

## ЗАХИСТ ІНФОРМАЦІЇ В ХОДІ ПЕРЕКЛАДАЦЬКОЇ ДІЯЛЬНОСТІ З ЗАСТОСУВАННЯ ПРОФЕСІЙНИХ ЕЛЕКТРОННИХ РЕСУРСІВ

**Матвієнко Л. Г.**

Проблема забезпечення інформаційної безпеки є актуальною для всіх сфер сучасного суспільства, оскільки професійне інформаційне середовище передбачає взаємодію широкого кола користувачів, програмних продуктів та електронних ресурсів. Електронні засоби навчання, які проникають в усі ланки освітнього процесу, забезпечують розширення застосування комп'ютерних технологій в системі підготовки перекладачів, створюючи всесвітній освітній інформаційний простір. В роботі професійних перекладачів та в їх всебічній професійній діяльності широко застосовуються інформаційно-комунікаційні технології. Тому необхідним стає моніторинг безпечної взаємодії перекладача та електронних засобів перекладу, електронних ресурсів отримання, систематизації та інтерпретації матеріалів в інформаційному середовищі. Таке питання також є важливим як для якісної ґрунтовної підготовки майбутніх перекладачів в середовищі вищого навчального закладу, професійної діяльності окремих приватних перекладачів, які користуються в своїй роботі Інтернет ресурсами, так і для підприємств, що здійснюють комерційну діяльність в сфері перекладів (перекладацькі бюро, міжнародні компанії тощо). Професія перекладача, яка сьогодні стала масовою, проходить свої етапи внутрішніх змін та цифрової трансформації, що впливає на процес виконання перекладу та підготовку перекладачів у вищих навчальних закладах<sup>1</sup>. Підбір системи електронних ресурсів для здійснення автоматизованого та машинного перекладу стає одним з ключових витань реалізації перекладацької взаємодії на міжнародній арені. Зростання конкуренції на ринку перекладів змушує підприємства та компанії перекладати свої маркетингові та технічні матеріали різними мовами світу. Причиною зростання попиту на переклад з залученням інформаційно-комунікаційних технологій є розвиток ІТ-ринку як сегменту складних технічних перекладів.

Автоматизація праці перекладачів пов'язана з тим, що значну частину перекладів роблять на комп'ютерах за допомогою спеціалізованого програмного забезпечення, Інтернет-технологій. Також всі

---

<sup>1</sup> Долинський С. В., Скиба К. М. Інформаційні технології у професійній діяльності перекладача: навчальний посібник. Хмельницький : ХНУ, 2016. 75 с.

перекладацькі та міжнародні компанії представлені в Інтернет-просторі, що означає високу актуальність перекладу сайтів компаній різними мовами світу та їхню підтримку в робочому стані, що додатково складає окремих сегмент ринку перекладацької діяльності.

Інформаційна безпека передбачає забезпечення її конфіденційності інформації, її цілісності та доступності. Робота з будь-якими електронними джерелами передбачає долучення до перекладацьких матеріалів певного кола користувачів та розміщення інформації в мережі Інтернет, що часто тягне за собою висвітлення особистих чи конфіденційних даних. Питання захисту конфіденційної інформації під час перекладу є дуже актуальним, оскільки часто несанкціоноване потрапляння інформації компаній, з якими працюють перекладачі в широкий доступ викликає проблеми у роботі фірми, співпраці з партнерами та інвесторами чи втрату іміджу компанії на міжнародному ринку. Захист інформації під час перекладацької діяльності з електронними ресурсами передбачає системний підхід до інформаційної безпеки, адже інформація зберігається не лише на цифрових носіях, а й передається людьми. Тому під час використання електронного програмного забезпечення в ході підготовки майбутніх перекладачів в середовищі вищого навчального закладу, перекладацьким бюро та міжнародними компаніями важливо приділяти увагу захисту інформації, яка є у відкритому доступі, а також побудувати культуру кібербезпеки та кібергігієни.

## **1. Безпека інформації як невід’ємна складова організації перекладацької діяльності**

Комп’ютеризація перекладацьких дій є необхідною частиною процесу роботи сучасного перекладача. Впровадження електронних засобів у перекладі іншомовного матеріалу відіграє важливу роль у застосуванні інформаційно-комунікаційних технологій в науці. Не зважаючи на те, що останньою інстанцією корекції та затвердження перекладу іншомовних текстів є людина, автоматизація основних етапів усного та письмового перекладу на сучасному етапі розвитку суспільства залишається актуальною проблемою у роботі перекладачів. Такий попит на долучення електронних ресурсів до перекладацької діяльності передбачає, що перекладач буде дбати про безпеку матеріалів та даних з якими він працює. Інформаційна безпека під час роботи з електронним програмним забезпеченням регулюється міжнародними законодавчими актами, стандартами та положеннями. В Україні захист інформації забезпечується Законом України «Про інформацію» від 02.10.1992 № 2657-XII, Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-

ВР, Законом України «Про державну таємницю» від 21.01.1994 № 3855-ХІІ, Законом України «Про захист персональних даних» від 01.06.2010 № 2297-VI, Доктриною інформаційної безпеки України. Сучасною українською законодавчою системою продовжують розроблятися та впроваджуватися стандарти забезпечення збереження інформації під час взаємодії з електронними ресурсами.

З 2015 року діяльність на міжнародному ринку перекладів регулюється сертифікатом ISO 17100:2015 «Послуги перекладу – Вимоги до перекладу», виданим Міжнародною організацією зі стандартизації. Вона включає вимоги до захисту особистих даних та конфіденційної інформації, що передається під час перекладацької діяльності.

Визначення ролі параметра ефективності використання програмних засобів спеціального перекладацького призначення у перекладацькій діяльності визначається їх безпосереднім застосуванням у перекладацькому процесі та підготовці майбутніх перекладачів до професійної діяльності, що включає собівартість надання перекладацьких послуг, окупність застосування сучасного програмного забезпечення, наявність та складність встановлених апаратних та програмних перекладацьких засобів, з використанням Інтернет-ресурсів, скорочення витрат у технологічному процесі перекладу<sup>2</sup>.

