УДК 811.161.2’373.45
DOI https://doi.org/10.32782/2710-4656/2022.5.1/05

Гончаренко А. В.
Інститут мовознавства імені О. О. Потебні Національної академії наук України

НОВІТНІ АНГЛІЗМИ ІЗ СЕМАНТИКОЮ ШАХРАЙСТВА У СУЧАСНІЙ УКРАЇНСЬКІЙ МОВІ[1]

У статті розглянуто й проаналізовано семантичну й словотвірну поведінку новітніх англізмів із семантикою шахрайства в українській мові. Зазначено, що розвиток інформаційних технологій, електронних платіжних систем, засобів сучасної комунікації зумовив появу нових засобів та способів скоєння злочинних дій і, відповідно, нових мовних одиниць на їх позначення, що активно проникають до лексичної системи української мови. Частина таких слів стає на шлях запозичення ще до того, як знаходить закріплення у лексикографічній практиці мови-донора. У процесі суцільної вибірки із матеріалів засобів масової інформації, спеціалізованих інтернет-ресурсів, соціальних мереж, наукової та науково-популярної літератури тощо засвідчено близько 30 некодифікованих українськими словниками іншомовних слів на позначення понять, котрі стосуються кібершахрайства – виду злочинності, що вчиняється за допомогою комп’ютерно-телекомунікаційних пристроїв, систем чи мереж. Здійснено класифікацію виділених найменувань за значеннєвим принципом – назви шахрайств, назви спеціальних засобів для скоєння шахрайських дій, назви осіб, що вчиняють шахрайські дії; у межах першої, найоб’ємнішої, групи слів виокремлено назви інтернет-шахрайств, назви телефонних шахрайств та назви банкоматних шахрайств. З’ясовано, що виділені найменування у більшості випадків у процесі засвоєння не зазнають семантичних змін, функціонуючи на українськомовному ґрунті з тим самим значенням, що й у мові-джерелі. Спостерігається їх входження до структури української мови не лише поодинокими одиницями, а й групами (парами) спільнокореневих слів. Усі виокремлені англізми відтворюються шляхом транскрипції і/або транслітерації, асимілюються на морфологічному рівні (набувають ознак граматичної категорії роду, змінюються за числами і відмінками). Найбільш освоєні лексеми реалізують свій деривaційний потенціал в похідних іменниках та, частіше, прикметниках. Установлено спектр словотвірних значень, засвідчених новотворами від чужомовних входжень; визначено сукупність словотворчих формантів, які передають ці значення.

Ключові слова: *англізм, новітнє запозичення, українська мова, адаптація, шахрайство.*

Постановка проблеми. Кінець XX – початок XXI ст. став часом розширення соціально-економічних, політичних, культурних зв’язків України з іноземними державами. Результатом таких контактів стало посилення входження до української мови чужорідної лексики. Особливо зросла кількість запозичень для позначення нових явищ і процесів, наявних у світовій англомовній практиці. Активне вживання засвоєних назв, динамічне зростання їх структурно-семантичних типів, відсутність лексикографічної фіксації зумовлює необхідність постійної реєстрації та наукового вивчення нових іншомовних одиниць в українському лінгвістичному просторі.

Аналіз останніх досліджень та публікацій. Збільшення кількості англізмів у структурі сучасної української мови спричинило посилення уваги лінгвістів до особливостей мовних контактів, специфіки засвоєння і функціонування запозичених слів у мові-реципієнті. У різних аспектах цей процес досліджували Б.М. Ажнюк, Г.В. Зимовець, І.О. Коробова, С.В. Семчинський, С.А. Федорець та ін. На сьогодні наявні детальні студії, у яких проаналізовано етапи та ступені освоєння чужовізмів (Л.М. Архипенко, І.М. Каминін, О.А. Стишов), їх словотвірну поведінку в новому лінгвокультурному просторі (Є.А. Карпіловська, Л.П. Кислюк, Н.Ф. Клименко, В.М. Фурса), тенденції семантичної адаптації (Я.В. Битківська, Т.М. Полякова, В.П. Сімонок) тощо. Однак ці дослідження не вичерпують усього різнопланового потенціалу засвоєних назв, уходження яких до лексико-семантичної системи української мови зростає відповідно до впровадження

[1] Статтю підготовлено в межах наукового проєкту «Новітні англізми в українській мові» (державний реєстраційний номер 0121U110505 від 12.04.2021).

