УДК 811.111’276.6:004.946.5.056:355.271
DOI https://doi.org/10.32782/2710-4656/2022.6.1/15

Ботвин Т. М.
Львівський державний університет безпеки життєдіяльності

ЩОДО АНГЛОМОВНОЇ ТЕРМІНОЛОГІНОЇ СИСТЕМИ СЕКТОРУ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ: АНАЛІЗ ДЕФІНІЦІЙ

У статті проаналізовано особливості засвоєння та вживання англомовних термінів сектору кібербезпеки України та проведено огляд основних проблемних моментів дотичних до теми статті в умовах воєнного стану. Серед труднощів, з якими стикається спеціаліст в певній галузі, особливу блокуючу роль відіграє загальноприйнята специфічна термінологія. Студенти в галузі кібербезпеки, які в силу своєї майбутньої професії вивчають англійську мову (офіційно визнана мова кіберпростору), також не уникають цих труднощів. Отже, виникає потреба в створені тематичних глосаріїв, в яких розкривається специфічний лексикон та додається довідник визначень рідною мовою. Лінгвісти вважають, що вивчати термінологію ефективніше на контрасті рідної мови. При тому, не слід забувати про потребу в інструментах та методах, пристосованих для засвоєння термінології в певній галузі. Запорука та роздуми про мову та терміносистему – ефективний спосіб вивчити іноземну мову та фахову лексику. Більшість слів, які використовує «не лінгвіст» в своїй сфері є технічними термінами з традиційною граматичною структурою, які є менш абстрактними ніж інші лінгвістичні категорії. Проте, вони становлять проблему при їх засвоєнні. Завдяки великій кількості визначень, розроблених для певних наук, та арсеналу дотичної наукової літератури, вченими було продемонстровано, що використання специфічної термінології в конкретній мові усуває усі двозначності та непорозуміння в мовному акті. У ракурсі описаної проблематики, висновуємо, що англомовна термінологія в секторі кібербезпеки складне явище та вивчати її необхідно в ракурсі “English by Ukrainian”. Для цього, англомовні терміни необхідно складати у тематичні глосарії, детально розглянути кожен термін, навести їх дефініції. Така методика вивчення фахової англійської мови уможливлює ефективність засвоєння складної та розгалуженої термінології в секторі кібербезпеки в розрізі L1/L2 (“English by Ukrainian”). Висновуємо, що труднощі, пов’язані з абсолютно новою термінологією, можна подолати вивчаючи її визначення рідною мовою за допомогою тематичних глосаріїв перед кожною новою темою.

Ключові слова: *військовий стан, загроза кібератак, кібербезпека, мова кіберпростору, терміносистема, лінгвістична проблема.*

Постановка проблеми. Для того, щоб розкрити специфіку функцій кібербезпеки та лінгвістичних проблем, з якими стикаються фахівці у цій сфері, необхідно зробити обзір актуального стану кібербезпеки України в умовах війни. Саме в умовах російської збройної агресії, Україна остаточно прийняла використання цифрових технологій і переробила пропозиції та послуги майже в усіх сферах, які зараз в основному відбуваються в онлайн режимі. Війна призвела до загострення інформаційної війни та нових видів шахрайства, спрямованих на усі сфери онлайн послуг і банкінгу [1, с. 46]. Захист користувачів, їх цифрової ідентичності та платіжних засобів на відстані є критичним питанням безпеки для України, з метою підтримки довіри своїх громадян. Для цього, фахівцям в цій сфері необхідно володіти глибокими знаннями в англійській фаховій мові. В роботі розписані сфери роботи кіберфахівців та розкрите широке поле діяльності з лінгвістичної токи зору.

