг [Зацний 2018].

Наприклад, розвиток інформаційних технологій призвів до появи нових термінів, пов'язаних з цифровими технологіями, соціальними мережами, інтернетом та електронною комунікацією. На сьогоднішній день, Інтернет став головним джерелом виникнення нових слів і виразів, які відображають

сучасну англомовну реальність. Це легко пояснюється широкою популярністю мережі та її постійною зміною. З появою нових технологій і гаджетів, створення нових слів стає необхідністю [Жулінська 2018, с. 88].

Особливо це стосується термінів, які описують нові технології та послуги. Наприклад, *phablet*, що поєднує *phone* і *tablet*, вказує на телефон із великим сенсорним екраном, схожим на планшет. *Bitcoin* – це електронна грошова операція, яку можна виконати без відвідування банку, *click and collect* – сервіс, що дозволяє замовляти товари онлайн та забирати їх у магазині у зручний час.

Також, активність користувачів в Інтернеті та соціальних мережах викликає створення нових слів, що описують їхню поведінку. Наприклад, *infomania* – це непереборне бажання постійно відслідковувати новини в Інтернеті, *textpectation* – момент очікування відповіді на відправлене повідомлення, *unsend* – можливість видалення електронного листа після відправлення. Крім того, збір, аналіз та використання даних з цифрових джерел, як соціальні мережі, також отримують свої назви, як от *datafication*.

Разом із цим, мережа сприяє створенню термінів, пов'язаних із популярністю в соціальних мережах, таких як *instafamous*, який вказує на популярність, досягнуту завдяки розміщенню фотографій в Instagram. Також існують слова, як *hate-watch*, що описує перегляд відео з негативними коментарями.

Поряд з цим, соціальні зміни в англомовних країнах, такі як зміни в цінностях, соціальних нормах та політичних установах, також відображаються в словниковому складі мови. Це включає зміни в термінології, яка відображає нові соціальні явища, політичні реалії та соціальні проблеми.

Неологізми в політичній сфері часто виникають на основі імен відомих осіб. Наприклад, ім'я Дональда Трампа та всі події, пов'язані з його президентством, спричинили створення численних нових слів і виразів [Жулінська 2018, с. 88].

Один із найсвіжіших термінів – *Trumpism*, який відображає політику та погляди самого Дональда Трампа в загальному контексті. *Trumponomics*

вказує на економічну політику, проведену президентом. *Trumpertantrum* відноситься до ранкових серійних твітів Трампа, які часто містять брехню.

Декілька неологізмів стосуються іконічного образу Трампа. *Trumpkin* – це гарбуз із виїмкою, яка нагадує обличчя Трампа. *Trumpshake* вказує на тривале рукостискання, яке може тривати досить довго.

Політика адміністрації Трампа також вплинула на економіку. *Trumpflation* відноситься до інфляції, яку деякі аналітики передбачають через політику нової адміністрації.

Терміни, такі як *Trumpist*, *Trumpette*, та *Trumpista*, описують різні прихильників і послідовників Трампа в різних соціальних групах та мовах.

Trumpcare відноситься до реформи охорони здоров'я, запропонованої Трампом та його партією як альтернатива програмі охорони здоров'я, запровадженій при попередньому президентові Обамі. *Trumpflakes* використовуються для позначення людей, які нездатні об'єктивно оцінювати Трампа і захищають його безкритично.

Ці неологізми є відображенням впливу Дональда Трампа на політичну риторику та культуру, і вони продовжують розширювати наше мовне багатство [Жулінська 2018, с. 88].

Економічні й політичні зрушення у світі також відображаються у словнику англійської мови через включення термінів, пов'язаних з економічною діяльністю, торгівлею, політичними процесами, міжнародними відносинами та іншими аспектами світової діяльності. Політичні реформи або економічні зміни можуть вимагати створення нових слів для вираження нових концепцій або явищ. Наприклад, глобалізація та міжнародний бізнес сприяли включенню термінології, що відображає міжкультурну взаємодію, світову торгівлю та інвестиції.

Неологізми в економічній галузі, що з'явилися в останньому році, відображають нові підходи до маркетингу, спрямовані на підвищення продажів. [Жулінська 2018, с. 89].

BlackFriday – це п'ятиденний період перед Днем подяки, коли магазини роблять знижки на товари, щоб привернути більше покупців. Іноді ця акція включає в себе і *doorbuster* – товар, який продається за дуже низькою ціною, щоб залучити покупців в магазин з надією на купівлю більш дорогих товарів.

Golden quarter відноситься до тримісячного періоду (жовтень - грудень), коли роздрібні торговці зазвичай отримують найбільший прибуток завдяки святковим покупкам.

Також, варто відзначити слово *genericide*, яке вказує на явище, коли певні характеристики продукції відомого бренду стають загальноприйнятими для всієї галузі [Жулінська 2018, с. 89].

Неологізми проходять кілька етапів взаємодії з суспільством, включаючи стадії соціалізації (прийняття в суспільстві) та лексикалізації (закріплення в мові). Якщо концепція, пов'язана з новоствореним словом, стає актуальною для суспільства, то воно швидко закріплюється в мові, особливо якщо це пов'язано з обговоренням важливих тем для світової спільноти.

Сучасними темами, що породжують неологізми, є, наприклад, вихід подружжя принца Гаррі і Меган Маркл із королівської родини та перебування на карантині в зв'язку з *COVID-19*. Так, з'явилися неологізми, які відображають сучасне сприйняття дійсності, такі як *to meghan markle* – дієслово, яке означає цінувати своє психічне здоров'я настільки, щоб вийти з ситуації, де не розуміють вашої істинної особистості. Ще одним прикладом є *covidiot* – іменник, що позначає людину, яка не дотримується правил соціального дистанціювання під час пандемії, або ж ту, яка викликає паніку та скуповує товари, ушкоджуючи інших.

Ці слова відображають нові реалії, але вони не завжди можуть бути легко перекладені або знайти аналоги. У такому випадку виникає потреба в описовому перекладі, оскільки вони виражають концепції, які не мають точного відповідника в інших мовах [Остапчук 2020, с. 156].

Отже, робимо висновок, що культурні зміни в суспільстві, такі як зростання популярності певних видів мистецтва, спорту або технологій,

можуть призвести до введення в мову нових слів та виразів, що відображають ці зміни. Такі терміни можуть виникати в реакції на нові тренди та інтереси суспільства.

Одночасно, соціокультурні зміни, що стосуються сексуальної орієнтації, расової різноманітності та інших аспектів ідентичності, також призводять до включення нових термінів, які відображають ці соціальні явища, в словник англійської мови.

Суспільство виступає важливим детермінантом в еволюції словникового складу сучасної англійської мови, впливаючи на структуру, зміст та функції слів у відповідності до змін у політичному, економічному, культурному та соціальному контексті.

1.2 Створення неологізмів, як один із шляхів розвитку словникового складу англійської мови

Неологізми – це терміни або слова, які є абсолютно новими для кожного конкретного історичного періоду. Вони ще не включені до активного словникового запасу і, отже, можуть бути нерозпізнаваними. Термін «неологізм» застосовується до нових слів, створених відповідно до існуючих словотвірних моделей, які позначають нові, раніше невідомі поняття, предмети, галузі науки, професії тощо [Пріт 2018].

У XVIII ст. лінгвісти упереджено ставились до явища неологізації, бо вважалося, що нові слова «ображають» народну мову тільки своїм існуванням, не говорячи про їх вживання [Зацний 2010, с. 194]. Проте процес збагачення лексики – історично неминучий, а також необхідний для відповідності мови сучасним потребам суспільства на певному етапі свого розвитку як при комунікації, так і в розвитку та поповненні народної культури. У лінгвістиці поняття неологізм має глибокі корені, хоча є суперечливим і досі через низку

фактів. Вперше в англійській мові термін неологізм був зафіксований у 1772 році.

У кінці ХХ та на початку ХХІ століть англійська мова у сфері економіки пройшла суттєві та різноманітні зміни в словниковому складі, які були обумовлені швидким розвитком бізнесу, економічною глобалізацією та поширенням сучасних інформаційних технологій. У сучасній лексико-семантичній системі англійської мови спостерігаються активні та динамічні процеси. Розвиток мови на лексичному рівні пов'язаний, передусім, з появою нових слів та фраз, які сприймаються носіями мови як нові за формою або змістом [Зацний 2010].

Неологізми виникають з різних причин, таких як:

1. Потреба найменувати нові об'єкти, явища або поняття, які раніше не мали чіткої лексичної форми;
2. Необхідність замінити існуючі назви більш точними та зрозумілими, щоб вони відповідали сучасним стандартам української мови (лексичні неологізми);
3. Присвоєння словам, які вже існують в мові, нових значень (семантичні неологізми);
4. Бажання надати предметові або явищу свіжу образну назву, яка краще відображає світогляд автора (індивідуальні або авторські неологізми) [Зіборова 2018].

Ознакою неологізму є абсолютна новизна слова для більшості користувачів мови. Таке слово є неологізмом лише на короткий період, оскільки, як тільки воно стає широко вживаним, втрачає свою новизну і стає загальноновживаним. Наприклад, слова *lunar rover*, *spaceport*, *radar*, *launcher rocket*, *programming* не є неологізмами в наш час, хоча в минулому вони були новими.

Процес створення неологізму розпочинається з того, що людина, названа *originator*, створює нове слово в прагненні до індивідуалізації і оригінальності. Далі це слово проходить стадії соціалізації, де його приймають в суспільстві, і

лексикалізації, де воно закріплюється в мовній системі. Слово розповсюджується посередниками, такими як викладачі, репортери, та фіксується в періодичній пресі, після чого воно поступово приймається широкими масами користувачів мови. Завершальним етапом є набуття навичок адекватного вживання нового слова та його повноцінне введення в комунікативний процес, що представлено у ланцюжку «ланцюжок неологізації» [Пріт 2018].

Погляди та підходи до визначення неологізмів в англійській мові можуть бути цікавими для дослідження. Деякі дослідники пропонують розглядати час як один з ключових параметрів конкретизації неологізмів. Іншими словами, слова вважаються неологізмами, доки вони існують у мові після певного періоду, який прийнято за вихідний, і в них зберігається відчуття новизни і актуальності. Проте, якщо слово використовується дуже часто, воно швидко втрачає цю ознаку.

Таким чином, визначають п'ять критеріїв визначення неологізмів:

- слова, що відображають нову реальність;
- стилістична категорія, де важливим критерієм є відчуття смислової новизни;
- існування синоніму з конотативним відтінком до вже існуючого слова;
- слова, які існують в певний момент часу та мовному просторі;
- характеристика як незазначеного або зазначеного слова у словника.

Підходи Л. Клименко [Клименко 2021, с. 23] також варто враховувати, оскільки вона виділяє кілька лінгвістичних теорій, які розкривають сутність неологізмів. Зокрема, стилістична теорія вказує на важливість конотації новизни при використанні слів. Актуальність є ключовим критерієм при ідентифікації неологізмів і залежить від різних аспектів компетенції людини та її життєвого досвіду.

Психолінгвістичний підхід додає ще один вимір до розуміння неологізмів. Він вивчає неологізми в контексті мовної діяльності та розвиває психолінгвістичну концепцію, де важливим є індивідуальний лексикон та

суб'єктивна новизна. Цей підхід враховує вплив соціального розвитку особистості на сприйняття нових слів.

Відносини людини зі світом і оточенням завжди були головними пріоритетами. Тому, коли мова йде про сфери, де виникають нові слова і вирази, це перш за все відображає те, як людина ставиться до себе, своїх звичок, зовнішності та характеру, і як вона порівнює себе з іншими. Нові слова найчастіше з'являються у таких сферах, як щоденне життя, культурна сфера, передові технології, мобільна комунікація та політична діяльність [Остафійчук 2020, с. 158].

Нові слова, як правило, з'являються в мові особистості, яка хоче виразити свою думку якимось оригінальним способом. Нові лексичні одиниці в основному використовуються викладачами університетів, репортерами газет, тими, хто пов'язаний із засобами масової інформації. Неологізми можуть розвиватися трьома основними способами:

1) лексична одиниця, що існує в мові, може змінити своє значення, позначаючи новий об'єкт або явище. У таких випадках ми маємо семантичні неологізми, наприклад, слово *umbrella* набуло значення: «авіаційне прикриття», «політичне прикриття»;

2) нова лексична одиниця може розвиватися в мові, щоб позначити об'єкт або явище, яке вже має певну лексичну одиницю для її позначення. У таких випадках ми маємо транснамінацію, наприклад, слово *slum* «трущоба» спочатку замінювалося словом *ghetto* «гетто», потім словосполученням *inner town* «внутрішнє місто»;

3) нова лексична одиниця може бути введена для позначення нового об'єкта або явища. У цьому випадку ми маємо належний неологізм, багато з них є випадками нової термінології [Новікова 2017, с. 101].

З погляду створення слів існують різні типи неологізмів, які можна виділити на різних рівнях мови, таких як фонологічний, семантичний та синтаксичний.