Для бюро перекладів, які працюють з великими замовленнями або на субпідрядах іноземних перекладацьких фірм, програми автоматизованого перекладу виконують складний менеджмент роботи з проектами. Крім функцій, які сприяють швидкому перекладу, вони дають можливість працювати команді перекладачів одночасно, користуючись загальною базою термінів та глосарієм.

У великих перекладацьких та міжнародних компаніях питання захисту комерційних даних є одним з ключових і цією проблемою займаються ІТ-спеціалісти. Але на сьогодні і в маленьких бюро перекладів всі співробітники працюють в локальній мережі, до неї також підключені ресурси загального користування – словники, офісні програми, спеціалізоване програмне забезпечення. В динамічному інформаційному середовищі роботи перекладача навіть короткочасне порушення роботи корпоративної мережі чи втрата цінних файлів може спричинити серйозні проблеми в роботі компанії. Здобувачі вищої освіти перекладацьких спеціальностей у вищих навчальних закладах також працюють з широким колом онлайн та офлайн перекладацьких програм, словників, тренажерів, мобільних застосунків, що передбачають внесення та обробку інформації.

---

<sup>2</sup> Ferrara, Gabriela. Data Protection for Translators: A Practical Guide to Secure Translation. Routledge, 2019. 211 p.

Розкриття конфіденційної інформації за межами та в середині компанії необхідно чітко контролювати, щоб забезпечити комплексний захист інтересів компанії, інвесторів, партнерів чи споживачів товарів цієї фірми. Щоб забезпечити збереження конфіденційної інформації, важливо дотримуватися сучасних методів інформаційного захисту та аналізувати загрози. Обробка персональних даних у великих міжнародних компаніях автоматизована, враховуючи значні обсяги персональних даних, що знаходяться в системі. Постійно виникає потреба у моніторингу безпеки інформації, що забезпечує швидкість та надійність обслуговування клієнтів та партнерів. Керівництво компаній, що дбають про свій імідж та якість надання послуг під час перекладів внутрішньої та зовнішньої документації проводять регулярний ІТ-аудит. Такі методи необхідні для забезпечення конфіденційності, доступності та цілісності інформації, а також відповідності системи менеджменту інформаційної безпеки, законам, стандартам про захист даних та політику щодо обробки персональних даних та виявлення слабких місць в інформаційних системах.

Ключовим питанням перекладацької взаємодії з застосування сучасних інформаційно-комунікаційних технологій є інформаційна безпека.

Інформаційна безпека – це набір технологій, стандартів та адміністративних практик, необхідних для захисту даних. Інформаційна безпека включає збереження та захист інформації, а також її найважливіших елементів, у тому числі системи та обладнання, призначені для використання, заощадження та передачі цієї інформації<sup>3</sup>. В перекладацькому середовищі інформаційна безпека передбачає набір технологій, стандартів та методів управління, які необхідні для забезпечення якісної обробки та інтерпретації іншомовних матеріалів.

Мета забезпечення інформаційної безпеки – захистити інформаційних даних та підтримуючої інфраструктури від випадкового чи навмисного втручання, що може спричинити втрату даних або їх несанкціоновану зміну. Інформаційна безпека допомагає забезпечити безперервність автоматизованого чи машинного перекладу<sup>4</sup>.

В середовищі вищого навчального закладу інформаційна безпека формується шляхом обмеження будь-якого несанкціонованого чи іншим неналежним чином отриманого доступу, унеможливлення розкриття, знищення, зміни чи копіювання такої інформації.

---

<sup>3</sup> Віблій В. М., Смотр О. О. Безпека інформації у хмарних сховищах : thesis. 2019. URL: <http://hdl.handle.net/123456789/6228> (дата звернення: 20.03.2023)

<sup>4</sup> Заплотинський Б. А. Основи інформаційної безпеки : конспект лекцій. КПІВІП НУ «ОЮА», кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.

Головна мета дотримання інформаційної безпеки під час роботи перекладача з Інтернет-ресурсами та спеціальним програмним забезпеченням – захист інформації та інфраструктури, що її обробляє, від втрати чи витоку даних третім особам.

Захист інформації – діяльність, на запобігання витоку інформації, несанкціонованих і ненавмисних впливів на інформацію, з якою працює користувач.

Система захисту інформації – сукупність органів і виконавців, техніки, яка ними застосовується та об'єктів захисту інформації, що організована та функціонує за правилами та нормами, встановленими відповідними документами в галузі захисту інформації.

Політика безпеки щодо інформації – сукупність задокументованих правил, процедур, практичних прийомів у сфері безпеки інформації, якими керується організація у своїй інформаційній діяльності з електронними ресурсами.

Політика безпеки інформації під час використання спеціального перекладацького програмного забезпечення має містити такі складники: предмет, основні цілі та завдання; умови застосування політики безпеки та можливі її обмеження; опис позиції розробників програмного забезпечення щодо застосування політики безпеки інформації до особистих даних та інформації, що застосовується в ході перекладацької діяльності; права та обов'язки, а також ступінь відповідальності працівників та користувачів за виконання політики безпеки інформації; порядок дії у надзвичайних ситуаціях у разі порушення політики безпеки.

Політика безпеки – сукупність документованих правил, процедур, практичних прийомів або керівних принципів у сфері безпеки інформації, якими керується організація у своїй діяльності<sup>5</sup>.

Існує ряд правил, слідування яким забезпечить захист конфіденційних документів та особистих даних, з якими працює перекладач під час автоматизованого чи машинного перекладу.

Основні вимоги до підбору засобів захисту інформації в ході перекладацької діяльності з застосуванням інформаційно-комунікаційних технологій:

1. Підтримка стабільності. Зловмисник у будь-який момент може спробувати обійти модулі захисту даних, які його цікавлять.

2. Формування ціленаправленості. Інформація повинна захищатися у межах певної мети, яку ставить організація чи власник даних.