Аналіз останніх досліджень і публікацій. Кібербезпека лежить в основі стратегій суспільного сектору щодо боротьби з кібер-зловмисниками та постійно зростаючою кількістю шахрайства. Йдеться про переоцінку методів верифікації особистості та переосмислення безпеки онлайн операцій, покладаючись, зокрема, на штучний інтелект для кращого виявлення та аналізу ризиків [2, с. 46]. Фахівці у цій сфері повинні бездоганно володіти англійською мовою, яка є цільовою у кіберпросторі. Кібербезпека та відповідність нормативним вимогам мають важливе значення для захисту промислових об’єктів та

забезпечення контрольованого розвитку індустрії в умовах війни. Українські промислові компанії повинні захищати свою інтелектуальну власність, цілісність і безперервність виробничого процесу від кіберзловмисників. Це робиться для того, щоб зберегти ринок, зберегти конкурентну перевагу, запропонувати нові послуги і продукти і забезпечити виживання українського народу в умовах війни [3, с. 172]. Цифровізація та нові форми автоматизації мають вирішальне значення і більше не можуть заважати кіберризикам. Тому кібербезпека є основним викликом та топовою професією сьогодення. Термінологія сектору кібербезпеки стосується не тільки ІТ але й усіх сфер економіки та управління, в цьому і її складність. Способи формування термінології кіберпростору специфічна: афікси, абревіатури, неологізми, метафори тощо. І всі вони мають широкий ареал використання. Наприклад енергетика – енергетичний сектор є критично важливою інфраструктурою для країн. Будь-яке відключення або злам в цьому секторі в результаті кібератак створює людські, фінансові, соціальні та екологічні ризики [4, с. 60]. Ці системи складні, а терміни що їх означають, складаються з пов'язаних об'єктів, і вимагають специфічних знань, навичок, протоколів, процесів і технологій [5, с. 7].

Кібербезпека в охороні здоров'я є основною проблемою. Зростаюча кількість нападів на медичні установи підкреслила вразливість цього сектора, а також людський і технологічний дефіцит з цього приводу. У той же час світ охорони здоров'я пережив цифрову трансформацію вже у до військовий період. Йдеться про трансформацію обробки медичних даних, особливо через IoHT [6, с. 21]. ІТ та телекомунікації впливають на всі компанії, організації, суспільства та держави. Вони являють собою технічну частину кібербезпеки, найбільш помітну частину також називають комп'ютерною безпекою. Дійсно, комп'ютерна безпека в умовах війни – це основа, яка захищає інші частини організації, компанії або в більш широкому сенсі компанії або держави. Однак, якою б важливою вона не була, ІТ-безпека необхідна, але не достатня, вона становить лише крихітну частину сфери кібербезпеки [7, с. 113]. Будь то морський, залізничний, повітряний або автомобільний, транспорт тепер контролюється комп'ютерними системами. Кібератака може поставити під загрозу безперервність бізнесу або фізичну безпеку користувачів цих послуг. Крім того, взаємозв'язок цих систем збільшує загрозу впливу і, отже, потенційну загрозу атаки кіберзловмисників [8].

Державні адміністрації та органи місцевого самоврядування під час війни стали головними мішенями для зловмисників через якість та кількість персональних даних, які вони обробляють та зберігають. Цей сектор також переживає свою цифрову трансформацію, оскільки все більше і більше послуг доступні лише онлайн. Виклики різноманітні, як з точки зору різноманітності ІТ-послуг, так і розміру громад та бюджетів [9, с. 9].

Зростання загроз і кібератак в Україні з боку ворога, сприяють усвідомленню важливості кібербезпеки та потребі в досвідчених фахівцях [10]. Необхідно зрозуміти, що для цієї спеціальності викладання англійської мови повинно бути на вищому рівні. Зважаючи на широке коло роботи в цій сфері, логічним є і складна фахова термінологія. На наш погляд, її слід вивчати як базову, починаючи з 1 курсу безперервно. Мова живе і розвивається, в умовах стрімкого розвитку технологій та геополітичної ситуації фахова термінологія видається нескінченним потоком нової інформації для студентів. Тому, термінологію в секторі кібербезпеки логічніше вивчати у розрізі "English by Ukrainian".