Фонологічні неологізми – це особливі звукові утвори, що складаються з окремих звуків. Вони вражають найсильнішою відмінністю від звичайних мовних образців і вважаються дуже несподіваними за своєю формою [Дзюбіна 2018, с. 39]. Цей тип неологізмів є найпоширенішим в англійській мові і формується шляхом поєднання звуків, часто із використанням звуконаслідувальних вигуків. Особливо активно це відбувається в американському сленгу, як, наприклад, слово *bazinga*, яке виникло на основі звуку *zing* [Волкова 2019, с. 113].

Іншим важливим аспектом є використання запозичень. Серед запозичень можна виділити дві основні категорії – варваризми та ксенізми. Варваризми – це слова, які мають синоніми в мові-реципієнта, тобто мови, в яку вони були запозичені. Ксенізми, натомість, є словами, які позначають явища і об'єкти, які існують тільки в країні-джерелі, або країні, з якої вони були запозичені, і відсутні в мові-реципієнта. Варваризми та ксенізми характеризуються незвичайними звуковими структурами, нетиповим морфологічним утворенням та відсутністю логічного пояснення для їх вживання в мові-реципієнта [Дзюбіна 2018, с. 39].

Особливо в епоху глобального спілкування через інтернет і соціальні мережі. Це також стає джерелом для створення нових слів. Навіть при тому, що англійська мова стала не тільки отримувачем слів, але і донором для інших мов, її словниковий запас продовжує розширюватися завдяки запозиченням з інших мов. Наприклад, слово *bokeh* було запозичено з японської мови. Оскільки англійська мова є загальноприйнятою в сфері інформаційних технологій і програмування, то відбувається обмежена кількість запозичень з інших мов, як, наприклад, слово *drone*, яке походить з німецької мови і означає комаху, схожу на бджолу [Волкова 2019, с. 113].

Морфологічні новоутворення – це слова, які формуються шляхом комбінування вже існуючих і стандартизованих мовних елементів в межах мовної системи. Вони виникають через застосування різних систематичних мовних процесів для створення нових слів. Морфологічні неологізми

характеризуються абсолютною унікальністю своєї структури та формальною новизною, оскільки вони представляють собою унікальні комбінації звуків та морфем, і не мають відповідників в мовних структурах. Такі слова сприймаються як неподільні, не походять від інших слів і не мають логічного пояснення для свого існування в мові [Дзюбіна 2018, с. 39].

Наприклад, слова *defriend* та *webmaster* використовують наявні у мові морфеми для своєї структури. Цей тип неологізмів може поділятися на різні види в залежності від способу створення. Найбільш поширеними і продуктивними є афіксальні неологізми, які формуються за допомогою префіксів або суфіксів, що вже існують у мові. Наприклад, слова *googlable* та *facebookian* створені за допомогою таких морфем. Інший спосіб створення морфологічних неологізмів – це словоскладання, яке також відіграє важливу роль у формуванні нових слів. Особливість цього виду неологізмів полягає в тому, що вони не базуються на коренях слів, але формуються шляхом поєднання двох повних слів. Однією з найбільш поширених моделей словоскладання є іменник + іменник, як у словах *Masnazi* та *mousepotato*. Також існує інший шаблон, де використовують прикметник + іменник, як, наприклад, у словах *cybercafe* та *digitaldetox* [Волкова 2019, с. 113].

Мовні неологізми створюються, переважно, для позначення нових предметів чи понять і включаються до активного словникового запасу, а також фіксуються у словниках. У сфері комп'ютерної та суспільно-політичної мови англійської мови існує велика кількість прикладів мовних неологізмів. Наприклад, *attention theft* означає втручання небажаного і несанкціонованого тексту, звуків або зображень в інтереси людини, а *Cord-never* вказує на людину, яка ніколи не підписувалася на пакет кабельного телебачення.

Однак, розглядаючи класифікацію нових слів, можна виділити дві основні категорії мовних неологізмів: лексичні та семантичні. Лексичні неологізми – це нові слова, які утворюються на основі вже існуючих слів та їх елементів, включаючи складні, афіксальні похідні, аббревіатурні утворення тощо, або слова, які запозичені з інших мов. Це можуть бути новостворені слова або

словосполучення, які відображають нові, раніше невідомі поняття, предмети в галузі науки, нові професії, рід занять та інші концепції, які раніше не існували в мові [Дзюбіна 2018, с. 39].

Прикладами лексичних неологізмів можуть бути слова, такі як *Blogject*, що означає пристрій, який регулярно публікує поновлення про стан, місцезнаходження та навколишнє середовище.

Семантичні неологізми включають вже відомі слова, які отримують нові значення через останні зміни у мові. Наприклад, *Hearable* означає маленький комп'ютер або електронний пристрій, призначений для носіння на вусі [Ситенко 2019, с. 46].

Авторські, індивідуально-стилістичні неологізми створюються з метою надання тексту більшого художнього виразу. Ці неологізми, які приписуються конкретному автору і часто використовуються в його творчості, мають певний стилістичний колір. Вони повинні залишатися незвичайними та оригінальними. Такі неологізми, які формуються на основі вже відомих мовних моделей, називають потенційними словами. Наприклад, *pizza parliament* вказує на парламент, складений з багатьох партій, де кожна з них має обмежену кількість місць, а *Zombie lie* – це неправильна твердження, яке постійно повторюється, незважаючи на те, що часто воно було спростовано.

Оказіоналізми, створені на основі незвичайних мовних моделей, також є авторськими неологізмами, але вони існують лише в конкретному контексті та в межах певного авторського твору. Наприклад, *infobesity* визначає надмірну інформацію або перенасиченість інформацією [Ситенко 2019, с. 47].

Багато нових слів в англійській мові виникають на фоні соціальних та культурних змін. На сучасному етапі спостерігається тенденція до здорового способу життя, і це відображається у виникненні нових слів, таких як *mascular* (сильний і мужній), *fattitude* (позитивне ставлення до власної ваги), *tobeast* (продемонструвати силу і витривалість), *coffeebreath* (проблеми з диханням через зловживання кавою). Ці слова відображають актуальні теми та поняття, які стають важливими для сучасного суспільства, і вони є результатом

лінгвістичних відображень змін у способі життя та цінностях [Meriam Webster Dictionary].

Отже, різні підходи та критерії визначення неологізмів надають багатогранну картину цього лінгвістичного явища і вказують на складність його аналізу та розуміння.

Зміни в активному досвіді людини і надалі будуть призводити до виникнення нових та розширення старих аспектів сприйняття світу, які, в свою чергу, потребуватимуть відображення на мовній карті світу. Англійська мова, так само, як і багато інших мов, постійно досвіджуватиме неологічний бум.

Це означає, що у мові з'являтимуться нові слова, які з часом проходилимуть всі стадії соціалізації та лексикалізації, тобто будуть прийняті суспільством і зафіксовані науковою галуззю, вивчаючою неологізми – неологією.

Цей процес свідчить про живий розвиток мови та її здатність адаптуватися до змін у суспільстві і культурі. Таким чином, створення неологізмів – це не лише лінгвістичний процес, але й відображення динамічної природи мови та її здатності відображати сучасні реалії. Розуміння цього явища має важливе значення для лінгвістів, мовознавців та культурологів, а також для всіх, хто вивчає англійську мову та цікавиться її еволюцією в контексті сучасного світу.

1.3 Аналіз структурно-семантичних особливостей творення нових номінативних одиниць

Мова постійно еволюціонує та поповнюється різноманітними мовними засобами, подібно до того, як живий організм розвивається. Однак, найбільш гнучкою та швидкозмінною частиною мови є її словниковий склад, або лексика. Лінгвісти завжди були зацікавлені питанням, як нові слова та вирази

потрапляють до мови та як відбувається процес їхньої формування [Демченко 2019].

Зокрема, у сучасному світі особливу увагу приділяють вивченню новоутворень у лексичному складі мови. Це пов'язано з швидким розвитком науки, сучасних інтернет-технологій, суспільнополітичного та культурного життя. Усі ці сфери активно сприяють появі нових слів та фраз, які швидко впроваджуються в усну та письмову мову.

Сучасна англійська мова, зокрема, переживає справжній бум у створенні нових лексичних одиниць, і необхідність вивчення цього процесу призвела до створення нової галузі лексикології, відомої як неологія. Неологія – це наука про новоутворення в мові, і вона досліджує як і коли нові слова та фрази з'являються, і як вони розповсюджуються серед мовців [Демченко 2019, с. 48].

Всі неологізми, їх будова та значення, формуються відповідно до англійських словотвірних методів, коли існує необхідність у створенні нового слова. На сьогоднішній день існують декілька надзвичайно продуктивних методів для розширення лексичного запасу англійської мови. Серед них виділяються такі як **телескопія**, **афіксація**, **словоскладання**, **конверсія** та **скорочення**. Приблизно 96% новоутворених слів в англійській мові створюються за допомогою цих методів словотвору [Зацний 2010].

Телескопія – це метод створення нових слів шляхом поєднання частин інших слів, зберігаючи їхні початкові морфеми [Баркасі, Каленюк, Коваленко 2017, с. 71].

Цей метод сприяє створенню нових термінів, які мають зрозуміле походження і широко використовуються в наукових, технічних та комунікаційних контекстах. Ця техніка створення слів часто ґрунтується на фонетичній схожості, яка полегшує їхнє вимовляння та розуміння.

У наукових галузях неологізми формуються так, щоб легко сприймалися обидва компоненти слова, які їх створюють. Наприклад, такі слова, як *cyborg*, *bionics* і *astrionics*.

У публіцистиці та рекламі, семантика слів може бути важкою для розуміння без відповідного контексту. Наприклад, *galumph* – це результат поєднання слів *gallop* і *triumph*, але для багатьох це може бути неочевидним [Opentalk].

Існують різні способи створення нових слів за допомогою телескопії:

1. Об'єднання граматичних основ. Цей метод включає в себе поєднання коренів двох слів, де вони зливаються в одне слово, враховуючи правила милозвучності. Прикладами такого поєднання є слова *cyborg* та *medicare*;

2. Комбінування початку одного слова та закінчення іншого: Цей підхід полягає в об'єднанні початку одного слова з закінченням іншого. Прикладами цього методу є слова *brunch*, *Oxbridge*, та *galumph*.

3. З'єднання повної основи одного слова зі скороченою основою іншого. Тут використовуються повні основи одного слова та скорочені основи іншого для створення нового слова. Прикладами є слова *workaholic* та *narcoma*;

4. Об'єднання двох повних граматичних основ з фонетичним накладанням. У цьому методі дві повні основи об'єднуються з фонетичним накладанням, створюючи новий термін. Прикладами можуть бути слова *glasphalt* та *slanguage*;

Основна цінність телескопії полягає в збереженні оригінальних морфем у нових словах, що полегшує розуміння сенсу цих слів з високою ймовірністю [Opentalk].

Телескопізми можуть функціонувати як різні частини мови. Наприклад, телескопізм-прикметник може бути утворено за моделлю А+А (прикметник + прикметник), зокрема: *swicy*, утворено від слів *sweet+spicy*.

Телескопізми-іменники можуть бути утворені за такими моделями:

- А+N (прикметник + іменник), наприклад: *carnisplorer*, утворено від слів *carnivorous+explorer*; *finfluencer*, утворено від слів *financial+influencer*; *flexcation*, утворено від слів *flexible+vacation*; *greenflation*, утворено від слів *green+inflation*; *holistorexia*, утворено від слів *holistic+anorexia*; *resimercial*,

утворено від слів *residential+commercial*; *soonicorn*, утворено від слів *soon+unicorn*;

- G+N (герундій + іменник), наприклад: *volunteercation*, утворено від слів *volunteering+vacation*;

- N+A (іменник + прикметник), наприклад: *pingdemic*, утворено від слів *ping+pandemic*;

- N+N (іменник + іменник), наприклад: *cardening*, утворено від слів *car+gardening*; *digi-dog*, утворено від слів *digit+dog*; *docuality*, утворено від слів *documentary+reality*; *emoticonomy*, утворено від слів *emotion+ecomony*; *flurona*, утворено від слів *flu+corona*; *hortpreneur*, утворено від слів *horticulture+entrepreneur*; *husean*, утворено від слів *hydrogen+ocean*; *seaganism*, утворено від слів *sea+veganism*; *tourdrobe*, утворено від слів *tour+wardrobe*; *wish-cycling*, утворено від слів *wish+recycling*; *zoomer*, утворено від слів *Generation Z+boomer*.

Узагалі серед телескопізмів переважають іменники, а інші частини мови і, зокрема, прикметники, трапляються рідше. Найчастотнішою моделлю утворення телескопізмів-іменників є N+N (іменник + іменник), також частотною є модель A+N (прикметник + іменник) [Омельченко 2013, с. 50].

Афіксація – це процес створення нових слів, використовуючи суфікси і префікси. В результаті афіксалізації лексичні одиниці перетворюються з самостійних лексем в слова, які мають внутрішню зв'язаність та втрачають комунікативну самостійність [Баркасі, Каленюк, Коваленко 2017, с. 8].