---

<sup>5</sup> Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. *Ефективна економіка*. № 4. 2015. URL: <http://www.economy.nayka.com.ua/?op=1&z=5514>

3. Забезпечення плановості. Усі методи захисту повинні відповідати державним стандартам, законам та підзаконним актам, що регулюють питання захисту конфіденційних даних.

4. Активізація оновлених програмних продуктів. Заходи для підтримки роботи та вдосконалення системи захисту повинні проводитись регулярно.

5. Комплексність та системність. Використання окремих модулів захисту або технічних засобів не діє. Необхідно застосовувати всі види захисту у взаємозв'язку, інакше розроблена система буде позбавлена сенсу.

6. Універсалізація процесів. Засоби захисту повинні бути обрані відповідно до існуючих у компанії каналів витоку.

7. Дотримання надійності. Усі прийоми захисту повинні надійно перекривати можливі шляхи до конфіденційної інформації з боку зловмисника, незалежно від форми подання даних.

Під час перекладу спеціальної документації з допомогою електронних ресурсів можна виділити ряд способів отримання доступу до інформації зловмисниками:

- Несанкціонований доступ – незаконне використання даних.

- Витік – неконтрольоване розповсюдження інформації за межі корпоративної мережі. Витік виникає через недоліки, слабкі сторони технічного каналу системи безпеки;

- Розголошення – наслідок впливу людського чинника. Санкціоновані користувачі можуть розголошувати інформацію, щоб передати її конкурентам або з необережності.

Комплексний захист інформації відбувається на базовому етапі розробки роботи компанії чи навчання здобувачів вищої освіти застосуванню інформаційно-комунікаційних технологій у подальшій професійній діяльності. Він включає кілька рівнів безпеки інформації, застосування яких необхідне під час роботи перекладача з особистими даними та матеріалами для перекладу.

У межах усіх рівнів обов'язкове застосування системи принципів захисту інформації в інформаційному середовищі вищого навчального закладу чи компанії, з якою співпрацює перекладач.

До основних принципів забезпечення інформаційної безпеки належать:

- Конфіденційність. Цей принцип означає введення в дію всебічного контролю та захисту інформації під час будь-яких дій з нею, для гарантії достатнього рівня безпеки з даними підприємства, активами та інформацією на різних етапах ділових операцій для запобігання небажаному або несанкціонованому розкриттю. Конфіденційність повинна

підтримуватися при збереженні інформації, а також під час різних операцій з нею (зокрема перекладацької діяльності).

– Цілісність. Цілісність інформації передбачає взаємодію між елементами управління, які пов'язані з забезпеченням зовнішньої та внутрішньої корпоративної інформації. Цілісність також гарантує запобігання спотворенню інформації під час перекладу даних та матеріалів різними мовами.

– Доступність. Доступність забезпечує надійний та ефективний доступ до інформації уповноважених осіб. Мережеве середовище має бути передбачуваним в контексті доступу до необхідної інформації та даних. Відновлення системи через збій є важливим фактором роботи перекладача з інформаційно-комунікаційними технологіями і не повинно негативно впливати на результат роботи спеціалістів та компанії.

Загрози інформаційної безпеки, які можуть впливати на професійну діяльність перекладача в ході застосування інформаційно-комунікаційних і перекладацьких технологій можна розділити на:

1. Природні (катаклізми, незалежні від людини: пожежі, урагани, повінь, удари блискавки тощо.).

2. Штучні, які також поділяються на:

– ненавмисні (вчиняються людьми з необережності чи незнання);

– навмисні (хакерські атаки, протиправні дії конкурентів, помста співробітників тощо).

3. Внутрішні (джерела загрози, що знаходяться усередині системи).

4. Зовнішні (джерела загроз за межами системи)<sup>6</sup>.

Під час роботи перекладача з сучасними спеціальними онлайн ресурсами перекладацького призначення виникають ризики, пов'язані з різними факторами взаємодії з інформацією:

– Крадіжка інформації. Такий тип порушення безпеки даних зазвичай відбувається задля подальшого застосування інформації в неправомірних цілях, шантажу, розповсюдження інформації на пірацьких сайтах, надання інформації посередникам.

– Підміна інформації, заміна даних недостовірними, збереження даних з метою подальшого застосування у власних цілях третіми особами, що не задіяні як замовники перекладу чи перекладачі.

– Програми-шпигуни, які відстежують дії користувачів на комп'ютері і в подальшому використовують отримані дані.

– Фішингові листи, які дозволяють шахраям вкрасти особисті дані. Присвоєння авторства також часто зустрічається, коли зловмисник,

---

<sup>6</sup> Заплотинський Б. А. Основи інформаційної безпеки : конспект лекцій. КПВіП НУ «ОЮА», кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.

зламавши електронну пошту, починає розсилати повідомлення від імені зламаного користувача.

– Розголошення інформації, що становить особисту чи комерційну таємницю. Таке часто трапляється при спробі помститися, зіпсувати репутацію.

Для забезпечення повного контролю за безпекою інформації під час роботи перекладача з онлайн та офлайн ресурсами перекладацького призначення необхідно всебічно охопити всі можливі ризики та загрози. Вирізняють такі види контролю за безпекою інформації в глобальній мережі Інтернет, що актуальні для роботи перекладача з інформаційно-комунікаційними технологіями та їх застосуванні в навчально-виховному процесі майбутніх перекладачів<sup>7</sup>:

### 1. Адміністративний.

Адміністративний вид контролю складається із затверджених комплексу процедур, стандартів та принципів. Він формує рамки для ведення організації перекладацького процесу та управління людьми. Закони та нормативні акти, створені державними органами, також є одним із видів адміністративного контролю. Інші приклади адміністративного контролю включають політику корпоративної безпеки, паролів та дисциплінарні заходи.

### 2. Логічний.

Логічні засоби управління (технічні засоби контролю за захистом інформації) побудовані на основі захисту доступу до інформаційних систем, програмного забезпечення, паролів, брандмауерів, інформації для моніторингу та контролю доступу до систем інформації.

### 3. Фізичний.

Це контроль середовища робочого місця та засобів інформаційно-комунікаційних технологій (комп'ютера, ноутбука чи планшета, колонок, принтера, мікрофону, сканера, тощо).