інноваційних технологій та пожвавлення зв'язків зі світовою спільнотою. Малодослідженою лишається група новітніх запозичень, що вказують на злочинні дії в умовах сучасного етапу розвитку суспільства. Побіжно про такі мовні одиниці згадано у дисертаційній праці І.О. Коробової. Утім виділені слова потребують детального лінгвістичного опису з огляду на стрімке поширення явищ, які вони позначають, та виявлення сучасних тенденцій розвитку мови.

Мета статті – проаналізувати семантичні особливості та словотвірний потенціал новітніх англомовних запозичень із семантикою шахрайства у сучасній українській мові.

Виклад основного матеріалу. Розвиток і масове використання комп'ютерних технологій, локальних, галузевих, регіональних та глобальних мереж зв'язку, електронних платіжних систем спричинили появу нових засобів та способів скоєння злочинних дій. Зародившись в англомовному світі, такі поняття не знаходять аналогів в українськомовному просторі, а тому засвоюються водночас із назвами, що їх номінують. Відтак українська мова поповнюється найменуваннями нових видів правопорушень, представленими англізмами, які позначають неправомірні вчинки в інформаційній сфері. За підрахунками І.О. Коробової подібні слова складають 3 % від загального числа новітніх входжень у структурі української мови [2, с. 89], а проте вони набувають активного вживання через зростання кількості випадків незаконного отримання матеріальної чи іншої вигоди шляхом втручання в системи обробки даних.

У процесі суцільної вибірки із матеріалів спеціалізованих інтернет-ресурсів, соціальних мереж, засобів масової інформації, наукової та науково-популярної літератури тощо засвідчено близько 30 лексикографічно не кодифікованих іншомовних лексичних одиниць на позначення понять, котрі стосуються нового виду злочинності, що вчиняється за допомогою комп'ютерно-телекомунікаційних пристроїв, систем чи мереж і називається кібершахрайством. Як показують спостереження, частину таких слів було запозичено в українську мову ще до того, як вона закріпилася у словникарській практиці мови-донора. Зокрема, у найавторитетніших сучасних лексикографічних виданнях англійської мови не фіксуються слова refilling, Jackpotting, Cash Trapping і под. [3; 4; 5; 6], однак вони активно функціонують в її узусі та засвоюються в інші мови.

На новому лінгвальному ґрунті чужовізми зазнають процесу адаптації, суть якого полягає в освоєнні іншомовної лексики системою мови-реципієнта на всіх її рівнях – графічному, фонетичному, морфологічному, лексико-семантичному та словотвірному. Проте найбільшу роль відіграють лексико-семантичний та словотвірний рівні як вищі ступені еволюційного процесу асиміляції лексичних запозичень у мові, що запозичує [1, с. 158].

У складі української мови англізми із семантикою шахрайства зазвичай відтворюються її засобами шляхом транскрипції і/або транслітерації, набувають ознак граматичної категорії роду, змінюються за числами і відмінками та засвоюються на лексико-семантичному рівні.

За значеннєвим принципом вони формують 3 умовні групи – 'назви шахрайств', 'назви спеціальних засобів для скоєння шахрайських дій', 'назви осіб, що вчиняють шахрайські дії'. Найбільшу кількість становлять безпосередньо засвоєні з мови-першоджерела лексеми, які позначають нові види шахрайств. З-поміж них загальну семантику незаконного використання інформаційних технологій у сферах телекомунікацій та банківського сектору задля присвоєння чужих коштів виражає англізм *фрод* (fraud). Напр.: *За прогнозами експертів, у майбутньому схеми* ***фроду*** *стануть все більш витонченими, тому бізнесам варто вже зараз посилити безпеку корпоративних ресурсів* [34]. Слід зауважити, що в українській мові слово зазнало звуження семантичного обсягу, позначаючи в англомовному середовищі будь-який тип шахрайства, обману, вчиненого з метою отримання нечесної вигоди [3; 4]. Утім щодо решти одиниць зазначеної групи помітною є тенденція їх засвоєння без зміни семантики.