Постановка завдання. Завданням даної роботи є опис категорій, присутніх в сфері кібербезпеки. Показати наскільки складною та розгалуженою є фахова мова цієї сфери. Довести, що такі складні категорії вимагають високого рівня знання англійської мови та що ці терміни слід впроваджувати у навчання від 1 курсу у вигляді тематичних глосаріїв та вчити їх у розрізі "English by Ukrainian" безперервно.

Виклад основного матеріалу. На часі наука і техніка, переживають значний розвиток, генерують новий лексикон. Такі тенденції ставлять перед викладачами іноземних мов нові завдання для покращення ефективності засвоєння фахової термінології. Лінгвісти в сфері кібербезпеки ведуть діалог з фахівцями та експертами під час розробки термінів та їх визначень, потім втручається фахівець з лінгвістики для полірування термінів та їх остаточної верифікації. Реалізація фахових термінів відбувається в рамках видання словників, глосаріїв та тезаурусів, максимально орієнтуючись на можливості студентів. Пропонуємо приклад тематичного глосарію англомовних термінів сектору кібербезпеки в розрізі запропонованої методики їх вивчення "English by Ukrainian" (табл. 1).

Розробка тематичних глосаріїв термінів сектору кібербезпеки в рамках вивчення англійської мови надає контекст для створення узгодженості

Таблиця 1

Тематичний глосарій "English by Ukrainian" в сфері IT

Firewall	Захист корпоративної мережі і пристроїв від атаки ззовні. Фільтрує з'єднання і дані, які проходять через Інтернет як всередині, так і зовні. Може бути апаратним, якщо є власний сервер, або у вигляді програмного забезпечення, встановленого на комп'ютері, і в більш загальному вигляді в інтрамережі або підключеного до Інтернету.
Cloud	Використання віддалених серверів через інтернет для зберігання даних і особливо доступу до них з будь-якого місця. Використовується для програмного забезпечення та обчислювальної потужності – хмарні обчислення.
Chiffring	Ця методика криптографії використовується з початку обчислень для захисту файлів від сторонніх осіб. Фахівцям з кібербезпеки безпеки, доцільно використовувати прикметник «зашифрований», а не англіцизм шифрування "Chiffring". Документ замикається алгоритмом, який буде залучати тисячі, якщо не мільйони, арифметичних операцій для його розшифрування. Необхідно розрізняти симетричне шифрування, де один і той же ключ шифрує і дешифрує, і асиметричне, де для відкриття файлу або електронного листа потрібен додатковий закритий ключ. Приватні месенджери, такі як WhatsApp, Telegram або Viber, покладаються на цю систему.
BYOD	BYOD або AP. Американська концепція «Користування власним пристроєм» (BYOD) теоретизує факт використання свого персонального комп'ютера, планшета або смартфона для роботи. Перевірка робочих електронних листів або віддалене управління бізнесом з незахищеної інтернет-мережі пов'язане з «кібернетичними» ризиками, які часто погано передбачаються. Ця плутанина між особистими та професійними пристроями помножує можливості зараження вірусом або програмами-вимагачами, які потім можуть поширитися по всій компанії. Особливо слід стежити за соціальними мережами.
Ransomware	«Програми-вимагачі» – вірус, який поширюється по електронній пошті і паралізує комп'ютер, замінений більш ефективною комп'ютерною атакою. Програми-вимагачі – це метод вимагання грошей віддалено. Перешкоджаючи заходам безпеки, невелика частина програмного забезпечення встановлюється на комп'ютери в мережі і шифрує всі дані, роблячи їх недоступними. Потім хакери надсилають суму викупу, має бути оплачена через криптовалюту, яку неможливо відстежити, в обмін на ключ дешифрування, який розблоковує файли.
Data leak	Витік даних. База клієнтів або книги замовлень, стають раптово доступні кожному в Інтернеті, можуть поставити усю структуру під загрозу. Збережені в Інтернеті на серверах, дані є конфіденційними та цікавлять як хакерів, так і конкурентів. Комп'ютерна атака або проста недбалість на погано захищеному сервері може стати причиною порушення таємниці фірми, даних, будь то у вигляді особистих даних або, ідентифікаторів і паролів.
Phishing	Фішинг – починається з невинного електронного листа або поста в Facebook від незнайомця, який пропонує відкрити посилання на приємну акцію або веселе відео. Потім ви повинні заповнити поля зі своїми особистими даними або розблокувати вміст, вказавши номер своєї кредитної картки. Сайти, які копіюють оригінал, також здатні зламати дані за лічені секунди. Цей прийом потім дає можливість перепродати інформацію.
DoS	Атака на відмову в обслуговуванні (DoS) Ця комп'ютерна агресія передбачає насичення мережі або веб-сайту, електронної комерції, лавиною одночасних автоматичних підключень. Хакери можуть домовлятися, щоб зупинити цю нищівну атаку.
DPO	Спеціаліст із захисту даних (DPO). Формалізований європейським законодавством з травня 2018 року та знаменитим Загальним регламентом захисту даних (GDPR), роль DPO полягає в забезпеченні дотримання компанією захисту даних. Завдяки своїм технічним навичкам та знанням законодавства він консультує внутрішньо чи зовні організації щодо гарантій та заходів безпеки, які необхідно впровадити. Обов'язковим є призначення DPO для компаній, незалежно від розміру, які масово обробляють персональні дані або тих, що працюють над конфіденційними даними, такими як расове або етнічне походження, членство в профспілках та інформація про здоров'я.
OIV	Оператор життєвого значення (OIV). Визначені державою і розділені на 12 секторів діяльності (енергетика, транспорт, охорона здоров'я і т.д.), зобов'язані за законом підтримувати бездоганний рівень IT-безпеки. Через свою стратегічну роль в економіці ці організації та компанії регулярно проходять аудит.