Разом із класичними методами словотвору існують і нові підходи. Наприклад, шляхом афіксації утворено слово *e-quaintance*, яке означає знайомого, з яким спілкуються виключно через Інтернет, а не в реальному житті. Це слово походить від *acquaintance* (знайомство), до якого додано початковий префікс *e-*, який є скороченням від *electronic*. Аналогічні приклади також включають *e-ticket* (електронний квиток), *e-wallet* (електронний гаманець), *e-business* (покупка і продаж через Інтернет) і *e-learning* (онлайн-навчання) [Longman Dictionary of Contemporary English].

Першим кроком у цьому процесі є включення лексеми до складу складних слів чи композитів. Дослідники виявили, що деякі з найбільш поширеними суфіксами у цьому контексті є *ing* та *ie*. Такі суфікси використовуються для створення нових слів, що відображають різні концепції та явища [Демченко 2019].

Наприклад, *dooring* вказує на вид дорожньої аварії, коли водій автомобіля відчиняє дверцята без перевірки безпеки і створює зіткнення з іншим учасником дорожнього руху. *Lampshading* – це одягання вільної блузки або короткої сукні з відкритими ногами і, іноді, з чоботами. *Stashing* – це практика не розповідати нікому про свої романтичні стосунки. *Surroundie* – це 360 - градусне фото, зняте спеціальною камерою. *Biohacking* – використання біологічних принципів для покращення функціонування організму. *Biobag* – пластикова торбина з особливою рідиною, яка може підтримувати життя тварини, народженої передчасно. *Micromastery* – це процес вивчення одного чи кількох малих навичок дуже добре. *Micro-influencer* – це людина з невеликою кількістю прихильників у соціальних мережах, яка впливає на покупки через продукти, про які вона пише [Демченко 2019, с. 51].

Усі ці нові слова створюються за допомогою афіксів та відображають сучасні явища та концепції.

Словоскладання – це лінгвістичний процес, за яким нові слова формуються шляхом об'єднання двох чи більше словосполучень або окремих слів. У результаті словоскладання створюються нові слова, які можуть мати унікальне значення або виражати нові концепції [Баркасі, Каленюк, Коваленко 2017, с. 64].

На сучасному етапі суспільного розвитку велике значення мають неологізми в економічній сфері, що пояснюється зростанням соціально – економічних зв'язків і міжкультурної комунікації на світовому рівні.

Одним з найбільш продуктивних способів створення слів у сучасній англійській мові є словоскладання. За допомогою цього процесу у мову увійшли такі слова, як *know-how* (технологія, експертні знання); *desktime* (час,

проведений службовцями між нарадами); *face-time* (час особистого спілкування з керівництвом, підлеглими або клієнтами, на відміну від телефонного або електронного спілкування); *just-in-time* (система поставок точно в строк); *downsizing* або *rightsizing* (оптимізація структури управління через скорочення управлінських ланок) [Архипенко 2019].

При утворенні неологізмів має місце власне словоскладання (утворення слів-комполітів), а також утворення неологізмів-словосполучень.

Власне словоскладання (утворення комполітів). Переважно таким способом утворюються іменники та прикметники.

Наприклад, утворення неологізмів-іменників може здійснюватися за такими моделями:

1. Двокомпонентні моделі:

1) $N+A$ (іменник + прикметник) : *flockdown*;

2) $N+N$ (іменник + іменник) : *foodprint, wallball, petfishing*;

3) $A+N$ (прикметник + іменник) : *overemployment, greenhushing*.

2. Трикомпонентна модель, наприклад, $N+Prep+N$ (іменник + прийменник + іменник): *cradle-to-career*.

3. Утворення неологізмів-прикметників може, наприклад, здійснюватися за моделлю $A+A$ (прикметник + прикметник), зокрема: *supercold*.

Слід зазначити, що словоскладанням утворюються переважно іменники, а інші частини мови – значно рідше. Іменники зазвичай утворюються з двох компонентів, рідше – із трьох. Найчастотнішою моделлю утворення неологізмів-іменників є $N+N$ [Квеселевич 1985].

Конверсія – це процес створення нових слів у мові, перетворюючи слова одного частини мови (зазвичай дієслова чи іменники) в інші, шляхом додавання або приглушення семантичних компонентів. Цей процес включає створення нових слів з вже існуючих, зокрема, дієслів в іменники або навпаки [Баркасі, Каленюк, Коваленко 2017, с. 33].

Конверсія виступає не лише лінгвістичним явищем, але й важливим механізмом для створення неологізмів – нових слів чи виразів, які виникають у мові для вираження нових ідей, понять або реалій. Цей процес полягає у використанні слів одної частини мови в іншій частині без суттєвої зміни їхньої форми. Модель $N \rightarrow V$ (іменник \rightarrow дієслово) є однією з найбільш продуктивних у конверсії, де іменники здатні перетворюватися у дієслова. Це дозволяє мові ефективно адаптуватися до нових концепцій та явищ, що виникають у суспільстві чи технологічному просторі.

Конверсія дозволяє мові створювати лексичні новотвори, які відповідають потребам сучасності. Вона активно використовується в таких галузях, як технології, наука, бізнес, соціальні науки та багато інших, де швидкі та точні терміни є ключовими для вираження інновацій та змін.

Специфічність конверсії полягає в її здатності до синтаксичної гнучкості. Важливим є також те, що конвертовані слова зберігають базову семантику, але набувають нового контексту та значення у новій лінгвістичній реалії.

Приклади конверсії включають слова, які перейшли від іменників до дієслів, наприклад, *to google* (пошук в Інтернеті за допомогою пошукового двигуна *Google*), *to email* (надсилати електронні листи). Ці терміни стали не лише невід'ємною частиною мовної практики, а й визначниками сучасного цифрового світу [Громовенко 2018].

У сучасній англійській мові конверсія досі є важливим засобом словотворення, особливо за моделлю дія + предмет для утворення нових іменників від дієслів. Наприклад, *leaflet* (дія – робити листівки) і *file* (дія – редагувати документи) є прикладами слів, утворених через конверсію.

Процес утворення іменників від прикметників також відбувається через конверсію. У цьому випадку, семантика слова змінюється шляхом приглушення компонента якості і додавання компонента предмет. Наприклад, *acrylic* – це приклад слова, де відбулася конверсія з прикметника до іменника, і слово означає акрил, як синтетичний матеріал. Конверсія допомагає

розширити семантичний обсяг понять і вводить нові компоненти значення в мову [Дудок 2009].

Скорочення – це процес скорочення довгих слів або фраз до більш короткої форми, яка зазвичай представлена лише початковими літерами слова чи фрази [Баркасі, Каленюк, Коваленко 2017, с. 61].

Найбільш продуктивним методом утворення політичних неологізмів у англійській мові є скорочення. Цей метод включає усічення основ (39%), як, наприклад, *corp* стає *corporation*; злиття (телескопію) (33%), таке як *Amerasian* від *American* і *Asian*; аббревіацію (28%), як *PM* від *Prime-Minister*.

Серед виділених способів скорочення, найпоширенішим є скорочення запозичених суфіксів: *member* стає *memb*.

Слова також можуть утворюватися шляхом елізії початкової або кінцевої частини слова, і ці скорочення розглядаються як усічені слова. Наприклад, *burb* від *suburb*, *vator* від *elevator*. Деякі слова, такі як *detox* від *detoxification* і *pol* від *politician*, утворилися шляхом відкидання кінцевої частини слова.

Усічені слова можуть також набувати граматичних флексій, таких як утворення множини, наприклад, *comms* від *communications* [Зацний 2015].

Один із способів створення нових слів, відомих як неологізми, полягає в використанні буквено-цифрових скорочень. За цим методом було створено ряд термінів, пов'язаних з електронною торгівлею. Наприклад, *B2B* вказує на *business-to-business* (від фірми до фірми), *B2C* – *business-to-consumer* (від фірми до споживача), *B2B2C* – *business-to-business-to-consumer* (від фірми до фірми до споживача), *C2C* – *consumer-to-consumer* (від споживача до споживача), *C2B2C* – *consumer-to-business-to-consumer* (від споживача до фірми до споживача), *B2E* – *business-to-employee* (від фірми до співробітника), *P2P* – *producer-to-producer, person-to-person* (від виробника до виробника, особисто до особисто).

Ці буквено-цифрові скорочення допомагають швидко та ефективно позначити різні види електронної торгівлі та бізнесові взаємодії, роблячи

комунікацію більш зручною та зрозумілою у цьому специфічному контексті [Архипенко 2019].

Абревіатури є важливими елементами скорочень. Вони широко використовуються для позначення термінів, назв груп, організацій і навіть осіб. Наприклад, *BCCs* відповідає *Business Communication Centres*, *AIF* – *Anti-Iraqi Forces*.

Абревіація відрізняється тим, що скорочене слово існує поруч із повним словом, від якого воно походить, і не завжди є єдиним способом позначення певного поняття. Наприклад, *EA* може вказувати на *economic advisor*, і *TA* – на *transfer agent*.

Цей процес стає все більш продуктивним завдяки збільшенню ролі синтаксичного словотворення в англійській мові, що призводить до зростання кількості абревіатур. У результаті абревіатури стають важливим інструментом для зручного та ефективного спілкування в різних галузях життя [Громенко 2018, с. 236].

Це лише декілька прикладів способів творення нових слів у мові. Різноманітність цих методів відображає різні аспекти культури, технології, науки та інших сфер життя, які знаходять своє відображення у словах і термінах мови.

Лінгвісти часто класифікують неологізм за ступенем його використання в одній мові. Новонароджене слово спочатку нестабільне, і важко здогадатися, чи закріпиться воно, і в кінцевому підсумку, чи стане воно словом, яке більшість людей знають і використовують. Дифузний неологізм означає, що багато людей використовують слово, але воно ще не має офіційного визнання як слово, і в остаточному підсумку, якщо слово залишається популярним, воно може досягти стабільного статусу. Воно стає частиною мови і, ймовірно, визначається в словниках.

Вивчення нового словника в функціональному аспекті передбачає аналіз того, як з'являються неологізми, і цей аналіз встановлює етап переходу до

прагматичного аспекту нових слів. За способом формування неологізми поділяються на:

1) фонологічні неологізми, які формуються з окремих звуків (наприклад, *zizz, to whee*);

2) запозичення – це сильні неологізми, які відрізняються фонетичним розподілом, не характерним для англійської мови, а також незвичайним морфологічним поділом та відсутністю вмотивованості (наприклад, *cinematheque, anti-roman* (з французької));

3) морфологічні неологізми, сформовані зразками, що існують в системі мови, і представленими в системі мови морфемами (такі регулярні дериваційні процеси, як афіксація, перетворення, словоскладання та менш регулярні, такі як скорочення, лексикалізація).

Окрім того неологізми можна розділити на [Мойсієнко 2014]:

1) корінні слова (наприклад, *jeep – a small light motor vehicle, zebra is street crossing place* тощо);

2) похідні слова (наприклад, *collaborationist – one in occupied territory works helpfully with the enemy, to accessorize – to provide with dress accessories*);

3) складні слова (наприклад, *microfilm – a reader*).

Отже, існує багато класифікацій неологізмів за їх особливостями.

У багатьох галузях науки і техніки, так само, як і сфері побутового спілкування неологізми зустрічаються дуже часто через їх здатність і силу інформаційної конденсації та їх експресивного ефекту [Моїсеєва 2011, с. 124].

Отже, вивчення структурно-семантичних особливостей творення нових слів в англійській мові має велике практичне і теоретичне значення. Це дослідження відкриває перед нами багатий світ лінгвістичних інновацій, які є відповіддю на зміни в суспільстві, технології та культурі.

Дослідження створення нових слів в англійській мові є лише однією складовою загального вивчення мови та лінгвістики. Проте ця складова має велике значення для розвитку мовознавства та наукового розуміння процесів, які формують мову та її роль у сучасному суспільстві.

РОЗДІЛ 2

КОМП'ЮТЕРНІ ЗЛОЧИНИ ЯК СУСПІЛЬНО-ПОЛІТИЧНЕ ЯВИЩЕ 21 СТОЛІТТЯ

2.1 Різновиди комп'ютерних злочинів

З поширенням нових технологій в повсякденному житті, коли обмін інформацією став швидким, доступним і продуктивним, злочинність в сфері інформації перейшла за межі тих звичайних кримінальних вчинків, які зазвичай визначають злочинність.

Нові інформаційні технології не лише надали унікальні можливості для активного та ефективного розвитку економіки, політики, держави і суспільства, але й спричинили виникнення негативних явищ.

Одним з таких негативних процесів є поширення комп'ютерної злочинності. На появу сприяє постійний ріст користувачів персональних комп'ютерів і мережі Інтернет, що в свою чергу призводить до нових негативних явищ, таких як атаки хакерів на веб-ресурси, Інтернет-шахрайство, поширення комп'ютерних вірусів і спаму, а також проблеми, пов'язані з дитячою порнографією та кібертероризмом [Столбов 2010].