Залежно від засобів чи сфери скоєння неправомірного вчинку найменування шахрайств можна типологізувати за трьома підгрупами – 'назви інтернет-шахрайств', 'назви телефонних шахрайств' та 'назви банкоматних шахрайств'.

Серед позначень шахрайств, що скоюються через мережу «Інтернет», засвоєно слова: *кіберсквотинг* (cybersquatting) 'реєстрація доменних імен, що містять назви вже наявних торгових марок або близьких до них за звучанням, з наміром подальшого перепродажу зацікавленим компаніям', *тайпсквотинг* (typosquatting) 'різновид кіберсквотингу – реєстрація доменних імен, співзвучних до адрес популярних сайтів, з розрахунком на помилку частини користувачів', *кейлогінг* (keylogging) 'відстеження натискань користувачем клавіш на клавіатурі для виявлення конфіденційної інформації', *клікджекінг* (clickjacking)

‘накладання поверх вебсторінки замаскованого гіперпосилання, що перенаправляє користувачів мережі «Інтернет» на сайт, якого вони не бажають відвідувати’, *клікфрод* (click fraud) ‘прихований перехід на рекламне посилання особою, не зацікавленою у рекламному оголошенні’, *спуфінг* (spoofing) ‘кібератака, за якої шахрай маскується під надійне джерело задля отримання доступу до конфіденційної інформації’, *фішинг* (phishing) ‘заманювання жертви на сайт-пастку шляхом розсилання електронних листів від імені популярних інтернет-магазинів, банків, соціальних мереж тощо з метою отримання доступу до конфіденційних даних (логінів, паролів) користувача’, *фармінг* (pharming) ‘різновид фішингу, що передбачає приховане перенаправлення користувачів зі справжньої IP-адреси на фальшиву’. Напр.: ***Кіберсквотинг*** *можна вважати як однією з можливостей для легального бізнесу, так і підставою для виникнення спірних правовідносин у сфері інтелектуальної власності чи навіть притягнення до кримінальної відповідальності* [15]; *Серед компаній, що зазнали* ***тайпсквотингу****, відомі такі гіганти як Verizon, Lufthansa, Lego і т.д.* [25]; *Один з інструментів, який існує протягом десятиліть і все ще є небезпечним, як і був, коли його винайшли, – це* ***кейлогінг*** [38]; ***Клікджекінг*** *– серйозна загроза не тільки для користувачів, але і для сайтів* [39]; *Головними ліками від* ***клікфроду*** *на сьогодні залишаються уважність та самоорганізованість рекламодавця* [16]; *Зазвичай основною метою* ***спуфінгу*** *є доступ до особистої інформації, викрадення грошей, обхід засобів контролю доступу до мережі або поширення шкідливого програмного забезпечення* [41]; *Для захисту від* ***фішингу*** *були створені безкоштовні сервіси, які допомагають швидко перевірити справжність сайту [*43]; *Механізм* ***фармінгу*** *нічим не відрізняється від стандартного вірусного зараження* [там же].

Різновиди телефонних шахрайств номінуються за допомогою лексем *вішинг* (vishing) ‘телефонне шахрайство, що передбачає виманювання реквізитів банківських карток або іншої конфіденційної інформації, примушування до переказу коштів на картку злодіїв’, *рефайлінг* (refiling) ‘незаконна підміна міжнародного телефонного трафіку’, *смішинг* (smishing) ‘різновид фішингу через текстові повідомлення на телефон’, *фрикінг* (phreaking) ‘зламування телефонних автоматів і мереж мобільного зв’язку за допомогою прихованих від користувача функцій з метою отримання безкоштовних дзвінків, поповнення рахунку тощо’, *боксинг* (boxing) ‘різновид фрикінгу, що передбачає підключення до телефона пристроїв для злому’. Напр.: *76 % користувачів, які стали об’єктом* ***вішингу****, розголошували реквізити карт* [там же]; *У майбутньому* ***рефайлінг*** *поступово втрачатиме свою актуальність через зростання популярності голосових сервісів та месенджерів* [26, с. 152]; *Вперше про* ***смішинг*** *ФБР повідомило в 2010 році* [31]; *Людей, котрі спеціалізуються на* ***фрикінгу,*** *називають фрикерами [*33]; ***Боксинг*** *об’єднує в собі більше 200 боксів, більшість з яких були створені наприкінці 1980-х або на початку 1990-х років* [там же].