Комплексна інформаційна безпека перекладацької діяльності під час роботи з іншомовною документацією включає кілька складників. Перш за все, забезпечується антивірусна безпека і вибудовується ефективний захист мережі від зовнішніх і внутрішніх загроз.

Часто цінна для співробітників підприємства перекладацького спрямування інформація буває загублена, втрачена, знищена або перевернена не в результаті зловмисних дій конкурентів по бізнесу, а через звичайний вірус, підхоплений кимось із користувачів в Інтернеті. Саме тому під час роботи перекладачів з інформацією в мережі Інтернет, завантаженні робочих матеріалів, роботі з онлайн перекладачами

---

<sup>7</sup>Віблій В. М., Смотр О. О. Безпека інформації у хмарних сховищах : thesis. 2019. URL: <http://hdl.handle.net/123456789/6228> (дата звернення: 20.03.2023).



внутрішня мережа компанії чи навчального середовища має бути надійно захищена від зовнішніх і внутрішніх загроз. Для вирішення цього питання спеціальними фахівцями встановлюються фаєрволи, антивіруси, проксі. Вони сприяють ідентифікації та вчасному знищенню потенційних загроз, підхоплених перекладачами в ході взаємодії зі спеціальним програмним забезпеченням чи Інтернет-ресурсами.

Перед перекладачами як учасниками процесу обробки та передачі інформації постає питання максимально безпечного виконання цих завдань під час застосування електронних ресурсів. Основними обов'язками перекладачів під час роботи з захисту інформації в ході перекладацької діяльності з застосуванням інформаційно-комунікаційних технологій є:

– Зберігання комерційної та виробничої таємниці, а також іншої інформації, яка стала доступною внаслідок трудових відносин, у тому числі щодо членів сім'ї чи друзів. Це стосується інформації про комерційних партнерів та клієнтів, яка не є загальнодоступною. Зобов'язання перекладача про збереження комерційної таємниці залишається чинним після припинення трудових відносин.

– Захист конфіденційної інформації компанії від ненавмисного розкриття.

– Захист конфіденційної інформації від крадіжки, використовуючи лише надані компанією інструменти та програмне забезпечення, а також створюючи та зберігаючи паролі відповідно до політики та стандартів компанії.

– Дотримання політики і стандартів щодо IT-інфраструктури та інформаційної безпеки, а також політики щодо розкриття інформації в соціальних мережах або по інших каналах.

Ще однією невід'ємною складовою захисту інформації під час роботи перекладачів з електронними ресурсами є шифрування і захист даних від несанкціонованого доступу. Для того, щоб їх забезпечити, необхідно налаштувати систему таким чином, щоб сторонні особи не змогли б скористатися важливою інформацією, що становить комерційну таємницю. Доступ до цих даних також повинен бути закритий для самих перекладачів, оскільки для виконання їх власних завдань ця інформація не потрібна.

Засоби захисту інформаційної безпеки – це набір технічних застосунків, приладів різного характеру, які перешкоджають витoku інформації та виконують її функцію<sup>8</sup>.

Засоби захисту інформації поділяються на:

---

<sup>8</sup> Ferrara, Gabriela. Data Protection for Translators: A Practical Guide to Secure Translation. Routledge, 2019. 211 p.

– Організаційні. Це сукупність організаційно-технічних (забезпечення комп'ютерними приміщеннями, налаштування кабельної системи тощо) та організаційно-правових (законодавча база, статут конкретної організації) активів.

– Програмні. Ті програми, які допомагають контролювати, зберігати та захищати інформацію та доступ до неї.

– Технічні (апаратні). Це технічні види пристроїв, які захищають інформацію від проникнення та витоку.

– Змішані апаратно-програмні. Виконують функції як апаратних, і програмних засобів.

Забезпечення захисту та безпеки особистої та конфіденційної інформації має бути першочерговим завданням перекладача під час роботи з інформаційно-комунікаційними технологіями перекладацького спрямування. Порушення правил роботи з такими даними може призвести до серйозних негативних наслідків у роботі компанії та позначитися на репутації перекладача та замовника перекладу. На вибір відповідних засобів захисту інформації впливають багато чинників, зокрема сфера діяльності компанії, її розмір, технічне забезпечення і навіть знання співробітників у сфері інформаційної безпеки.

## **2. Специфіка організації**

### **автоматизованого та машинного перекладу**

Несанкціоноване розповсюдження конфіденційних даних може відбуватися в ході автоматизованого чи машинного (автоматичного) перекладу з застосуванням інформаційно-комунікаційних технологій.

Насьогодні машинний та автоматизований переклад у поєднанні з подальшим редагуванням тексту стає конкурентоздатним перекладацьким напрямком, в основі якого лежать стратегічні спрямованості перекладацької діяльності та рекомендації різногалузевих фахівців. Не можна не відзначити постійний, інноваційний прогрес у сфері комп'ютерних технологій та усвідомлення необхідності їх використання. Таким чином, професійні перекладачі освоюють корисні та продуктивні надбання постійного розвитку інформаційних систем, і ефективність від такої взаємодії людини і машини у світі перекладу, постійно та динамічно зростає.

Головною перевагою машинного перекладу, порівняно з перекладом вручну, є те, що він виконується комп'ютером і, отже, швидше, ніж за допомогою людини. Таким чином, економиться час при перекладі великих обсягів інформації. До того ж такий вид перекладу дешевший, ніж переклад вручну. Крім того, використовуючи системи машинного перекладу, перекладач також може перевести зміст будь-якого вебсайту

або запит пошукової системи. Це особливо ефективно при комбінаціях мов, які відносяться до однієї мовної сім'ї (наприклад, іспанська/португальська, іспанська/французька, іспанська/італійська).