Комп'ютерні злочини – це правопорушення, які виконуються або спрямовані на комп'ютери, мережі, інформацію та дані, що зберігаються в електронному форматі.

Комп'ютерні злочини можна умовно розділити на дві основні категорії:

1. злочини, які пов'язані з втручанням у роботу комп'ютерів;
2. злочини, де комп'ютери використовуються як необхідні технічні засоби.

Сьогодні з поширенням персональних комп'ютерів з'явилися програми-віруси, які самостійно поширюються і завдають завдання комп'ютерам. Вони

можуть пошкодити файловою структурою дисків та завдати шкоду інформації, збереженій на комп'ютері. Навіть при прийнятті законів щодо боротьби з комп'ютерною злочинністю та розробці програмного забезпечення для захисту від вірусів у багатьох країнах, кількість нових програм-вірусів постійно зростає [Кундеус 2020, с. 44-45].

Характерною особливістю комп'ютерних злочинів є їх висока латентність та великі розміри завданих збитків. Інформація про такі злочини не завжди стає загальновідомою, як свідчать наукові дослідження. Лише 10-15% комп'ютерних злочинів стають об'єктом публічної уваги, оскільки постраждалі організації, утримуючись від розголошення інформації через страх втрати репутації або можливого повторення атак, неохоче діляться даними про подібні неправомірні дії.

Таким чином, повна картина комп'ютерної злочинності залишається невідомою для світу. Зрозуміло, що державні та комерційні структури, які стали об'єктом атак, не ретельно афішують наслідки інцидентів та «ефективність» своїх систем захисту. Навіть ті факти, які стають відомими, залишають сильне враження [Столбов 2010].

Важливо відзначити, що питання визначення кіберзлочинності та заходів її протидії, хоч і мають свої правові визначення, залишаються несуттєвими. У той же час, концепції кібервійни, правила її проведення, кібератаки та відповідальність за такі дії лишаються поза областю регулювання міжнародного права. Наукове вивчення кібервійни, як самостійного явища, залишається недостатньо розвиненим у вітчизняній доктрині, навіть при наявності деяких прикладних досліджень вчених. Це може бути зумовлено різними факторами, такими як відсутність чітких меж об'єкта дослідження, застарілі методи збору та аналізу емпіричних даних, ігнорування результатів досліджень вчених з розвинених країн, зокрема з Європи та США. У зв'язку з цим сутність кібервійни спотворюється та спрощується до розуміння як комп'ютерних злочинів [Дикий 2022, с. 493].

На даний момент найбільш поширеною класифікацією кіберзлочинів є та, яка базується на структурі Конвенції Ради Європи про кіберзлочинність від 23 листопада 2001 року. Згідно цієї конвенції існують чотири основні групи кіберзлочинів:

1. **Порушення конфіденційності, цілісності та доступності комп'ютерних даних і систем:** Ця група включає в себе такі правопорушення, як незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему та зловживання пристроями;

2. **Правопорушення, пов'язані з комп'ютерами:** Сюди входять підробка та шахрайство, пов'язані з комп'ютерами;

3. **Правопорушення, пов'язані зі змістом:** Ця група охоплює правопорушення, пов'язані з дитячою порнографією;

4. **Правопорушення, пов'язані з порушенням авторських та суміжних прав:** Сюди включаються правопорушення, які стосуються порушення авторських та суміжних прав [Лісайчук 2014].

Також комп'ютерні злочини можуть бути класифіковані за допомогою кодифікатора Генерального Секретаріату Інтерполу. Цей кодифікатор включає різні види комп'ютерних злочинів і надає їм ідентифікатори, які починаються з букви Q. За цим кодифікатором можуть використовуватися до п'яти кодів для опису злочину, розташованих у порядку їх важливості:

1. **QA – несанкціонований доступ і перехоплення:** Це включає в себе незаконний доступ до комп'ютерної системи та перехоплення інформації;

2. **QD – зміна комп'ютерних даних:** Ця категорія стосується змін у комп'ютерних даних без належного дозволу;

3. **QF – комп'ютерне шахрайство:** Включає в себе шахрайство, пов'язане з комп'ютерами, таке як шахрайство з банкоматами та платіжними засобами;

4. **QR – незаконне копіювання:** Це стосується незаконного копіювання програмного забезпечення та іншої інформації;

5. QS – комп'ютерний саботаж: Ця категорія включає в себе дії, спрямовані на саботаж комп'ютерних систем, як з апаратним, так і з програмним забезпеченням;

6. QZ – інші комп'ютерні злочини: В цю категорію входять різні інші види комп'ютерних злочинів, такі як використання комп'ютерних дощок оголошень, розкрадання комерційних таємниць, передача конфіденційної інформації та інші [Лісайчук 2014, с. 145].

Ця класифікація допомагає органам правопорядку і спеціалістам з кібербезпеки легше ідентифікувати та класифікувати різні види кіберзлочинів, що відповідає міжнародним стандартам і сприяє боротьбі з цими злочинами.

Зі збільшенням користувачів Інтернету зростає ризик у сфері кібербезпеки. Збільшена залежність суспільства від інформаційних технологій призводить до його вразливості перед різноманітними інформаційними загрозами. Розширюється можливість використання мережі для злочинів, і збільшується потенційна загроза стати жертвою зловживання інформаційними технологіями для злочинних цілей.

Особливість полягає в тому, що вчинення злочину не вимагає значних зусиль і витрат. Достатньо мати комп'ютер, програмне забезпечення та підключення до мережі. Навіть глибокі технічні знання не є обов'язковими, оскільки існують спеціальні форуми, де можна придбати програмне забезпечення для здійснення злочинів, отримати вкрадені номери кредитних карт та особисті дані користувачів, а також скористатися послугами для здійснення електронних крадіжок і вторгнень в комп'ютерні системи [Лісайчук 2014, с. 146].

Описуючи особу комп'ютерного злочинця, слід відзначити його основну характеристику – в широкий спектр електронної злочинності втягнуті різні особи, від висококваліфікованих фахівців до аматорів. Злочинці походять з різних сфер життя і мають різний рівень підготовки.

Для протидії цьому новому виду злочинів необхідно дослідження цієї проблеми та аналіз криміналістичних та психологічних особливостей

кіберзлочинців. Вітчизняні та зарубіжні дослідження дозволяють створити портрет типового комп'ютерного злодія, а саме відповідний профіль даного соціального типу.

Створення бази типових моделей різних категорій злочинців та вивчення загальних рис їхньої особистості дозволяє оптимізувати процес виявлення осіб, серед яких ймовірно можна шукати злочинця [Біленчук 2011].

Практика свідчить, що особливу категорію комп'ютерних злочинців складають хакери, розглянемо їх більш детально.

Поява комп'ютерної злочинності в суспільстві великою мірою пов'язана з діяльністю так званих «хакерів». Це користувачі обчислювальних систем і комп'ютерних мереж, які займаються пошуком незаконних методів отримання несанкціонованого доступу до комп'ютерних ресурсів та їх несанкціоноване використання з особистою корисливою метою.

Хакери визначаються за метою та сферою своєї злочинної діяльності. Вони можуть бути розділені на кілька підгруп:

1. Хакери (*hacker*): Здійснюють вторгнення та вивчення великих ЕОМ за допомогою телефонних ліній та комп'ютерних мереж. Це комп'ютерні хулігани, які проникають в чужі інформаційні мережі для задоволення та влади над системою, а не завдання шкоди.

2. Крекери (*cracker*): Серйозні порушники, здатні спричинити шкоду системі, викрадаючи інформацію та використовуючи її несанкціоновано.

3. Фрікери (*phreak*): Спеціалізуються на використанні телефонних систем для уникнення оплати телекомунікаційних послуг та подолання труднощів технічного плану.

4. Колекціонери (*codes kids*): Збирають та використовують програми для перехоплення паролів та іншої інформації.

5. Кіберплути (*cybercrooks*): Спеціалізуються на крадіжці грошей та конфіденційної інформації для подальшої продажу.

6. Торгаші або пірати (*wares dudes*): Займаються збиранням та торгівлею піратським програмним забезпеченням.

Ці групи визначаються їхніми метами та технічними можливостями, а їх діяльність відображає різноманіття комп'ютерних злочинів у сфері інформаційних технологій [Біленчук 2011].

У світі стрімкого розвитку інформаційних технологій та високої активності в електронному просторі, термінологія пов'язана з комп'ютерними злочинами постійно еволюціонує. Нові явища та поняття в цій галузі визначаються та описуються через використання неологізмів, що є новоствореними словами чи фразами. Ці терміни стають важливим інструментом для розуміння та аналізу найсучасніших тенденцій у кібербезпеці та віртуальній кримінальній діяльності.

У цьому контексті, важливо розглянути неологізми, пов'язані з різновидами комп'ютерних злочинів, для більшого розуміння і виявлення сучасних викликів, що стоять перед суспільством у цифровій епохі. Серед таких термінів можна виділити:

- *Cyberheist* – вчинення злочинів, таких як крадіжка, шахрайство чи вимагання в області кіберпростору (словоскладання);
- *Cyber Extortion* – вимагання грошей або послуг з загрозою розкриття конфіденційної інформації або завдання шкоди системам (словоскладання);
- *Electronic Espionage* – використання програмного забезпечення для незаконного збору конфіденційної інформації (афіксація);
- *Computer Destabilization* – створення та використання вірусів для знищення або пошкодження комп'ютерних систем (словоскладання);
- *Electronic Robbery* – вчинення крадіжок або ограблень за допомогою електронних засобів, таких як хакінг або фішинг (афіксація);
- *Network Terrorism* – використання інтернет-технологій для вчинення актів тероризму або дестабілізації суспільства (скорочення);
- *Cybercriminality* – взламання, крадіжка інформації чи завдання шкоди за допомогою комп'ютерних технологій (словоскладання);
- *Virtual Kidnapping* – захоплення електронних акаунтів чи ідентичності для вчинення злочинів (афіксація);

- *Cyberdiscrimination* – дискримінація осіб в електронному середовищі (словоскладання) [Крамар 2022; Longman Dictionary Online; WordSense Dictionary Online].

Терміни *cybercrime, hackers, computer intrusion, and theft of machine time* вже не є чимось екзотичним для юристів. Проблеми боротьби з злочинами, пов'язаними з використанням комп'ютерної техніки, активно обговорюються серед вчених, і швидко розвивається практика застосування відповідних норм законодавства, що регулюють кримінальну відповідальність у цій галузі.

На сьогодні комп'ютерні злочини є однією з найдинамічніших груп суспільно небезпечних злочинів. Показники поширення цих злочинів стрімко зростають, і їх суспільна небезпечність постійно зростає.

Попередження та протидія комп'ютерним злочинам є важливими завданнями в умовах сучасного цифрового суспільства. Можна виділити декілька ключових аспектів у цьому контексті:

1. **Захист інформації:** Забезпечення надійного захисту конфіденційної інформації, яка зберігається на комп'ютерних системах. Це включає в себе використання сучасних методів шифрування, механізмів аутентифікації та контролю доступу.

2. **Оновлення програмного забезпечення:** Регулярне оновлення програм та операційних систем для заповнення вразливостей і усунення можливих точок доступу для зловмисників.

3. **Інформаційна гігієна:** Підвищення обізнаності користувачів щодо безпеки в Інтернеті. Сприяння використанню складних паролів, обізнаність з соціальною інженерією та іншими методами атак.

4. **Захист від фішингу:** Розробка та впровадження заходів для виявлення та уникнення фішингових атак, які можуть використовуватися для отримання конфіденційної інформації.

5. **Мережева безпека:** Захист мережевої інфраструктури від несанкціонованого доступу, включаючи використання мережевих брандмауерів, антивірусного програмного забезпечення та інших заходів.

6. Кіберзахист організацій: Розробка та впровадження комплексних стратегій кіберзахисту для організацій, включаючи моніторинг, реагування на інциденти та відновлення після атаки.

7. Міжнародне співробітництво: Зміцнення міжнародного співробітництва для обміну інформацією про загрози та спільних заходів з протидії кіберзлочинності.

8. Інновації в кіберзахисті: Сприяння дослідженням та розробкам нових технологій у сфері кіберзахисту для вдосконалення систем та заходів протидії [Ніколаюк, Никифорчук, Томма, Барко 2006].

Отже, кіберзлочини є серйозною загрозою сучасному інформаційному суспільству, і вони вимагають постійного удосконалення законодавства, заходів з кібербезпеки та співпраці між правоохоронними органами та технічними експертами. Попередження та протидія комп'ютерним злочинам є важливими завданнями в умовах сучасного цифрового суспільства. Можна виділити декілька ключових аспектів у цьому контексті: захист інформації, оновлення програмного забезпечення, інформаційна гігієна, захист від фішингу, мережева безпека, кіберзахист організацій, міжнародне співробітництво, інновації в кіберзахисті.

2.2 Комп'ютерні злочини пов'язані з суспільством

Показником розвитку суспільства в сучасному світі стає не лише доступ до інформації, але й ефективний захист конфіденційної інформації. У XXI столітті, коли інформаційні технології проникають у всі сфери нашого життя, національна безпека стає нерозривною від інформаційної безпеки. Це визначає стабільність суспільства, забезпечення прав і свобод громадян, а також збереження правопорядку.