Джерело: власна розробка автора

засвоєння термінів. Це особливо важливо з огляду на різноманіття інформації в цій галузі та складності їх запам'ятовування. Вважаємо тематичні глосарій – групу термінів, які створюються для встановлення узгодженої та гармонізованої роботи зі студентами.

Висновки і пропозиції. Термінологія має вирішальне значення для будь-якої галузі навчання. Студентам часто доводиться витрачати багато свого часу на переклад та засвоєння технічних термінів. Точність термінології також є серйозною проблемою, оскільки технічний переклад, в якому не використовуються правильні терміни, може перешкодити їх розумінню. Вичерпний глосарій або лексикон, адаптований до теми заняття часто має вирішальне значення для засвоєння матеріалу у вивчення іноземної мови. Глосарій дає можливість встановити «спільну мову» для всієї групи та забезпечує послідовність і засвоєння та використання термінології, полегшуючи її розуміння.

В роботі запропоновано власний підхід до створення тематичного глосарію англомовної термінології в секторі кібербезпеки. Перш за все, необхідно зробити вичерпний аналіз всього дидактичного матеріалу згідно робочої програми, витягти термінологію, яка використовується мовою оригіналу, а потім надати пояснення термінів рідною мовою. Цей процес виснажливий, але він створює досить повний «словник» термінів, які можна використовувати на постійній основі. Створення базового глосарію, що містить основні ключові тематичні терміни, стане ефективним методом засвоєння такої складної фахової термінології.

Список літератури:

1. Зарницький А. В. Вербалізація збройного конфлікту в англомовному медіадискурсі. *Науковий вісник Міжнародного гуманітарного ун-ту*. 2018. Вип. 32 (3). С. 45–47.

2. Кирилюк О. Суспільно-політичні неологізми як віддзеркалення мовної картини воєнного протистояння. *Наукові записки НАУКМА*. 2018. Т. 1. С. 58–62. https://ekmair.ukma.edu.ua/handle/123456789/14602

3. Мілова О. Є. Скорочення як характерна риса військового тексту і шляхи їх перекладу. *Науковий вісник Міжнародного гуманітарного ун-ту.* 2018. Вип. 32 (2). С. 172–174.

4. Павленко О. В. Дослідження професійної підготовки фахівців з електроніки в Україні та США: базові поняття. Неперервна професійна освіта: теорія і практика. 2018. Вип. 3–4(56–57). С. 57−61.