Машинний (автоматичний) переклад – переклад, виконаний комп'ютерною програмою<sup>9</sup>. Машинний переклад може бути представлений як у вигляді вебверсії, так і програмним забезпеченням, яке потрібно встановлювати на носії інформації (комп'ютері, ноутбучі, планшети, телефони). Машинний переклад виконує сама програма, а людина тільки редагує отриманий результат. Основною метою такого перекладу є замінити працю людини, отримуючи при цьому швидкий переклад низької якості. Перекладач має опосередковану участь у роботі з машинним перекладом, а саме<sup>10</sup>:

- передредагування – підготовка тексту до перекладу, розбиття та видалення некоректних еквівалентів;

- - постредагування – перекладач виправляє результат, зроблений програмою;

- інтерредагування – людина чи перекладач втручається у роботу програми.

Також система обробки може бути змішаною і включати всі етапи.

До основних переваг машинного перекладу іншомовної інформації можна віднести<sup>11</sup>:

- Легкодоступність. Програмне забезпечення для здійснення машинного перекладу пропонується онлайн у вільному доступі чи з установкою на носії інформації.

- Зручність та швидкість. Сучасне програмне забезпечення спеціального призначення одразу перекладає документ чи фрагмент документу, що пришвидшує та спрощує перекладацьку діяльність.

- Безкоштовний доступ. Значна частина програм для машинного перекладу безкоштовна і не передбачає значних затрат часу на реєстрацію. Це дозволяє швидко обробляти великі обсяги інформації з подальшим її редагуванням та форматуванням.

- Універсальність. Програмне забезпечення для здійснення машинного перекладу має зручний інтерфейс для максимального доступу користувача до всіх функцій та інструментів.

---

<sup>9</sup>Novak B. Machine Translation URL: Advantages and Disadvantages: <http://dlsdc.com/blog/machinetranslation-advantages-and-disadvantages>

<sup>10</sup>Geisser Daniel The Impact of Technology on Translation Quality. *The Journal of Specialised Translation*. 2018. № 29. P. 107–126.

<sup>11</sup>Яфтумова А. А. Системи машинного перекладу як складова підготовки майбутніх перекладачів. *Діалог мов і культур у сучасному освітньому просторі* : І Всеукраїнська наукова інтернет конференція. Суми, 2017. С. 573–576.

Більшість програм для автоматичного перекладу мають багато додаткових корисних опцій, що дозволяють: використовувати голосове введення; отримувати посилання на переклад; копіювати перекладений текст для подальшої роботи з ним; бачити транскрипцію; прослуховувати правильну вимову; перевіряти орфографію; вносити виправлення.

В свою чергу застосування в перекладацькому процесі спеціалізованого програмного забезпечення для здійснення машинного перекладу має ряд недоліків та труднощів:

– Необхідність постійного доступу до мережі Інтернет (для онлайн сервісів).

– Неточність перекладу (фразеологізми, спеціальна термінологія тощо). Основний недолік машинного перекладу – низька якість вихідного іншомовного тексту. Ця проблема виникає тому, що сервіси автоматичного (машинного) перекладу здебільшого перекладають текст дослівно, без розуміння інформації та врахування контексту. Вони можуть передати загальну суть тексту, однак допускають лексичні та граматичні помилки. У деяких випадках зміст окремого речення чи навіть усього тексту може зовсім спотворитися після перекладу. Машинний переклад не може враховувати контекст і адекватно обрати перекладацькі еквіваленти у невизначених ситуаціях.

Розробники програм з машинного перекладу постійно удосконалюють програмне забезпечення для підвищення якості перекладу та збільшення кількості мов в середовищі перекладацької взаємодії.

Автоматизований переклад – це переклад, виконаний не машиною, а людиною, але з використанням спеціального перекладацького програмного забезпечення<sup>12</sup>. Під таким програмним забезпеченням найчастіше розуміються САТ-програми (Computer Assisted/Aided Translation). Вони ґрунтуються на технологіях перекладацької пам'яті. САТ-програми зараз використовують багато перекладачів. В автоматизованому перекладі основну роботу виконує перекладач, а спеціальні програми виступають лише як допоміжний інструмент. Його головною метою є скорочення часу процесу перекладу, забезпечення диференціації термінів та загальної відповідності матеріалу перекладу.

Системи автоматизованого перекладу – це збірне визначення спеціалізованих програм та Інтернет-сервісів, які використовують перекладачів в процесі роботи<sup>13</sup>. Вони добре підходять для роботи над художніми, юридичними та технічними перекладами. До них відносяться:

---

<sup>12</sup> Williams P., Sennrich R., Post M., Koehn P. Syntax-based Statistical Machine Translation. 2016. 208 с.

<sup>13</sup> Ibid.

– Окремі або вбудовані редактори, які допомагають автоматично перевірити граматику тексту та правопис слів.

– Програмне забезпечення, таблиці, текстові редактори, що забезпечують управління термінологією (MultiTerm, Termex тощо).

– Програмне забезпечення, за допомогою якого здійснюється менеджмент перекладацьких проєктів.

– CAT-інструменти, що використовують ТМ (Translation Memory – Пам'ять перекладів), які включають зразки раніше перекладених текстів або речень. До найпопулярніших програм такого типу відносяться: Trados, Déjà Vu, MemoQ, MemSource, Wordfast.

– Корпуси, що являють собою систему документів з використанням однієї або декількох мов. З їхньою допомогою складається стислий опис вживання слів і виразів у конкретних випадках або з урахуванням будь-якої певної предметної теми.

В даний час розрізняють три типи систем автоматичного перекладу:

– Системи на основі граматичних правил (Rule-Based Machine, Translation, RBMT).

– Статистичні системи (Statistical Machine Translation, SMT).

– Нейронний автоматичний переклад.

Системи автоматичного перекладу на основі граматичних правил (RBMT) були першими комерційними системами. Ці системи дозволили уникнути послівного перекладу. На основі розроблених лінгвістичних правил системи автоматичного перекладу стали здатні змінювати порядок слів у реченні, обирати значення залежно від контексту.

Системи автоматичного перекладу на основі правил здійснюють аналіз тексту, що використовується у процесі перекладу. Переклад проводиться на основі вбудованих словників для даної мовної пари, охоплюють семантичні, морфологічні, синтаксичні закономірності обох мов. На основі цих даних вихідний текст послідовно, речення за реченням, перетворюється на текст на потрібній мові. Основний принцип роботи таких систем – зв'язок структур вихідного та кінцевого текстів. Найбільш поширеною програмою цього типу є PROMT.