Споживачі стають все більше зацікавленими в цих питаннях, оскільки кожен власник або користувач комп'ютера може потенційно стати жертвою, очікуючи серйозних наслідків у випадку вчинення злочину. Це особливо актуально в комерційному та промисловому секторах, де можуть виникнути значні фінансові втрати.

Комп'ютерні злочинці використовують міжнародні комп'ютерні мережі, такі як Інтернет, для поширення свого кримінального досвіду, ігноруючи національні кордони. Це вимагає співпраці з боку поліцейських органів для ефективного протидії цьому виду злочинів. Одним із необхідних елементів є оперативний обмін інформацією про комп'ютерні злочини [Біленчук 2011].

Одним із основних мотивів комп'ютерних злочинів у суспільстві вважаються корисливість і бажання демонструвати власний професіоналізм через так званій «інтелектуальний виклик». Згідно з більшістю експертів, комплекс причин та умов, що призводять до комп'ютерної злочинності, включає такі фактори:

- складнощі працевлаштування високоінтелектуальної частини населення;
- пов'язаної з науковою діяльністю, технологіями, обороною тощо;
- безробіття серед інтелектуальної еліти суспільства;
- можливість швидкого збагачення через комп'ютерні розкрадання з невеликою ймовірністю викриття, враховуючи високу латентність цих злочинів;
- недостатня захищеність автоматизованих систем обробки даних;
- відставання технічної оснащеності та професіоналізму співробітників правоохоронних органів від дій професійних комп'ютерних злочинців;
- відсутність узагальненої практики розслідування комп'ютерних злочинів в судовій системі;
- лояльне ставлення суспільства до цього виду злочинності, оскільки вона часто використовується особами для інтелектуального збагачення тощо [Борзенков, Комісаров 2012].

Комп'ютерні злочини пов'язані з суспільством можуть виявлятися у різних формах, включаючи порушення приватності, шахрайство, кібертероризм та інші аспекти. Ось деякі типові види комп'ютерних злочинів, які взаємодіють із суспільством:

1. Шахрайство в інтернеті:

- фішинг (*phishing*): злочинці використовують підроблені веб-сайти та електронні листи для витягання особистої інформації від користувачів, такою як паролі, номери кредитних карт і т.д;

- онлайн-шахрайства (*online scams*): махінації з електронними товарами, аукціонами чи іншими онлайн-платформами для отримання незаслужених вигод.

2. Ідентифікаційна крадіжка (*identity theft*):

- незаконний доступ до особистої інформації: здобуття доступу до особистих даних з метою вчинення шахрайства або інших злочинних дій.

3. Розповсюдження дезінформації та фейків:

- кіберпропаганда (*cyber propaganda*): розповсюдження неправдивої інформації або маніпулювання соціальними мережами для впливу на громадську думку.

4. Кібертероризм (*cyber terrorism*):

- атаки на критичну інфраструктуру: злочинці можуть спробувати атакувати енергетичні системи, мережі зв'язку або інші важливі інфраструктурні об'єкти з метою завдання шкоди суспільству.

5. Ексторшн та блокування даних (*ransomware*):

- шифрування даних: зловмисники шифрують дані користувачів та вимагають викуп за їх розшифрування.

6. Крадіжка інтелектуальної власності (*theft of intellectual property*):

- вторгнення в системи компаній: Здобуття несанкціонованого доступу до конфіденційних даних та технологічних розробок.

7. Кібербулінг та онлайн-зловживання:

- онлайн-здавання (*online distribution*): зловмисники використовують інтернет для поширення ганьбливої інформації або загроз в сторону осіб чи груп.

8. Кібердомаганство (*cyberbullying*):

- спроби вплинути на виборчі процеси: атаки на системи голосування чи розповсюдження дезінформації під час виборчих кампаній.

9. Торгівля людьми та дитяча порнографія (*Human trafficking and child pornography*):

- використання інтернету для реклами та обміну матеріалами порнографічного чи експлуатаційного характеру.

10. соціальний інжиніринг (*social engineering*):

- маніпулювання відомостями користувачів: зловмисники використовують техніки психологічного впливу для отримання конфіденційної інформації.

Ці види комп'ютерних злочинів можуть мають значний вплив на суспільство, порушуючи приватність, піддаючи ризику безпеку та економічні інтереси громадян, а також загрожуючи стабільності та нормальному функціонуванню суспільства в цілому [Самойленко 2020, с. 8].

Комп'ютерні злочини можуть призводити до різноманітних наслідків для суспільства, таких як фінансові втрати, втрати особистих даних, емоційне страждання та пошкодження репутації. Крім того, кіберзлочини можуть викликати серйозні психологічні наслідки, такі як депресія, збентеження та тривога [Ісмайлов 2017].

Злочинність в кіберпросторі, особливо якщо вона проявляється у формі організованих груп, створює значні проблеми для суспільства. Дослідження в різних країнах вказують на те, що комп'ютерні злочини, вчинені організованими угрупованнями, найбільше привертають увагу та викликають негативний резонанс. Особливо актуально це питання в США, де інтенсивна комп'ютеризація та інформатизація сприяли формуванню критичної маси інформації про загрози комп'ютерної злочинності.

США визначаються як країна, де виникла масова комп'ютеризація, і, зрозуміло, вона має значний запас соціальної інформації про наслідки комп'ютерних злочинів для суспільства. Питання щодо того, чому у США так відкрито та широко обговорюється комп'ютерна злочинність, може бути пояснене тим, що саме тут виникла інформаційна культура та усвідомлення загроз, пов'язаних із зловживанням комп'ютерами.

Ментальність американського суспільства передбачає розуміння того, що колективне обговорення може допомогти виробити ефективні стратегії подолання суспільних проблем та зменшити негативний вплив комп'ютерних злочинів на інформаційне суспільство [Цимбалюк 2011, с. 209-210].

Роль громадян у спільній боротьбі з кіберзлочинами в сучасному інформаційному суспільстві виявляється критичною для ефективного протидії цьому складному виклику. Глобальний характер кіберзагроз вимагає активного внеску індивідів у формування безпечного кіберпростору та захисту цифрової інфраструктури.

Перш за все, громадяни грають ключову роль у власній кібербезпеці, розуміючи основні принципи та ризики, пов'язані з використанням інтернету. Самосвідомість щодо методів атак, які використовуються кіберзлочинцями, дозволяє громадянам уникати потенційно небезпечних ситуацій, будучи більш обізнаними про те, як захищати свої особисті дані та інформаційні ресурси.

Важливою частиною ролі громадян є прийняття відповідальності за свої дії в онлайн-середовищі та захист власної інформації. Створення сильних паролів, регулярна зміна паролів, а також обережне використання особистих даних у соціальних мережах — це лише деякі засоби, які може використовувати громадянин для зниження ймовірності потрапляння під вплив кіберзлочинців.

Громадяни також можуть відігравати активну роль у виявленні кіберзагроз та повідомленні відповідних інстанцій. Спостереження за незвичайною активністю в електронних облікових записах, підозрілими

повідомленнями чи спробами атак може сприяти ранньому виявленню та запобіганню кіберзлочинам [Веселова 2021, с. 18].

Швидкі темпи технологічного розвитку призводять до появи нових явищ, які вимагають нових термінів та визначень для їхнього належного опису.

Такі неологізми, пов'язані з комп'ютерною злочинністю в контексті суспільства, можуть включати терміни, що визначають нові види атак:

- *synthetic identity theft (SIT)* – створення нового, інтернет-заснованого ідентифікатора, використовуючи комбінацію реальних та вигаданих персональних даних для уникнення виявлення (скорочення);

- *AI-driven phishing* – використання штучного інтелекту для персоналізації та ускладнення атаки перехоплення конфіденційної інформації (телескопія);

- *cryptojacking* – використання комп'ютерів або мобільних пристроїв для таємного майнінгу криптовалют без належного повідомлення власників (словоскладання);

- *distributed denial of wallet (DDoW)* – атака, спрямована на криптовалютні гаманці, з метою блокування доступу до них (конверсія);

- *e-skimming* – крадіжка фінансової інформації під час онлайн-платежів або покупок шляхом враження шкідливого коду на веб-сайтах (словоскладання);

- *rogue software updates* – розповсюдження фальшивих програмних оновлень для внедрення шкідливого коду чи вразливостей (телескопія);

- *smart contract manipulation* – використання вразливостей в розумних контрактах блокчейну для втручання та зміни їхньої логіки (телескопія);

- *AI-powered evasion* – використання штучного інтелекту для уникнення виявлення та обхід заходів кібербезпеки (телескопія);

- *typosquatting attacks* – створення доменних імен, подібних до відомих, з метою введення користувачів у спокусу та отримання їхніх особистих даних (словоскладання) [Зацний 2022; Крамар 2022; Cambridge Dictionary Online].

У подальшому методи вразливості в цифровому середовищі:

- *zero-click exploits* – використання вразливостей у програмному забезпеченні чи операційних системах без потреби в будь-якому взаємодії користувача (телескопія);

- *side-channel attacks* – використання побічних каналів комунікації, таких як електромагнітні випромінювання або час виконання, для отримання конфіденційної інформації (телескопія);

- *binary planting (DLL hijacking)* – використання вразливостей в системах завантаження програм для запуску шкідливого коду (словоскладання);

- *DNS spoofing (pharming)* – перенаправлення користувачів на фальшиві веб-сайти за допомогою впливу на систему доменних імен (телескопія);

- *bluejacking* – надсилання непроханих *Bluetooth*-повідомлень або файлів для отримання несанкціонованого доступу до пристроїв (словоскладання);

- *rowhammer attack* – використання фізичного впливу на пам'ять для зміни бітів і викликання вразливостей у віртуальних оточеннях (телескопія);

- *watering hole attacks* – атаки на відвідувачів конкретних веб-сайтів, які вони зазвичай використовують, для введення шкідливого коду на їхні пристрої (телескопія);

- *USB harpoon (juice jacking)* – використання зловмисного пристрою USB, підключеного до зарядного порту, для крадіжки даних або введення шкідливого коду (телескопія);

- *credential stuffing* – використання викрадених облікових даних для незаконного доступу до різних облікових записів користувачів (телескопія);

- *fault injection attacks* – введення помилок або порушень у роботу системи з метою викликати вразливості та отримання несанкціонованого доступу (телескопія) [Зацний 2022; Meriam Webster Dictionary; WordSense Dictionary Online].

Або навіть поняття, пов'язані з соціальними аспектами кіберзлочинів:

- *catfishing* – використання фальшивого профілю в соціальних мережах для намагання обману чи створення фіктивного онлайн-ідентитету (телескопія);

- *sextortion* – вимагання грошей або інших послуг за допомогою загрози розкриття особистих або компрометуючих матеріалів (словоскладання);
 - *online impersonation* – незаконне використання чужого ім'я чи ідентифікаційних даних для створення фальшивого враження про особу (телескопія);
 - *revenge porn* – розповсюдження інтимних фото чи відео без згоди особи на зображенні, з метою нанесення шкоди чи морального тиску (словоскладання);
 - *phishing for trust* – використання довіри користувачів до впливу на їхні емоції та отримання особистої інформації (телескопія);
 - *social engineering attacks* – використання психологічних маніпуляцій для отримання конфіденційної інформації або здійснення несанкціонованих дій (телескопія);
 - *cyberbullying* – використання електронних засобів для систематичного та агресивного задирати, турбувати або ображати інших людей у віртуальному просторі (словоскладання);
 - *deepfake manipulation* – створення фальшивих відеоматеріалів з використанням штучного інтелекту для розповсюдження дезінформації (телескопія);
 - *online harassment* – неприємні та ворожі дії в Інтернеті, спрямовані на створення негативного впливу на особу чи групу осіб (телескопія);
 - *cyberstalking* – систематичне слідкування та переслідування особистостей в Інтернеті з метою викликання страху чи тривоги (телескопія)
- [Крамар 2022; Longman Online Dictionary].

Терміни, такі як *cyberbullying*, *social engineering*, *phishing*, *cyber diversion* та інші, є прикладами неологізмів, які відображають нові реалії сучасного інтернет-середовища та комп'ютерних технологій [Urban Online Dictionary].

Такі терміни не лише відображають технічні аспекти комп'ютерних злочинів, але також віддзеркалюють соціокультурні та етичні виміри цих явищ. Неологізми у цій сфері слугують не лише інструментом для точного

вираження нових понять, а й свідчать про постійну еволюцію сучасного мовлення в контексті розвитку кіберпростору та супутніх йому явищ.

Отже, зростання комп'ютеризації та використання цифрових технологій в суспільному житті призводять до нових викликів, і комп'ютерні злочини стають неодмінною частиною цього розвитку.

Розглядаючи неологізми, пов'язані з комп'ютерною злочинністю, можна відзначити, що вони відображають не лише технічні аспекти цих явищ, але також їхні соціокультурні та етичні виміри. Це свідчить про необхідність адаптації мовного апарату до постійно змінюючихся реалій сучасного інтернет-середовища.