5. Павленко О. В. Перспективні напрями застосування досвіду США до професійної підготовки фахівців з електроніки в Україні : метод. рек. Київ : КПІ ім. Ігоря Сікорського, 2020. 35 с. URL: https://doi.org/10.32839/2304-5809/2018-12-64-29 (дата звернення: 02.01.2023).

6. Павленко О. В. Професійна та іншомовна підготовка фахівців з електроніки: досвід США : метод. рек. Київ : КПІ ім. Ігоря Сікорського, 2020. 39 с. URL: https://doi.org/10.28925/2312-5829.2020.3.15 (дата звернення: 02.01.2023).

7. Павленко О. В. Сучасний стан підготовки фахівців з електроніки в закладах вищої освіти США. *Молодий вчений*. 2018. № 12(64). С. 111−114. URL: https://doi.org/10.32839/2304-5809/2018-12-64-29 (дата звернення: 02.01.2023).

8. Сібрук А., Барабаш О. Сучасний український науковий дискурс у мовознавчих працях. Гуманітарна освіта в технічних вищих навчальних закладах. 2019. № 40. С. 39–44. URL: https://doi.org/10.18372/2520-6818.40.14257 (дата звернення: 02.01.2023).

9. Сіденко В. Р. Глобальні структурні трансформації та тренди економіки України. *Економіка і прогнозування*. 2018. № 2. С. 7–29. URL: https://razumkov.org.ua/uploads/article/EP_18_1_37_uk.pdf (дата звернення: 02.01.2023).

10. Шишка Р. Б. Концепт безпеки в сучасній правовій доктрині. *Безпека як правовий концепт*: виступи учасників Всеукраїнської науково-практичної конференції (Київ, 20 квітня 2018 р.). Київ: Видавництво Ліра-К. 2018. С. 43–46. URL: https://www.academia.edu (дата звернення: 02.01.2023).

Botvyn T. M. REGARDING THE ENGLISH TERMINOLOGY SYSTEM OF THE CYBERSECURITY SECTOR OF UKRAINE UNDER THE CONDITIONS OF THE WAR STATE: DEFINITIONS ANALYSIS

The article analyzes the peculiarities of the acquisition and use of English-language terms in the cyber security sector of Ukraine and provides an overview of the main problematic points related to the topic of the article in war conditions. Among the difficulties faced by a specialist in a certain field, the generally accepted specific terminology plays a special blocking role. Students in the field of cyber security who, by virtue of their future profession, study English (the officially recognized language of cyberspace), do not escape these difficulties either. Therefore, there is a need to create thematic glossaries, where a specific lexicon is disclosed and a directory of definitions in the native language is added. Linguists believe that studying

terminology is more effective in contrast to the native language. At the same time, one should not forget about the need for tools and methods adapted for learning terminology in a certain field. The understanding of the vocabulary and thinking about language and terminology is an effective way to learn a foreign language and professional vocabulary. Most of the words used by a «non-linguist» in his field are technical terms with a traditional grammatical structure that are less abstract than other linguistic categories. However, they pose a problem in their assimilation. Thanks to the large number of definitions developed for certain sciences and the arsenal of relevant scientific literature, scientists have demonstrated that the use of specific terminology in a specific language eliminates all ambiguities and misunderstandings in the speech act. From the perspective of the described problems, one concludes that English-language terminology in the cyber security sector is a complex phenomenon and it is necessary to study it from the perspective of "English by Ukrainian". For this, it is necessary to compile English-language terms into thematic glossaries, consider each term in detail, and provide their definitions. This method of learning professional English enables the effective assimilation of complex and extensive terminology in the cyber security sector in the L1/L2 section ("English by Ukrainian"). One concludes that the difficulties associated with completely new terminology can be overcome by learning its definitions in the native language with the help of thematic glossaries before each new topic.

Key words: *martial law, the threat of cyber-attacks, cyber security, the language of cyberspace, terminology, linguistic problem.*