В застосуванні систем на основі граматичних правил виділяється багато переваг: граматична та синтаксична точність; стабільність та передбачуваність результату; можливість налаштування на специфічну предметну область.

До недоліків систем на основі граматичних правил відносять: необхідність створення, підтримки та постійного оновлення лінгвістичних баз даних; трудомісткість створення такої системи в спеціальному інформаційному середовищі; висока вартість технічного

обладнання для створення та застосування таких систем у перекладацькій діяльності.

Статистичні системи є підвидом методу, заснованого на корпусах тексту (*corpus-based machine translation, CBMT*). У своїй роботі вони використовують статистичний аналіз. В систему завантажуються двомовний корпус текстів (що містить велику кількість тексту вихідною мовою та її «ручний» переклад на потрібну мову), після чого система аналізує статистику міжмовних відповідностей, синтаксичних конструкцій тощо. Передбачається, що слова з найбільшою частотністю дають найточніший переклад. Чим більший словник усередині мовної пари і чим точніше він складений, тим кращий результат статистичного автоматичний перекладу. З кожним новим перекладеним текстом покращується якість наступних перекладів. прикладами даного типу автоматизованих перекладачів є Google Translate та META<sup>14</sup>.

До переваг статистичних систем належать: швидкість налаштування програмного забезпечення на основі цих систем; легкість додавання нових напрямків перекладу за рахунок поширеного та безкоштовного програмного забезпечення для перекладацької діяльності.

Серед найбільш значущих недоліків можна виділити: наявність численних граматичних помилок, що виникають через неможливість врахування програмним засобом контексту матеріалу, з яким працюють системи; нестабільність перекладу за рахунок постійної динаміки словникового складу мов; недостатня технічна забезпеченість.

Нейронний автоматичний переклад – це відносно новий тип систем, що допомагає вирішити проблеми автоматизованого перекладу. Цей тип перекладу набуває поширення в останні роки, в зв'язку з розвитком та удосконаленням інформаційно-комунікаційних технологій перекладацького спрямування. Нейронний переклад схожий на статистичний, так як також у своїй основі містить аналіз паралельних даних і на основі нього формує певні залежності та закономірності. Але він має кардинально інший принцип роботи. Функціонування цього методу засноване на використанні нейронних мереж, обчислювальних моделей, що за своєю структурою нагадують будову людського мозку, в яких сигнал поширюється через послідовні шари елементів, що імітують нейрони. Саме завдяки таким системам перекладу можливе врахування контексту та правильної побудови речення, в залежності від типу та структури мови.

Програми автоматизованого перекладу CAT-tool – це цілий набір інструментів, які виводять послуги, що надаються перекладачем, на

---

<sup>14</sup> Katan David Translation as Intercultural Communication: Towards a Theory of Translating. Routledge, 2018. 132 p.

новий рівень щодо ціна-якість-швидкість. В середовищі програм для автоматизованого перекладу можливо: перевірка правопису; перевірка граматики; робота з термінами, коли перекладач керує своєю власною; термінологічною базою; робота зі словниками; робота з програмами-індексторами, які працюють із запитами та звертаються до раніше перекладених матеріалів; керування пам'яттю перекладів, де можна збирати базу сегментів тексту з перекладами англійською та іншими мовами.

Вони можуть бути реалізовані у вигляді безкоштовних програм, які потрібно встановлювати на комп'ютер (Мемо-Т та МАТ); платних програми для десктопу з доступом до сервера (дорогий інструмент) для роботи в команді над загальним проектом перекладу (SDL Trados, MemoQ, Star Transit); хмарних інструментів (Memsources та smartCAT), які працюють через браузер. Також це можуть бути надбудови і макроси, вбудовані в текстові редактори.

Машинний переклад також представлений набором програм та Інтернет-сервісів. Найбільш популярні з них: PROMT, Google translate, METAПерекладач тощо.

Організація застосування машинного та автоматизованого перекладу в ході перекладацької взаємодії потребує від спеціаліста ґрунтовного дослідження спеціального програмного забезпечення та добору найбільш безпечного та корисного програмного засобу для досягнення еквівалентності та адекватності перекладу. Системи автоматизованого та машинного перекладу спрощують та пришвидшують переклад інформації, але кожен з таких перекладів потребує глибокого аналізу перекладачем та редагування.

### **3. Аналіз програмного забезпечення перекладацького спрямування**

Контроль та систематизація інформації, що використовується для навчальної та професійної діяльності забезпечує доступ перекладачів та здобувачів вищої освіти перекладацьких спеціальностей до корисних електронних ресурсів<sup>15</sup>. Фільтрування навчальних сайтів та електронних засобів навчання з боку викладача вищого навчального закладу забезпечує професійну спрямованість здобутої інформації в мережі Інтернет та в подальшій професійній діяльності.

Збереження інформації в ході перекладацької діяльності передбачає підбір доцільного електронного програмного забезпечення.

Програмне забезпечення для перекладу – програми, які здійснюють повністю автоматизований та машинний переклад<sup>4</sup>. Головним

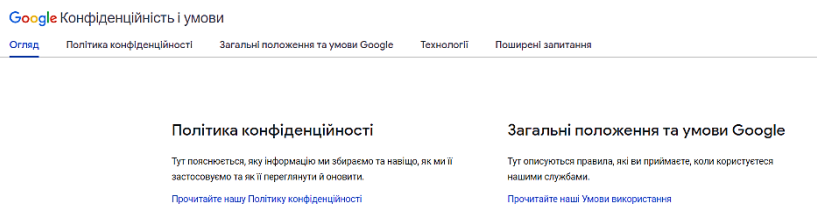
---

<sup>15</sup>Translator program: pros and cons. URL: <https://taskforce.ua/uk/programa-perekladachplyusy-i-minusy> (дата звернення: 16.03.2023).