Зростаюча кількість кіберзлочинів та їхній вплив на особисту безпеку та соціальні структури наголошують на необхідності співпраці між суспільством, владою та технічними експертами для розробки та впровадження ефективних заходів боротьби з цим явищем.

Отже, маємо зробити висновки, що комп'ютерні злочини пов'язані з суспільством можуть виявлятися у різних формах, включаючи порушення приватності, шахрайство, кібертероризм та інші аспекти. Наступні неологізми, пов'язані з комп'ютерною злочинністю в контексті суспільства, можуть включати терміни, що визначають нові види атак: *synthetic identity theft (SIT)*, *AI-driven phishing*, *cryptojacking*, *distributed ddniel of wallet (DDoW)*, *e-skimming*, *rogue software updates*, *smart contract manipulation*, *AI-powered evasion*, *typosquatting attacks*, *zero-click exploits*, *side-channel attacks*, *binary planting (DLL hijacking)*, *DNS spoofing (pharming)*, *bluejacking*. Загалом нами було опрацьовано 30 неологізмів, пов'язаних з комп'ютерною злочинністю в контексті суспільства.

2.3 Комп'ютерні злочини пов'язані з економікою

Дослідження способів вчинення економічних транснаціональних злочинів, які використовують сучасні комп'ютерні технології, представляє собою недостатньо вивчену галузь в криміналістичній методології. Це через те, що більшість дослідників відокремлює методи вчинення економічних злочинів від методів комп'ютерних злочинів. Також вважається, що класифікація способів вчинення досліджуваних транснаціональних злочинів постійно потребує удосконалення через зміну існуючих методів відповідно до сучасного стану розвитку комп'ютерних технологій.

Однією з ключових особливостей способів скоєння економічних транснаціональних злочинів з використанням сучасних комп'ютерних технологій є їх комплексний характер. Це виявляється в тому, що основний злочин спрямований на порушення нормальної економічної діяльності, яка відповідає інтересам держави, громадян, фінансів та торгівлі. У той же час, підпорядкований злочин направлений на вчинення проти засобів комп'ютерної техніки.

Всі наведені методи вчинення злочинів, пов'язаних із незаконним доступом до комп'ютерної мережі, можуть поєднуватися між собою в різноманітних варіаціях. Отже, незважаючи на різноманіття економічних транснаціональних злочинів, вчинених з використанням комп'ютерних технологій, практично всі методи мають свої індивідуальні особливості.

Згідно з цим, пропонується такий поділ способів неправомірного доступу до комп'ютерної мережі в рамках економічних транснаціональних злочинів, здійснених із застосуванням сучасних комп'ютерних технологій:

1. Вчинення з використанням комп'ютерних технологій і відповідної техніки (*actions using computer technologies and related equipment*) економічних злочинів, включаючи порушення, спрямовані на незаконне привласнення або пошкодження самої цієї техніки;

2. Незаконне отримання товарів та послуг (*illegal acquisition of goods and services*);
3. Несанкціоноване перехоплення інформації (*unauthorized interception of information*);
4. Неправомірний доступ до комп'ютерної інформації суб'єктів (*illegal access to computer information of subjects*) господарювання та її розкрадання, включаючи атаки на комп'ютерну інформацію на серверах глобальної комп'ютерної мережі (*attacks on computer information on servers of the global computer network*) та інформацію в апаратних засобах некомп'ютерного типу;
5. Розкрадання, пов'язане з переказом електронної готівки (*theft associated with the transfer of electronic cash*);
6. Шахрайство в сфері електронної торгівлі та інвестування (*fraud in the field of electronic trade and investment*);
7. Електронні способи легалізації злочинних доходів (*electronic methods of legalization of criminal income*);
8. Ухилення від оподаткування (*tax evasion*).

Хочемо звернути увагу на те, що видалення, блокування, зміна та копіювання комп'ютерної інформації не виключає можливість вчинення конкретних самостійних дій. Іншими словами, несанкціонований доступ до інформації не лише представляє собою самостійний злочин, але також може бути підготовчим етапом для здійснення інших неправомірних дій.

Ця класифікація способів неправомірного доступу до комп'ютерної мережі не є вичерпною, що пояснюється швидким розвитком інформаційної сфери та комп'ютерних технологій [Завидняк 2021, с. 93].

Наведена класифікація методів неправомірного доступу до комп'ютерної мережі не є вичерпною, оскільки інформаційна сфера та комп'ютерні технології стрімко розвиваються. В цілому ці методи можна поділити на три групи в залежності від форми контакту з комп'ютерною технікою.

1. Методи безпосереднього впливу на комп'ютерну інформацію. Це включає видачу відповідних команд з комп'ютера, на якому знаходиться інформація, що може призвести до проникнення в закриті зони приміщення для обробки інформації. Такі атаки зазвичай залишають сліди тільки в комп'ютерній системі, де зберігається цільова інформація.

2. Методи опосередкованого (віддаленого) доступу до комп'ютера та інформації. Це включає проникнення в інформаційні мережі через автоматичний перебір абонентських номерів, використання паролів, підключення до ліній зв'язку законного користувача та використання шкідливих програм для віддаленого доступу.

3. Змішані методи, які можуть використовувати як безпосередній, так і віддалений контакт з комп'ютерною технікою. Це може включати несанкціоноване введення команд до програм, протиправну зміну програм, протиправний доступ до баз даних через слабкі місця в системах захисту та використання помилок логіки побудови програм.

Ці методи можуть бути використані як особами з правом доступу, так і особами, що спеціально проникають у зони обмеженого доступу. Також важливо враховувати, що розвиток технологій може призводити до нових методів інформаційних атак [Завидняк 2021, с. 93].

Кіберзлочинність має суттєвий вплив на економіку. Один успішний кіберзлочин може спричинити фінансові втрати і крадіжку інтелектуальної власності. Експерти, які вивчають боротьбу з комп'ютерною злочинністю в правоохоронних органах країн Центральної та Східної Європи, наголошують, що прибутки від злочинної діяльності у сфері використання комп'ютерно-обчислювальних машин займають третє місце за доходами, випереджаючи навіть виручку від наркоторгівлі та торгівлі зброєю. Масштабні збитки вже на даний момент оцінюються на мільярди доларів. Щорічно лише в Сполучених Штатах економічні втрати від цього типу злочинності становлять приблизно 100 мільярдів доларів [Столбов 2010, с. 158].

В сукупності, як суспільство, ми щороку втрачаємо мільярди доларів через кіберзлочинність. У 2020 році світова економіка зазнала збитків на суму 945 мільярдів доларів внаслідок кіберзлочинності, і ця цифра очікується продовжувати зростати. Кіберзлочинність приносить значно більше доходів, ніж незаконний обіг наркотиків, контрафакція та торгівля людьми взяті разом. За оцінками, у 2023 році кіберзлочинність може скласти 8 трильйонів доларів США, а до 2025 року вона може досягти приблизно 10,5 трильйона доларів [Буров 2021].

Захист банківських систем та фінансових даних є необхідним завданням у світлі зростаючої кількості та складності кіберзагроз, які спрямовані на фінансовий сектор. Ефективний захист вимагає інтегрованого підходу, охоплюючи технічні, організаційні та правові аспекти. Одним із ключових елементів є впровадження сучасних систем аутентифікації та авторизації.

Спочатку, важливо встановити механізми сильної аутентифікації, такі як двофакторна аутентифікація та біометричні методи, для обмеження несанкціонованого доступу. Це важливо не лише для захисту самої банківської системи, але й для запобігання неправомірному доступу до фінансових даних клієнтів.

Шифрування даних є іншим ключовим елементом у захисті фінансової інформації. Всі чутливі дані повинні бути ефективно зашифровані як під час зберігання, так і під час передачі. Це надає додатковий шар безпеки та гарантує конфіденційність фінансової інформації.

Регулярне оновлення програмного та апаратного забезпечення є також невід'ємною частиною стратегії захисту. Використання останніх версій операційних систем, антивірусного програмного забезпечення та інших важливих компонентів допомагає усунути вразливості та запобігати використанню застарілих методів атак [Нестяк 2013, с. 94].

Окрім технічних заходів, важливо покласти акцент на обладнання персоналу навичками та знаннями щодо кібербезпеки. Регулярні тренінги з питань виявлення соціально-інженерних атак та фішингових спроб

допомагають персоналу бути більш осведомленим та реагувати ефективно на потенційні загрози.

Крім того, створення та підтримка центрів моніторингу для постійного виявлення аномалій та реагування на них є невід'ємним елементом стратегії захисту. Ці центри надають можливість вчасно реагувати на потенційні загрози та вживати необхідні заходи [Нестяк 2013, с. 103].

Загалом, використання інтегрованого підходу, що поєднує технічні, організаційні та навчальні заходи, є важливим компонентом захисту банківських систем та фінансових даних від кіберзлочинів. Прийняття цих заходів дозволить забезпечити стійкість та надійність фінансових інститутів в умовах непередбачуваної кіберсередовища.

У світі швидкого технологічного розвитку та постійної еволюції фінансових систем виникають нові терміни, які описують сучасні комп'ютерні злочини, пов'язані з економікою. Одним із таких понять є *cryptofraud* (криптошахрайство), яке охоплює різноманітні злочинні дії в сфері криптовалют, включаючи обмани з першими монетними пропозиціями та пірамідальні схеми.

Інший новостворений термін – *FinTech Phishing* (фінтех-фішинг), який вказує на використання традиційних методів фішингу для атак на користувачів фінансових технологій. *Algorithmic Embezzlement* (алгоритмічне розкрадання) стає актуальним у зв'язку зі зростанням автоматизованих фінансових систем, яке передбачає використання алгоритмів для неправомірного перенаправлення коштів. Ці нововведення в термінології свідчать про необхідність визначення та розуміння сучасних викликів у сфері комп'ютерної безпеки та фінансових ризиків.

Також нами було виявлено наступні терміни неправомірного втручання в глобальні фінансові системи:

1. *Insider trading* – використання конфіденційної інформації для отримання фінансового прибутку на фондовому ринку (телескопія);

2. *Pump and dump scheme* – маніпулювання цінами акцій шляхом штучного підняття (pump) і, наступно, швидкого розпродажу (dump) для отримання прибутку (словоскладання);
3. *Spoofing* – подача фальшивих заявок на фондових ринках для впливу на ціни та отримання фінансових вигод (афіксація);
4. *Front running* – передовиця виконання угод на фондовому ринку перед виконанням зазначених угод клієнтів, щоб отримати прибуток (словоскладання);
5. *Flash crash exploitation* – використання тимчасового стрімкого зниження цін для вигідного виконання угод (телескопія);
6. *Wash trading* – штучне створення вигляду реальних угод для впливу на ціни активів (словоскладання);
7. *High-frequency trading (HFT) exploits* – використання високочастотного торгівельного програмного забезпечення для отримання прибутку зі стрімкого виконання угод (скорочення);
8. *Money laundering through cryptocurrencies* – використання криптовалют для відмивання грошей та приховування походження фінансів (телескопія);
9. *Blockchain manipulation* – зловживання технологією блокчейн для маніпулювання фінансовою інформацією чи вироблення фальшивих транзакцій (телескопія);
10. *Hacking financial institutions* – вторгнення в системи банків та фінансових установ для отримання несанкціонованого доступу до конфіденційної інформації (телескопія);
11. *Dark web financial fraud services* – використання послуг фінансового обману, що пропонуються в області темного вебу (телескопія);
12. *Ransomware attacks on financial organizations* – кібератаки, які включають шифрування даних та вимагання викупу від фінансових установ (словоскладання);

13. *SIM swapping for account takeover* – використання заміни SIM-карти для отримання доступу до банківських або фінансових облікових записів (телескопія);
14. *Blockchain pump and dump* – маніпулювання цінами криптовалют шляхом штучного збільшення та різкого зниження їхньої вартості (телескопія);
15. *Mobile banking exploits* – використання вразливостей в мобільних банківських додатках для отримання несанкціонованого доступу до фінансових ресурсів (телескопія);
16. *ATM skimming* – використання пристроїв для крадіжки банківських карток та пін-кодів в банкоматах (телескопія);
17. *Cross-border payment frauds* – вчинення обману в міжнародних платіжних системах для отримання фінансових вигод (телескопія);
18. *Insolvency schemes* – вчинення шахрайських дій для виклику банкрутства підприємств чи фінансових організацій (телескопія);
19. *Initial coin offering (ICO) scams* – шахрайські схеми, пов'язані з продажем фальшивих токенів під час ініціювання криптовалютних проєктів (афіксація);
20. *Wire fraud* – вчинення обману за допомогою маніпулювання електронними грошовими переказами та банківськими транзакціями (телескопія) [Крамар 2022; Cambridge Online Dictionary; Urban Online Dictionary].