Посягання злочинців на доступ до чужих коштів та банківських рахунків зумовили появу шахрайських дій з банкоматними системами. Серед новітніх запозичень на позначення таких понять зафіксовано слова: *джекпотинг* (Jackpotting) ‘використання зовнішніх електронних пристроїв або шкідливих програм задля отримання контролю над апаратною складовою банкомату’, *кардинг* (carding) ‘різновид шахрайства, за якого здійснюється операція з використанням банківської картки або її реквізитів без участі та відома власника’, *кештрепінг* (Cash Trapping) ‘встановлення на отвір для видачі готівки банкомата шахрайських пристроїв, які унеможливлюють отримання коштів жертвою’, *скімінг* (skimming) ‘крадіжка даних банківської карти за допомогою спеціальних пристроїв для зчитування інформації, які встановлюють ззовні банкоматів’, *шимінг* (shimming) ‘крадіжка даних банківської картки за допомогою спеціального пристрою для зчитування інформації, який встановлюється у картоприймач банкомату’. Напр.: *Атаки на банкомати в європейських країнах з використанням шкідливих програм і* ***джекпотингу*** *виявилися неефективними в першій половині 2019 року* [13]; *Основний захист від* ***кардингу*** *– пильність користувача* [43]; ***Кештрепінг*** *масово використовувався шахраями в Україні в останні роки* [23]; *Кіберполіція викрила злочинну групу у привласненні мільйона гривень за допомогою* ***скімінгу*** [14]; *Єдиним дієвим захистом від* ***шимінгу*** *є застосування чипових платіжних карток* [12].

Адаптувавшись до графічної, фонетичної, граматичної систем української мови, частина виділених запозичень на позначення різних типів кібершахрайств проявляє словотвірну активність та продукує новотвори, переважно ад’єктивного типу. Серед них засвідчуємо прикметники, утворені за допомогою суфікса *-ов-*, який передає відносне словотвірне значення ‘властивий

предметові або явищу, яке називає твірний іменник', 'такий, що має стосунок до названого твірним іменником' – *кіберсквотинговий*, *спуфінговий, фішинговий, фармінговий, вішинговий, смішинговий, скімінговий*. Напр.: *Відповідно до рекомендацій була введена в дію Універсальна стратегія розгляду спорів щодо доменних імен, покликана надавати допомогу власникам знаків для товарів і послуг, які постраждали від* ***кіберсквотингової*** *діяльності* [20, с. 87]; *Як розпізнавати* ***спуфінгові*** *листи й реагувати на них* [8]; *У світі кожні півхвилини створюються* ***фішингові*** *сайти, здатні вкрасти дані банківських карт або основний обліковий запис* [42]; *Рекомендуємо вам підготувати LP-токени пари EXON/USDT, щоб у найближчий час додати їх у* ***фармінговий*** *пул* [45]; *Якщо в результаті* ***вішингової*** *атаки карткові реквізити все ж були розголошені, першочерговою дією будь-якого користувача має бути негайне блокування платіжної картки* [7]; ***Смішингові*** *повідомлення можуть надходити з телефонних номерів у дивному або незрозумілому форматі* [27]; *У першому півріччі 2017 р. було зафіксовано 50 випадків встановлення* ***скімінгового*** *обладнання на банкоматах України* [23].