критерієм програми є якість перекладу. Під час роботи перекладача з такими програмами важливими аспектами добору є перш за все її безпечність, а вже потім зручність інтерфейсу, легкість інтеграції програми з іншими засобами обробки документів, вибір тематики, утиліта поповнення словника. З появою глобальної мережі Internet основні виробники систем машинного перекладу включили в свої продукти Web-інтерфейси, забезпечивши при цьому їх інтеграцію з іншим програмним забезпеченням і електронною поштою, що дозволило застосовувати механізми електронних засобів перекладу для роботи з Web-сторінками, електронною кореспонденцією та онлайн переговорами.

Розглянемо кілька найпоширеніших онлайн перекладачів у сучасному інформаційному просторі, що дають можливість одразу перекладати інформацію з інших мов на українську і навпаки.

Найпопулярнішим ресурсом для перекладів є Google Перекладач (<https://translate.google.com>), який дозволяє перекладати 51 мовою фрагменти тексту чи окремі документи. Сервіс є безкоштовним, зі зручним інтерфейсом та швидкою дією. Перекладач має змогу копіювати перекладену інформацію на інші носії чи поширювати її через гугл сервіси. Крім того, перекладач містить опцію «показати транслітерацію», що особливо важливо в ситуаціях, коли необхідно працювати зі складними словами або необхідно правильно написати адресу на конверті при відправці листа за кордон. Google Перекладач є глобальною програмою і не містить спеціалізованого поділу перекладу відповідно до різних галузей.



**Рис 1. Скрин вкладок з моніторингу безпеки інформації в системі Google-перекладача**

Значну увагу цей онлайн перекладач приділяє конфіденційності та безпеці інформації. В середовищі перекладача містяться вкладки, що передбачають моніторинг підозрілих програмних продуктів, фішингу, завантаження особистої інформації тощо (Рис. 1). В полі безпеки онлайн перекладача зазначається, що дані про дії дозволяють підвищувати



зручність продуктів та сервісів. Дані про дії користувачів, збережені в обліковому записі Google, використовуються для персоналізації продуктів Google. Це дозволяє розробникам онлайн перекладача отримувати автоматичні рекомендації та швидше знаходити потрібний контент. Користувач онлайн перекладача може в будь-який момент обрати інформація, про які дії буде додаватися до облікового запису, завантажити свої дані та видалити збережену інформацію.

Доступ до даних онлайн перекладача Google дозволяє: забезпечувати коректну роботу сервісів; відстежувати збої та усувати проблеми, про які повідомляють користувачі; вдосконалювати послуги. Наприклад, знаючи, в яких пошукових запитах часто бувають друкарські помилки, розробники можуть покращувати перевірку правопису в новіших версіях.

Онлайн сервіс «Мета Перекладач» (<https://translate.meta.ua>) дає змогу працювати з 7 мовами, майже миттєво перекладати незначні за обсягом тексти. Перевагою сервісу є сортування інформації та вихідного тексту перекладу відповідно до певної галузі (закони, туризм, фінанси тощо). Вебпрограма має простий інтерфейс та є безкоштовною. В середовищі програми можливо застосування додаткових інструментів редагування та форматування іншомовного тексту. Інтерфейс цього перекладацького онлайн сервісу містить діалогове вікно з порадами для досягнення максимальної еквівалентності та адекватності текстів (обрати тематику тексту, технічні поради щодо правильного введення та виведення тексту, максимально доцільне розташування та добір засобів перекладу).

Цей онлайн перекладач також дотримується політики конфіденційності ресурсу МЕТА щодо персональних даних та обробки інформації (рис 2.) В середовищі перекладача чітко визначено правила використання та обробки особистих даних та конфіденційної інформації: «МетаПерекладач з повагою відноситься до особистої (персональної) інформації всіх без винятку фізичних осіб, які використовують та(або) відвідують Сайт, а також тих осіб, які в будь-якій формі користуються сервісами Сайту. Зважаючи на це, ми прагнемо захищати конфіденційність персональних даних (відомостей та сукупностей відомостей про фізичну особу, за допомогою яких користувач ідентифікований або може бути конкретно ідентифікований), тим самим створивши і забезпечивши максимально комфортні умови використання Сайту та сервісів Сайту для кожного користувача»<sup>16</sup>. Крім безпеки роботи з персональними даними під час онлайн перекладу матеріалів

---

<sup>16</sup>The five best free translation programs URL: [https://its.at.ua/publ/programni\\_zasobi/p\\_jat\\_krashhikh\\_bezkoshtovnikh\\_program\\_dlja\\_perekladu/2-1-0-27](https://its.at.ua/publ/programni_zasobi/p_jat_krashhikh_bezkoshtovnikh_program_dlja_perekladu/2-1-0-27) (дата звернення: 04.03.2023).

в середовищі Мета Перекладача моніториться використання файлів соокіе, взаємодія сайту з іншими електронними ресурсами. Це дозволяє досягнути максимального захисту матеріалів, з якими працює перекладач та зберегти конфіденційність особистих даних, з якими він взаємодіє в ході перекладацької діяльності.

## Політика конфіденційності

Політики конфіденційності та захисту персональних даних  
Meta.ua (надалі - «Політика»)

Зміст:

- 1 [Загальні положення](#)
- 2 [Види оброблюваних персональних даних](#)
- 3 [Обробка персональних даних](#)
- 4 [Мета обробки/використання персональних даних](#)
- 5 [Термін зберігання персональних даних](#)
- 6 [Використання файлів cookie](#)
- 7 [Взаємодія Сайту з іншими ресурсами](#)
- 8 [Безпека дітей](#)
- 9 [Взаємодія МЕТА з третіми особами щодо персональних даних](#)
- 10 [Конфіденційність активності суб'єкта персональних даних на Сайті](#)