Отже, комп'ютерні злочини, пов'язані з економікою, стали важливим викликом для сучасного суспільства. Розмаїття неологізмів у цій області свідчить про постійну еволюцію технологічного ландшафту та швидкі темпи розвитку кіберзлочинності. Вплив таких злочинів на економіку виявляється у фінансових втратах, викраденні інтелектуальної власності, а також у загрозі стабільності фінансових інститутів. Загальна кількість злочинів та їхній фінансовий вплив підкреслюють необхідність посилення заходів кібербезпеки та удосконалення законодавства для протидії цьому роду загрозам.

Ми дійшли до висновку, що наявний наступний розподіл способів неправомірного доступу до комп'ютерної мережі в рамках економічних транснаціональних злочинів, здійснених із застосуванням сучасних комп'ютерних технологій: вчинення з використанням комп'ютерних технологій і відповідної техніки (*actions using computer technologies and related equipment*); незаконне отримання товарів та послуг (*illegal acquisition of goods and services*); несанкціоноване перехоплення інформації (*unauthorized interception of information*); неправомірний доступ до комп'ютерної інформації суб'єктів (*illegal access to computer information of subjects*); Розкрадання, пов'язане з переказом електронної готівки (*theft associated with the transfer of electronic cash*); шахрайство в сфері електронної торгівлі та інвестування (*fraud in the field of electronic trade and investment*); електронні способи легалізації злочинних доходів (*electronic methods of legalization of criminal income*); ухилення від оподаткування (*tax evasion*).

Також нами було виявлено наступні терміни неправомірного втручання в глобальні фінансові системи: *insider trading, pump and dump scheme, spoofing, front running, flash crash exploitation, wash trading, high-frequency trading (HFT) exploits, money laundering through cryptocurrencie, blockchain manipulation, hacking financial institutions, dark web financial fraud services, ransomware attacks on financial organizations, SIM swapping for account takeover, blockchain pump and dump, mobile banking exploits, ATM skimming, cross-border payment frauds, insolvency schemes, initial coin offering (ICO) scams, wire fraud.*

2.4 Комп'ютерні злочини пов'язані з політикою

Політика виступає джерелом новаторських рішень для легалізації процесів, що виникають у суспільстві. Кіберпростір об'єднує в собі різні методи комунікації, впливу та взаємодії між учасниками політики та

активними громадянами. Одночасно кіберсередовище представляє собою сукупність засобів, за допомогою яких можна здійснювати цю взаємодію та комунікацію, оскільки рівень сучасних технологій у сфері телефонів, планшетів, комп'ютерів та ноутбуків постійно зростає.

Метою поданого дослідження є з'ясування корпусу неологізмів у сфері комп'ютерних злочинів, пов'язаних з політикою. Тому, як зазначає лінгвіст

Ю. В. Завгородня, виникає потреба в систематизації існуючої інформації щодо можливих видів кіберконфліктів, які можуть завдати шкоди політичним процесам, вплинути на хід політичних подій, зміну політичних еліт, концентрацію влади як у глобальному, так і в регіональному контексті [Завгородня 2023, с. 74].

Розглянемо різновиди політичних кіберконфліктів, запропоновані В. О. Жадько:

- кібервандалізм (*cybervandalism*): цей вид конфлікту включає в себе зміни або знищення змісту, наприклад, веб-сайту, вимкнення або перевантаження сервера;

- інтернет-злочини (*Internet crimes*): ця діяльність спрямована переважно на отримання прямого фінансового зиску і може включати як злочини, пов'язані з комп'ютерною технікою, так і комп'ютерні злочини загалом;

- кібершпигунство (*cyber espionage*): головною жертвою цього виду кіберконфлікту часто стає корпоративний сектор. За деякими оцінками, збитки компаній від такої діяльності становлять до 1 трільйона доларів США на рік;

- кібертероризм (*cyber-terrorism*): хоча потенційні масштаби збитків від кібертерактів оцінюються як надзвичайно високі, дотепер не було жодного реального випадку кібертероризму;

- кібервійна (*cyber warfare*): цей вид кіберконфлікту охоплює можливість ведення кібервійни [Жадько 2018, с. 76].

Також кіберконфлікти в політиці можна класифікувати за об'єктом спрямування кібератак, тобто способи впливу можуть бути спрямовані на різні цілі:

1. Об'єктом кібервпливу може бути громадянське суспільство. У цьому випадку, кібератаки можуть приймати форму поширення фейків і дезінформації через інформаційні ресурси та соціальні мережі. Головною метою таких атак є вплив на громадську думку, створення паніки або маніпуляція громадянським суспільством;

2. Об'єктом кібервпливу може бути критична інфраструктура. В цьому випадку, кібератаки можуть включати в себе «знищення критичної інформаційної інфраструктури», шпигунство для отримання важливої розвідки про логістику, озброєння, плани та операції з оборони та безпеки;

3. Об'єктом кібервпливу може бути суб'єкт політики, політична партія або політична група. У цьому випадку, кібератаки можуть приймати форму створення штучних ботів, фейкових сторінок та коментарів, які працюють на користь опонента і виконують замовлення. Такі атаки можуть призвести до розвитку суспільного резонансу та підриву політичної позиції політика, політичної партії або групи [Завгородня 2023, с. 76].

Завдяки постійному вдосконаленню комп'ютерних систем виникають нові можливості для здійснення раніше невідомих порушень закону, а також для вчинення традиційних злочинів за допомогою нових засобів [Гриців 2009].

Неологізми, пов'язані з кіберзлочинами у політиці, є свідченням швидкого розвитку цифрового світу та появи нових феноменів у сфері кібербезпеки та політичного впливу. Ці терміни і вирази виникли, щоб відобразити сучасні техніки та загрози, які стали характерними для політичних процесів у кіберпросторі.

Ці неологізми відображають складність та актуальність сучасних політичних викликів у кіберпросторі і є важливими для розуміння та боротьби з цими новими видами кіберзлочинів у політиці. Наприклад:

1. *Politihactivism* — поєднання політичного активізму та хакінгу для досягнення політичних цілей (телескопія);

2. *E-leaksphere* — електронна сфера розголошення та розповсюдження конфіденційної інформації (телескопія);

3. *Cybercorruption* — використання кібертехнологій для корупційних дій в політичних структурах (афіксація);
4. *Hacktivistocracy* — управління або вплив на політику за допомогою хакерського активізму (скорочення);
5. *Electrodefamation* — використання електронних засобів для наклепу та порочення репутації політичних діячів;
6. *Disinfotech* — розповсюдження дезінформації за допомогою кібертехнологій (словоскладання);
7. *Votebotting* — використання програмних ботів для маніпулювання результатами виборів або голосувань (телескопія);
8. *Cryptoespionage* — використання криптовалют для ведення шпигунської діяльності в політичних структурах (телескопія);
9. *Hacktivate* — хакерські атаки з метою впливу на виборчий процес та його результати (телескопія);
10. *Cyberlobbying* — використання кіберзасобів для лобювання політичних інтересів (телескопія);
11. *Deepstatehack* — хакінг для виявлення або розкриття прихованих політичних структур (телескопія);
12. *Hackocracy* — управління суспільством або політичними процесами за допомогою хакерських методів (телескопія);
13. *Cybergovernance* — вплив на уряд та його рішення через кібератаки (телескопія);
14. *Hacktivistvisionary* — особа, яка використовує хакінг для реалізації своєї візі політичної та суспільної трансформації (телескопія);
15. *Cryptoanarchy* — використання криптовалют та кібертехнологій для створення анонімних політичних структур (телескопія);
16. *Cyberdissidence* — використання інтернет-технологій для вираження дисидентства та протесту проти політичної системи (телескопія);
17. *Electioneeringhacks* — хакінг для маніпулювання інформацією та впливу на виборчий процес (телескопія);

18. *Hyper trollitics* — використання соціальних мереж та технологій для систематичної образи політичних опонентів, яка сигналізує агресивну поведінку (скорочення);

19. *Blockchainocracy* — використання технології блокчейн для створення нових форм політичного управління (словоскладання);

20. *Cyberfactionalism* — використання кіберзасобів для стимулювання та підтримки фракційних розбіжностей в політиці (телескопія) [Cambridge Dictionary Online; WordSense Dictionary Online].

Отже, комп'ютерні злочини стали потужним інструментом для впливу на політичні рішення, громадську думку та демократичні процеси. Кібератаки, кіберпропаганда, дезінформація та інші види кіберзлочинів впливають на виборчі кампанії, політичну риторику та рішення держав.

У світлі цих загроз політики, правоохоронні органи та суспільство повинні бути готові до реагування на комп'ютерні злочини та забезпечення кібербезпеки. Важливо розробляти та впроваджувати ефективні заходи для захисту інформаційної безпеки та демократичних процесів.

Нами було розглянуто наступні різновиди політичних кіберконфліктів: кібервандалізм (*cybervandalism*), інтернет-злочини (*Internet crimes*), кібершпигунство (*cyber espionage*), кібертероризм (*cyber-terrorism*), кібервійна (*cyber warfare*).

За результатами дослідження доходимо до висновку, що наступні неологізми відображають складність та актуальність сучасних політичних викликів у кіберпросторі і є важливими для розуміння та боротьби з цими новими видами кіберзлочинів у політиці: *politihactivism*, *E-leaksphere*, *cybercorruption*, *hacktivistocracy*, *electrodefamation*, *disinfotech*, *votebotting*, *cryptoespionage*, *hacktivote*, *cyberlobbying*, *deepstatehack*, *hackocracy*, *cybergovernance*, *hacktivistvisionary*, *cryptoanarchy*, *cyberdissidence*, *electioneeringhacks*, *hyper trollitics*, *blockchainocracy*, *cyberfactionalism*.

ВИСНОВКИ

Суспільство виступає важливим детермінантом в еволюції словникового складу сучасної англійської мови, впливаючи на структуру, зміст та функції слів у відповідності до змін у політичному, економічному, культурному та соціальному контексті.

Зміни в активному досвіді людини і надалі будуть призводити до виникнення нових та розширення старих аспектів сприйняття світу, які, в свою чергу, потребуватимуть відображення на мовній карті світу. Англійська мова, так само, як і багато інших мов, постійно досвіджуватиме неологічний бум.

Цей процес свідчить про живий розвиток мови та її здатність адаптуватися до змін у суспільстві і культурі. Створення неологізмів – це не лише лінгвістичний процес, але й відображення динамічної природи мови та її здатності відображати сучасні реалії. Розуміння цього явища має важливе значення для лінгвістів, мовознавців та культурологів, а також для всіх, хто вивчає англійську мову та цікавиться її еволюцією в контексті сучасного світу.

Вивчення структурно-семантичних особливостей творення нових слів в англійській мові має велике практичне і теоретичне значення. Це дослідження відкриває перед нами багатий світ лінгвістичних інновацій, які є відповіддю на зміни в суспільстві, технології та культурі.

Аналіз структурно-семантичних аспектів творення нових слів дозволяє нам краще розуміти еволюцію мови та її здатність адаптуватися до нових реалій. Цей процес також підсилює виразність та точність комунікації, допомагаючи мові виражати нові ідеї та концепції.

Кіберзлочини є серйозною загрозою сучасному інформаційному суспільству, і вони вимагають постійного удосконалення законодавства, заходів з кібербезпеки та співпраці між правоохоронними органами та технічними експертами. Попередження та протидія комп'ютерним злочинам є важливими завданнями в умовах сучасного цифрового суспільства. Можна

виділити декілька ключових аспектів у цьому контексті: захист інформації, оновлення програмного забезпечення, інформаційна гігієна, захист від фішингу, мережева безпека, кіберзахист організацій, міжнародне співробітництво, інновації в кіберзахисті.

Неологізми, пов'язані з комп'ютерною злочинністю відображають не лише технічні аспекти цих явищ, але також їхні соціокультурні та етичні виміри. Це свідчить про необхідність адаптації мовного апарату до постійно змінюючихся реалій сучасного інтернет-середовища.

Комп'ютерні злочини пов'язані з суспільством можуть виявлятися у різних формах, включаючи порушення приватності, шахрайство, кібертероризм та інші аспекти. Наступні неологізми, пов'язані з комп'ютерною злочинністю в контексті суспільства, можуть включати терміни, що визначають нові види атак: *synthetic identity theft (SIT)*, *AI-driven phishing*, *cryptojacking*, *distributed denial of wallet (DDoW)*, *e-skimming*, *rogue software updates*, *smart contract manipulation*, *AI-powered evasion*, *typosquatting attacks*, *zero-click exploits*, *side-channel attacks*, *binary planting (DLL hijacking)*, *DNS spoofing (pharming)*, *bluejacking*. Загалом нами було опрацьовано 30 неологізмів, пов'язаних з комп'ютерною злочинністю в контексті суспільства.

Наявний наступний розподіл способів неправомірного доступу до комп'ютерної мережі в рамках економічних транснаціональних злочинів, здійснених із застосуванням сучасних комп'ютерних технологій: вчинення з використанням комп'ютерних технологій і відповідної техніки (*actions using computer technologies and related equipment*); незаконне отримання товарів та послуг (*illegal acquisition of goods and services*); несанкціоноване перехоплення інформації (*unauthorized interception of information*); неправомірний доступ до комп'ютерної інформації суб'єктів (*illegal access to computer information of subjects*); Розкрадання, пов'язане з переказом електронної готівки (*theft associated with the transfer of electronic cash*); шахрайство в сфері електронної торгівлі та інвестування (*fraud in the field of electronic trade and investment*);

електронні способи легалізації злочинних доходів (*electronic methods of legalization of criminal income*); ухилення від оподаткування (*tax evasion*).