Окрім назв нових видів шахрайств, українською мовою засвоєно також лексичні одиниці на позначення спеціальних пристроїв та програм, за допомогою яких скоюються злочинні дії: *скімер* (skimmer) 'пристрій для зчитування даних банківських карток у вигляді відеокамери або спеціальної накладки на клавіатуру, картоприймач', *шимер* (shimmer) 'тонка гнучка плата для зчитування даних банківських карток, що прикріплюється до картоприймача банкомата', *кейлогер* (keylogger) 'пристрій або програма, що використовується для відстеження натискань клавіш користувачем', *руткіт* (rootkit) 'програма, що використовує технології перехоплення системних функцій та приховування слідів присутності зловмисника чи шкідливої програми в системі', *сніфер* (sniffer) 'програма або спеціальний пристрій для перехоплення й аналізу мережевого трафіку'. Напр.: ***Скімери****, як правило, встановлюють на банкомати, які знаходяться в нелюдних місцях, коли в темний час доби там точно не буде людей [*30]; ***Шимер*** *– воістину геніальний винахід* [37]; ***Кейлогери*** *відомі своєю здатністю збирати всі ваші особисті дані абсолютно непомітно* [38]; *Зловмисник, який за допомогою* ***руткіта*** *отримав можливість керувати комп'ютером, може викрадати паролі, дані банківських карток, здійснювати DDoS атаки, шпигувати за користувачем і багато іншого [*40]; ***Сніфери*** *застосовуються як у благих, так і в деструктивних цілях* [28]. На сучасному етапі такі слова виявляють нульову деривaційну спроможність.

У системі української мови засвідчуються також новітні назви осіб, які вчиняють неправомірні дії в сучасному інформаційному просторі, – кібершахраїв. Серед них засвідчуємо слова, які мають прямі відповідники в англійській мові, що дає підстави припускати їх безпосереднє засвоєння в українську мову, – *кіберсквотер* (cybersquatter) 'той, хто займається кіберсквотингом', *тайпсквотер* (typosquatter) 'той, хто займається тайпсквотингом', *фішер* (phisher) 'той, хто намагається обманути когось за допомогою фішингу', *фрикер* (phreaker) 'телефонний хакер', *кардер* (carder) 'той, хто займається шахрайством з платіжними картками', *крекер* (cracker) 'фахівець зі створення програм для злому захисту ліцензійного програмного забезпечення'. Напр.: *В окремих випадках бізнес може стати навіть жертвою вимагання* ***кіберсквотерів****, які за «відступ» зареєстрованого ними доменного імені, ... вимагають грошові кошти чи здійснення інших дій майнового характеру* [15]; ***Тайпсквотер*** *за рахунок перенаправлення трафіку може зібрати на своєму сайті певний відсоток тих відвідувачів, які помилилися, у результаті чого отримати економічні вигоди, наприклад, за рахунок показу реклами* [21]; *Далеко не всі користувачі орієнтуються в правилах безпеки в мережі та мають достатній рівень обізнаності, чим і користуються досвідчені* ***фішери*** [10]; *Зараз* ***фрикери*** *воліють гратися з GSM і CDMA лише для того, щоб інколи похуліганити і познущатися над співвітчизниками* [36]; *Якщо фальшивомонетнику для зразка досить узяти першу-ліпшу купюру, яка перебуває в обігу, то* ***кардеру*** *треба якимось чином проникнути в базу даних банку* [11]; *В абсолютній більшості випадків крекер не має у своєму розпорядженні вихідного коду програми* [17]. Деякі з нових позначень осіб-кібершахраїв не відомі в англійській мові та утворилися, імовірно, на українськомовному ґрунті шляхом додавання питомого афікса *-ер* до основи слова-етимона – *фродер* (fraud) 'той, хто незаконно використовує інформаційні технології у сферах телекомунікацій та банківського сектору з метою присвоєння чужих коштів', або виникли внаслідок переосмислення і звукової подібності до прямого запозичення з іншим, предметним, значенням – *скімер* 'той, хто незаконно знімає готівку з чужих банківських карток за допомогою спеціального облад-

нання’ (пор. *скімер* вище). Напр.: ***Фродери*** *завдають збитків не лише операторам мобільного зв’язку – побічно від них страждають і звичайні абоненти* [35]; *У вересні в Києві було затримано банду* ***скімерів****, яка викрадала дані клієнтів українських банків і знімала кошти за підробленими картками* [29].

Агентивна семантика виділених неологізмів на *-ер* уможливила деривацію похідних одиниць із суфіксом *-ств-* зі словотвірним значенням ‘заняття особи, названої твірним іменником’ – *кіберсквотерство, кардерство, фродерство*. Напр.: *Галузеве* ***кіберсквотерство*** *є одним з найприбутковіших, оскільки володіння доменом, що точно відповідає назві галузі або товару, це завжди запорука успіху та прибутку* [32]; *Найгострішими загрозами для бізнесу підприємці назвали: рейдерство, шахрайство, неврегульовані земельні питання та нестабільність валюти, проблеми кредитування, грінмейл та* ***кардерство*** [24]; *Новий вид злочинності –* ***фродерство*** **[**22].

Новітніми позначеннями осіб, що скоюють шахрайські дії, мотивовані відсубстантивні прикметники, що передають значення властивості, стосунку до особи, виразником якого є словотворчий афікс *-ськ- – тайпсквотерський, фішерський, кардерський, скімерський*. Напр.: ***Тайпсквотерський*** *URL-локатор буде, як правило, схожим на адресу сайту жертви за одним із зазначених критеріїв* [18, с. 218]; *Якщо є доступ до статистики трафіку* ***фішерського*** *вебсайту, можна встановити і перевірити всіх користувачів, які зверталися до цього сайту* [19, с. 14]; *Хакери здобули* ***кардерський*** *ресурс, на якому здійснювалися купівля і продаж крадених банківських карт, що спричинило значний витік даних* [9]; *У Харкові працівники СБУ затримали двох чоловіків, які ставили* ***скімерське*** *обладнання на банкомати і термінали [*44].

Висновки і пропозиції. Отже, у сучасній українській мові активно функціонують запозичені з англомовного простору неологічні лексеми із семантикою шахрайства. Проведене дослідження засвідчує випадки не лише поодинокого запозичення таких слів, а й уходження їх до структури української мови групами (парами) спільнокореневих одиниць – назва шахрайства/назва спеціального засобу для скоєння шахрайської дії (keylogging/keylogger, skimming/skimmer, shimming/shimmer), назва шахрайства/назва виконавця шахрайської дії (cybersquatting/cybersquatter, typosquatting/typosquatter, phishing/phisher, phreaking/phreaker, carding/carder). Здебільшого у процесі засвоєння слова виділеної тематичної групи не зазнають семантичних змін, функціонуючи на українськомовному ґрунті з тим самим значенням, що й у мові-джерелі. Спостерігається їх активна адаптація на фонетичному, графічному, морфологічному рівнях, реалізація деривaційного потенціалу частини найменувань в похідних іменниках та, частіше, прикметниках.

Перспективним видається подальше вивчення складного та динамічного характеру освоєння новітніх запозичень та визначення їх місця у лексичній системі української мови.

Список літератури:

1. Каминін І.М., Чурсіна Л.В. Асиміляція англо- та франкомовних запозичень на семантичному та словотвірному рівнях у сучасній українській мові. *Лінгвістичні дослідження: зб. наук. праць ХНПУ ім. Г.С. Сковороди*, 2018. Вип. 47. С. 157–164.

2. Коробова І.О. Семантичне та словотвірне освоєння новітніх запозичень в українській мові: дис. … канд. філол. наук: 10.02.01. Запоріжжя, 2018.443 с.

3. Cambridge Dictionaries Online. URL: https://dictionary.cambridge.org (дата звернення: 17.10.22).

4. Collins Online Dictionary. URL: https://www.collinsdictionary.com (дата звернення: 17.10.22).

5. Dictionary by Merriam-Webster: America’s most-trusted online. URL: https://www.merriam-webster.com (дата звернення: 17.10.22).

6. Oxford Learner’s Dictionaries Online. URL: https://www.oxfordlearnersdictionaries.com (дата звернення: 17.10.22).

Джерела ілюстративного матеріалу:

7. Вішингова атака: припиніть розмову або втратите гроші. *Фінансовий портал Fin.Org.UA*. URL: http://www.fin.org.ua/news/1225151 (дата звернення: 17.10.22).

8. Захист бізнесу від внутрішніх кіберзагроз. *Microsoft 365.* URL: https://bit.ly/3fKjb1y (дата звернення: 17.10.22).

9. Злам сайту BriansClub спричинив витік даних 26 млн банківських карт. *Букви*. URL: https://bit.ly/3fyU1Tb (дата звернення: 17.10.22).

10. Інтернет-фішинг. *Portmone.com.* URL: https://bit.ly/3RABN18 (дата звернення: 17.10.22).