Терміни неправомірного втручання в глобальні фінансові системи: *insider trading, pump and dump scheme, spoofing, front running, flash crash exploitation, wash trading, high-frequency trading (HFT) exploits, money laundering through cryptocurrencie, blockchain manipulation ,hacking financial institutions, dark web financial fraud services, ransomware attacks on financial organizations, SIM swapping for account takeover, blockchain pump and dump, mobile banking exploits, ATM skimming, cross-border payment frauds, insolvency schemes, initial coin offering (ICO) scams, wire fraud.*

Комп'ютерні злочини стали потужним інструментом для впливу на політичні рішення, громадську думку та демократичні процеси. Кібератаки, кіберпропаганда, дезінформація та інші види кіберзлочинів впливають на виборчі кампанії, політичну риторику та рішення держав.

У світлі цих загроз політики, правоохоронні органи та суспільство повинні бути готові до реагування на комп'ютерні злочини та забезпечення кібербезпеки. Важливо розробляти та впроваджувати ефективні заходи для захисту інформаційної безпеки та демократичних процесів.

Різновиди політичних кіберконфліктів: кібервандалізм (*cybervandalism*), інтернет-злочини (*Internet crimes*), кібершпигунство (*cyber espionage*), кібертероризм (*cyber-terrorism*), кібервійна (*cyber warfare*).

Наступні неологізми відображають складність та актуальність сучасних політичних викликів у кіберпросторі і є важливими для розуміння та боротьби з цими новими видами кіберзлочинів у політиці: *politihacktivism, E-leaksphere, cybercorruption, hacktivistocracy, electrode defamation, disinfotech, votebotting, cryptoespionage, hacktivate, cyberlobbying, deepstatehack, hackocracy, cybergovernance, hacktivistvisionary, cryptoanarchy, cyberdissidence, electioneeringhacks, hypertrollitics, blockchainocracy, cyberfactionalism.*

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

СПИСОК ТЕОРЕТИЧНИХ ДЖЕРЕЛ

1. Архипенко Л. М. Інтеграція новітніх англіцизмів у термінологію економічної галузі. *Науковий журнал «Молодий вчений»*. Одеса, 2019. №2 276 с.
2. Біленчук П. Д. Питання соціальної та криміналістичної характеристики комп'ютерного злочинця. *Держава та регіони. Серія : Право*. Київ, 2011. 221 с.
3. Буров О. К. Вплив кіберзлочинності на цифрову економіку. Київ, 2021. 345 с.
4. Борзенков Н. Г., Комісаров С. В. Поняття і загальна характеристика злочинів у сфері комп'ютерної інформації. Курс кримінального права в п'яти томах. 2012. Т. 4. 236 с.
5. Веселова Л. Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни. Одеса, 2021. С. 18–19.
6. Волкова С. Г. Неологізми у сучасній англійській мові на прикладі мови інтернет-ресурсів. *Вісник Маріупольського державного університету*. 2019. С. 113–114.
7. Громовенко В. В. Скорочення як спосіб словотворення політичних неологізмів у сучасній англійській мові. Одеса, 2018. С. 235–237.
8. Гриців М. І. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електров'язку. Верховний суд України. 2009. 743 с.
9. Жадько В. О. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник. Київ, 2018. 356 с.

10. Завгородня Ю. В. Різновиди політичних конфліктів у кіберпросторі. *Актуальні проблеми політики*. 2023. Вип. 71. С. 74–78.
11. Завидняк І. О. Учинення економічних транснаціональних злочинів шляхом незаконних операцій, пов'язаних із неправомірним доступом до комп'ютерної мережі. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2021. С. 93–94.
12. Зацний Ю. А. «Внутрішні» запозичення сучасної англійської мови. *Вісник СумДУ №11*. 2016. С. 28–29.
13. Зацний Ю. А. Інновації у словниковому складі англійської мови початку ХХІ століття. *Англоукраїнський словник*. Вінниця, 2018. 360 с.
14. Зацний Ю. А. Розвиток словникового складу сучасної англійської мови. Запоріжжя : Запорізь. ун-т, 2015. 429 с.
15. Зацний Ю. А., Янков А. В. Нова розмовна лексика і фразеологія. *Англо-український словник*. Вінниця, 2010. 224 с.
16. Дудок Р. І. Проблема значення та смислу терміна в гуманітарних науках : монографія. 2009. 358 с.
17. Дзюбіна О. І. Типологічні принципи класифікації неологізмів у сучасній англійській мові. *Вісник Міжнародного гуманітарного університету*. 2018. № 33. С. 39–41.
18. Дзюбіна О. І. Структура, семантика та прагматика сленгових неологізмів соціальних мереж Twitter та Facebook (на матеріалі англійської мови). Львів : Львівський національний ун-т імені Івана Франка, 2016. 206 с.
19. Демченко Н. С. Особливості функціонування неологізмів в сучасній англійській мові. Біла Церква, 2019. С. 48–53.
20. Дикий О. В. Кіберзлочинність та кібервійна: сучасні виклики. Одеса, 2022. С. 493–497.
21. Ісмайлов К. Ю. Кіберзлочинність та кібербезпека. Одеса, 2017. 295 с.
22. Жулінська М. О. Нова лексика як відображення життя суспільства. *Науковий журнал*. 2019. №8. С. 87–91.

23. Клименко Л. Продуктивні моделі творення неологізмів. *Вісник Прикарпатського університету. Філологія*. 2001. Вип. 7. С. 71.
24. Квеселевич Д. І. Інтеграція словосполучення в сучасній англійській мові. Житомир, 1985. 328 с.
25. Кундеус В. Г. Поняття та види кіберзлочинів. Харків, 2020. С. 44–45.
26. Ладоня К. Ю. Неологізми в україномовному сегменті соціальної мережі “Facebook”. Київ, 2021. 234 с.
27. Мурко І. І. Зміни в повсякденному житті носіїв американського та британського національних варіантів і поповнення словникового складу сучасної англійської мови. *Вісник СумДУ*. 2012. № 4. С. 139–140.
28. Моїсєєва Н. Мовні та позамовні фактори неологізації лексичного складу німецької мови. *Наук. зап. Сер. Філологічні науки (мовознавство)*. РВВ КДПУ ім. В. Винниченка, 2011. Вип. 96 (1). С. 587–590.
29. Мойсієнко А. К. Динамічний аспект номінації. Київ : Київський університет. 2014. 100 с.
30. Ніколаюк С. І., Никифорчук Д. Й., Томма Р. П., Барко В. І. Протидія злочинам у сфері інтелектуальної власності. Київ, 2006. 256 с.
31. Нестеряк Ю. В. Державна інформаційна політика та управління національними інформаційними ресурсами : збірник наукових праць. Дніпропетровськ, 2013. С. 94–104.
32. Новікова Є. Б. Неологізм, okazіоналізм, потенційне слово. Проблеми розмежування: зб. наук. праць ХНПУ ім. Г. С. Сковороди, 2017. Вип. 45. С. 97–102.
33. Остафійчук О. Д. Неологізми англійської мови в сучасному суспільстві. Вчені записи ТНУ імені В. І. Вернадського. *Філологія. Соціальні комунікації*. 2020. С. 158–160.
34. Самойленко О. А. Виявлення та розслідування кіберзлочинів. Одеса, 2020. С. 8–9.

35. Ситенко О. О. Лексичні іновації у сфері іноваційних технологій англійської мови. Вінниця, 2019. С. 46–50.
36. Сухенко В. Г. Мова і суспільство: взаємодія і розвиток. *Харківський національний економічний університет імені С. Кузнеця*. 2016. С. 734–735.
37. Столбов Ф. В. Аналіз боротьби з комп'ютерною злочинністю. Тези доповідей міжнародної НПК «Інформаційна та економічна безпека». 2010. С. 158–160.
38. Торнолог Н. В. Неологізми-запозичення сучасної англійської мови. Наукові конференції. *Вісник СумДУ*. 2016. 487 с.
39. Омельченко Л. Ф. Телескопійні слова сучасної англійської мови та їх структурно-семантична характеристика. *Збірник Львівського університету. Іноземна філологія*. Львів, 2013. Вип. 15. С. 49–52.
40. Цимбалюк В. С. Причини латентності комп'ютерної злочинності. *Наукові записки*. Спеціальний випуск. 2011. Т. 19. С. 208–210.
41. Зіборова О. І. Неологізми, стилістичні функції. URL: <https://naurok.com.ua/urok-neologizmi-h-stilistichni-funkci-18898.html> (дата звернення: 10.09.2023).
42. Лісайчук А. А. Проблеми боротьби з кіберзлочинністю на міжнародному рівні. URL : <https://core.ac.uk/reader/153586200> (дата звернення: 12.10.2023).
43. Неологізми англійської мови. URL: <https://opentalk.org.ua/langstory/neologizmy-anglijskoyi-movy/> (дата звернення: 15.10.2023).
44. Пріт Т. А. Неологізм, його характеристика та способи будови. URL: <https://naurok.com.ua/neologizm-yogo-harakteristiki-ta-sposobi-budovi-35623.html> (дата звернення: 04.09.2023).
45. Хмельницька Обласна Бібліотека імені Островського. URL: <http://www.ounb.km.ua> (дата звернення: 02.09.2023).

СПИСОК ЛЕКСИКОГРАФІЧНИХ ДЖЕРЕЛ

46. Зацний Ю. А. Словник неологізмів. Іновації у словниковому складі англійської мови початку ХХІ століття: англо-український. 2022. 322 с.
47. Крамар Н. О. Словник англійських неологізмів ХХІ століття. Київ, 2022. 256 с.
48. Cambridge Dictionary Online. URL: <https://dictionary.cambridge.org/ru/> (accessed: 17.10.2023).
49. Longman Dictionary of Contemporary English. URL: <https://www.ldoceonline.com/> (accessed: 17.11.2023).
50. Meriam Webster Dictionary. URL: http://nws.merriamwebster.com/opendictionary/newword_display_cat.php (accessed: 21.11.2023).
51. Oxford English Dictionary. URL: <https://www.oed.com/?tl=true> (accessed: 21.11.2023).
52. Urban Dictionary Online. URL: <https://www.urbandictionary.com/> (accessed: 21.11.2023).
53. WordSense Dictionary Online. URL: <https://www.ats-group.net/dictionaries/dictionary-neologisms.html> (accessed: 23.10.2023).

SUMMARY

The presented paper is dedicated to the analysis of the research is the structural and semantic parameters of English-language neologisms in the field of computer crimes.

The object of the work can be defined as English-language neologisms in the field of computer crimes of the 21st century.

The main aim of the paper consists in revealing the structural and semantic parameters of English-language neologisms in the field of computer crimes.

The analysis of neologisms was carried out in the context of theoretical conclusions (L. M. Arkhipenko, S. G. Volkova, V. V. Gromovenko, etc.) and lexicographic studies (“Dictionary of neologisms. Innovations in the vocabulary of the early English language 21st century”, “Cambridge Dictionary Online”, “Meriam Webster Dictionary”, etc.).

Among the structural and semantic parameters of English-language neologisms in the field of computer crimes, the influence of affixation, composition and abbreviation for the formation of new terms is singled out.

Given the semantic features, many neologisms are directly related to the characteristics of computer crimes, such as “phishing”, “ransomware”, or “cyberbullying”. A group of neologisms that are actively used to describe aspects of computer crimes on a large scale and their impact on society has also been identified.

A comparative analysis using different dictionary sources, such as “Cambridge Dictionary Online” and “Longman Dictionary of Contemporary English”, complements and confirms the results obtained.

Key-words: *neologism, structural and semantic parameters, computer crime*

Декларація
академічної доброчесності
здобувача ступеня вищої освіти ЗНУ

Я, Дедюкіна Ольга Костянтинівна, студентка 2 курсу магістратури, форми навчання заочної, факультету іноземної філології, спеціальність 035 Філологія, освітньо-професійна програма Мова і література (англійська), адреса електронної пошти dediukinaolga@gmail.com,

- підтверджую, що написана мною кваліфікаційна робота на тему «Структурно-семантичні параметри англійськомовних неологізмів сфери комп'ютерних злочинів» відповідає вимогам академічної доброчесності та не містить порушень, що визначені у ст. 42 Закону України «Про освіту», зі змістом яких ознайомлений/ознайомлена;

- заявляю, що надана мною для перевірки електронна версія роботи є ідентичною її друкованій версії;

- згоден/згодна на перевірку моєї роботи на відповідність критеріям академічної доброчесності у будь-який спосіб, у тому числі за допомогою Інтернет-системи, а також на архівування моєї роботи в базі даних цієї системи.

Дата _____

Підпис _____

ПІБ (студент) Дедюкіна О. К.