11. Кардер за сумісництвом. *ZN.UA*. URL: https://bit.ly/3Ef656o (дата звернення: 17.10.22).
12. Кардинг. *Вікіпедія.* URL: https://uk.wikipedia.org/wiki/Кардинг (дата звернення: 17.10.22).
13. Кіберзлочинці "відмовляються" від зламу банкоматів. *CyberCalm*. URL: https://bit.ly/3REp910 (дата звернення: 17.10.22).
14. Кіберполіція викрила злочинну групу у привласненні мільйона гривень за допомогою скімінгу. *Юридична газета*. URL: https://bit.ly/3CxZmU8 (дата звернення: 17.10.22).
15. Кіберсквотинг: як захистити «візитівку» бізнесу. *Юридична газета*. URL: https://bit.ly/3SBRgiF (дата звернення: 17.10.22).
16. Клікфрод: не плати за шахрайський клік. *Zillya! Антивірус*. URL: https://zillya.ua/klikfrod-ne-plati-za-shakhraiskii-klik (дата звернення: 17.10.22).
17. Крекер (комп'ютерний зламувач). *Вікіпедія*. URL: https://bit.ly/3yyzmWe (дата звернення: 17.10.22).
18. Матяш О. Кіберсквотинг як різновид порушення прав інтелектуальної власності в мережі Інтернет. *Правові засади функціонування публічної влади щодо забезпечення інтелектуального розвитку та безпеки суспільства: матеріали Міжнародної науково-практичної конференції (Суми, 19-20 травня 2016 р.)*. Суми: СДУ, 2016. С. 217–219.
19. Мілентьєва А.М., Ісмайлов К.Ю. Фішинг як сучасна проблема суспільства. *Актуальні питання протидії правопорушенням у сфері використання інформаційно-телекомунікаційних систем: матеріали науково-практичної інтернет-конференції (Одеса, 28 жовтня 2016 р.).* Одеса: Одеський державний університет внутрішніх справ, 2016. С. 12–15.
20. Науменко Ю.М. Кіберсквотинг як загроза системі правової охорони доменних імен в Україні. *Право та інноваційне суспільство*, 2006. № 2(7). С. 86–90.
21. Новгородська І.М. Доменні імена як засоби індивідуалізації учасників цивільного обороту: дипломна робота. Київ, 2020. URL: https://bit.ly/3CL3d04 (дата звернення: 17.10.22).
22. Новий вид злочинності – фродерство. *Телевізійна служба новин*. URL: https://bit.ly/3SBQHW3 (дата звернення: 17.10.22).
23. Обережно: шахраї. Як з карткових рахунків українців зникають гроші. *Dsnews*. URL: https://bit.ly/3C6NMOj (дата звернення: 17.10.22).
24. Підприємці назвали найбільшу загрозу для бізнесу. Офіційний сайт *Львівської торгово-промислової палати*. URL: https://lcci.com.ua/pidpryyemci-nazvaly-najbilshu-zagrozu-dlya-biznesu/ (дата звернення: 17.10.22).
25. Про кіберсквотерство. *Ліга.Блоги*. URL: https://blog.liga.net/user/ytrachuk/article/8762 (дата звернення: 17.10.22).
26. Савченко А.В. Рефайлінг як спосіб вчинення несанкціонованого втручання в роботу мереж електронного зв'язку. *Юридична наука*, 2018. № 1(79). С. 149–165.
27. Смішинг. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Смішинг (дата звернення: 17.10.22).
28. Сніфер – аналізатор трафіку. *Snooper.in.ua.* URL: https://bit.ly/3ydSaK0 (дата звернення: 17.10.22).
29. У Києві затримали скімера з Польщі. *Financial club*. URL: https://finclub.net/ua/news/u-kievi-zatrimali-skimera-z-polshchi.html (дата звернення: 17.10.22).
30. У Трускавці у людей масово зникають гроші з карток. *VGORODE*. URL: https://bit.ly/3UZ5jAs (дата звернення: 17.10.22).
31. ФБР попередило про аферу з SMS. Як працює смішинг. *ГО «Детектор медіа».* URL: https://bit.ly/3CxZPFS (дата звернення: 17.10.22).
32. Фоя О.А., Золоєва А.О. Проблеми кіберсквотингу в Україні. URL: http://www.rusnauka.com/21_TSN_2015/Pravo/9_197281.doc.htm (дата звернення: 17.10.22).
33. Фрикінг. *Вікіпедія.* URL: https://bit.ly/3e5FVsg (дата звернення: 17.10.22).
34. Фрод та як від нього захиститися: все, що потрібно знати власникам eCommerce. *Minfin.com.ua*. URL: https://minfin.com.ua/ua/2022/02/07/80373483/ (дата звернення: 17.10.22).
35. Хто вони, фродери? *Kriminal.tv*. URL: https://kriminal.tv/news/hto-voni-froderi.html (дата звернення: 17.10.22).
36. Хто такі фрикери та чому вони з легкістю можуть зламати вашу телефонну мережу? *Bit.ua*. URL: https://bit.ua/2021/02/telephone-hacker/ (дата звернення: 17.10.22).
37. Шимінг: поговоримо про новий спосіб шахрайства. URL: https://bit.ly/3Ch717C (дата звернення: 17.10.22).
38. Що таке кейлогінг? Як виявити та попередити атаки кейлогерів. *Hideez.com*. URL: https://hideez.com/uk/blogs/news/keylogging (дата звернення: 17.10.22).
39. Що таке клікджекінг та як від нього захиститися. *Інтернет Свобода*. URL: https://bit.ly/3fFGedM (дата звернення: 17.10.22).

40. Що таке руткіт і як з ними боротися. *Antivirus.pp.ua.* URL: http://antivirus.pp.ua/post28_ua.html (дата звернення: 17.10.22).

41. Що таке спуфінг і як запобігти атаці? Поради. *Cybercalm*. URL: https://bit.ly/3VgdvMW (дата звернення: 17.10.22).

42. Що таке фішинг і як від нього захиститись? *Офіційний сайт Фонду гарантування вкладів фізичних осіб*. URL: https://bit.ly/3rQt93S (дата звернення: 17.10.22).

43. Як захистити кошти на банківській картці. *Конкурент*. URL: https://bit.ly/3s4efHL (дата звернення: 17.10.22).

44. Як не потрапити на "гачок" аферистів та вберегти гроші на банківській картці. *Новини Харкова*. URL: https://bit.ly/3egOUXP (дата звернення: 17.10.22).

45. Facebook. URL: https://bit.ly/3EbXO3e (дата звернення: 17.10.22).

Honcharenko A. V. NEW ENGLISH BORROWINGS WITH THE SEMANTICS OF FRAUD IN THE MODERN UKRAINIAN LANGUAGE

The article examines and analyzes the semantic and word-formative behavior of newest Englishisms with the semantics of fraud in the Ukrainian language. It is noted that the development of information technologies, electronic payment systems, and modern means of communication led to the emergence of new means and methods of committing criminal acts and, accordingly, new linguistic units for their designation, which are actively entering the lexical system of the Ukrainian language. Some of these words are borrowed before they find their place in the lexicographic practice of the donor language. In the process of continuous sampling from the materials of the mass media, specialized Internet resources, social networks, scientific and popular science literature, etc., about 30 foreign words not codified by Ukrainian dictionaries were found to indicate concepts related to cyber fraud – a type of crime committed with the help of computer and telecommunication devices, systems or networks. Classification of selected names according to the meaning principle was carried out – names of frauds, names of special means for committing fraudulent actions, names of persons committing fraudulent actions; within the first, most voluminous, group of words, the names of internet frauds, the names of telephone frauds, and the names of ATM frauds are distinguished. It was found that in most cases, during the process of assimilation, the selected names do not undergo semantic changes, functioning on the Ukrainian-language soil with the same meaning as in the source language. Their entry into the structure of the Ukrainian language is observed not only as single units, but also as groups (pairs) of words with the same root. All selected Englishisms are reproduced by transcription and/or transliteration, assimilated at the morphological level (they acquire signs of the grammatical category of gender, change in number and case). The most mastered lexemes realize their derivational potential in derived nouns and, more often, adjectives. The range of word-forming meanings, evidenced by innovations from foreign borrowings, has been established; a set of word-forming formants that convey these meanings is defined.

Key words: *Englishism, newest loan word, Ukrainian, adaptation, fraud.*