### Рис 2. Скрин умов конфіденційності під час роботи з онлайн перекладачем МЕТА

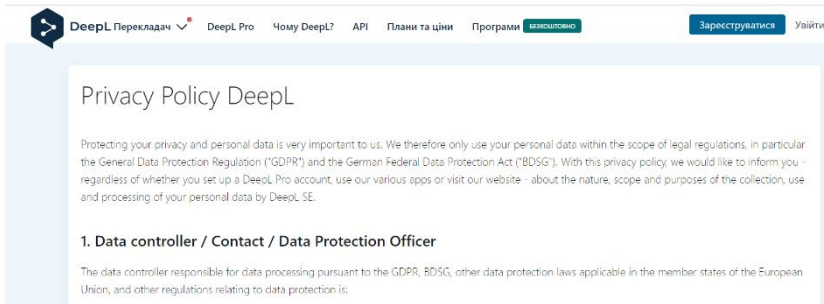
Широкого поширення серед перекладачів набуває перекладацький онлайн ресурс DeepLПерекладач. Програмний засіб має інтерфейс, адаптований до сучасних потреб спеціалістів з перекладу, ряд корисних супровідних інструментів. З його допомогою можна здійснювати повний машинний переклад фрагментів тексту чи документу, а також в ньому міститься словник, де перекладач має змогу перевірити конкретне значення слова. Сервіс дозволяє перекладачам створювати власний глосарій та користуватися вже створеними іншими спеціалістами<sup>17</sup>. Електронний ресурс працює з перекладами на 31 мову та має суміжні додатки для Windows, Android, Chrome. Даний перекладач крім браузерної версії має мобільну, що представлена у вигляді за стосунків IOS та Android. У браузерній версії онлайн перекладача DeepL є можливість перекладу файлів у форматі docx, pdf, pptx розміром до 5 Мб. Цю функцію можна застосовувати під час роботи з невеликими бізнес-документами, науковими статтями. Результат перекладу

---

<sup>17</sup> Translator program: pros and cons. URL: <https://taskforce.ua/uk/programa-perekladachplyusy-i-minusy> (дата звернення: 16.03.2023).

подається у вигляді окремого файлу з перекладом статті. У мобільному додатку перекладач має можливість перекладу аудіо матеріалів та знімків з камери з подальшою транслітерацією тексту. У додатку для Windows можна перекладати скріншоти. Це корисний інструмент для документів, у яких відсутній режим виділення тексту або встановлений захист на виділення тексту.

Вкладка щодо політики безпеки інформації містить кілька розгалужень, що передбачають застосування спеціальних програм з захисту даних, опис сфери захисту даних, безпека під час роботи з текстами та перекладами, захист інформації під час роботи з сервісом DeepL Write Alpha/Beta, створення облікового запису DeepL і підписки на DeepL Pro, взаємодія з конфіденційною інформацією в середовищі онлайн перекладача (рис. 3).



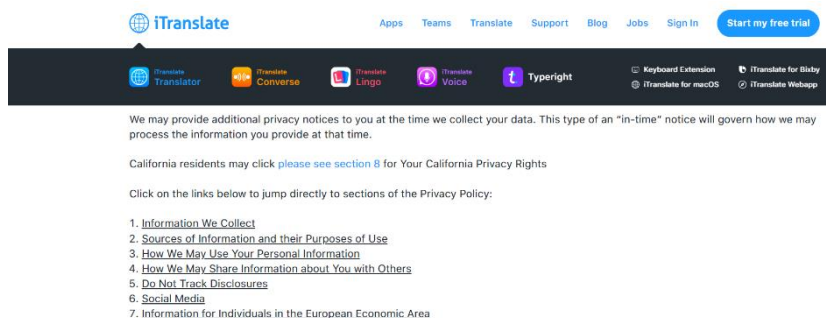
**Рис 3. Правила роботи з конфіденційною інформацією в середовищі онлайн перекладача DeepL.**

Окремим розділом виділено умови захисту інформації під час перекладу документів. Ця вкладка містить роз'яснення щодо захисту даних під час роботи з перекладом документів .docx і .pptx за допомогою DeepL Translator і DeepL Pro; перекладом PDF-документів за допомогою DeepL Translator і DeepL Pro; правила тимчасового зберігання метаданих під час перекладу документів. В середовищі онлайн перекладача зазначається, що якщо спеціаліст працює з перекладом спеціальних документів, увійшовши у свій обліковий запис DeepL Pro, надіслані тексти оброблятимуться лише тимчасово та видалятимуться після завершення процесу перекладу, включаючи самі переклади, відповідно до політики конфіденційності).

Програма iTranslate є зручною як мобільний додаток, так і як спеціальний програмний засіб для персонального комп'ютера чи ноутбука. Програмний засіб співпрацює з 101 мовою, дає змогу перекладу голосових повідомлень та тексту, але в автономному режимі

можна перекладати лише англійською. В середовищі перекладача існує опція збереження історії використання. Програма може працювати як онлайн, так і без доступу до мережі Інтернет, що дозволяє перекладачам знаходити перекладацькі еквіваленти в будь-якому місці. Програмне забезпечення для перекладацької діяльності iTranslate використовує сучасні технології та підтримує голосове введення. Віджет швидкого доступу можна закріпити на головному екрані, тому перекладач може дуже швидко відкрити застосунок. До спеціальних інструментів електронного перекладача, які пришвидшують та автоматизують процеси перекладу іншомовних матеріалів можна віднести: голосове введення та виведення інформації, де користувач може вибрати чоловічий чи жіночий голос для озвучення тексту, швидкість читання; латинська транслітерація; відображення різних значень слова, залежно від спеціальної сфери застосування. Крім виконання миттєвого перекладу, додаток також дозволяє зберегти систему фраз конкретними мовами в списку найбільше використовуваних. Перекладач має вільний доступ до них і потрібний час і у необхідній ситуації.

В політиці конфіденційності розробники програми окреслили, які дані вони можуть запозичити та яким способом (рис 4.) У цій вкладці розміщені пункти, які передбачають максимальний моніторинг інформації та забезпечення її повного захисту під час роботи з іншомовними матеріалами: інформація, яка збирається і систематизується онлайн ресурсом; джерела інформації та цілі їх використання; способи використання особистої інформації; відстеження поширення конфіденційної інформації; соціальні мережі та медіа; вибір конфіденційності в мережі Інтернет тощо.



**Рис. Скрин правил обробки інформації в електронному середовищі iTranslate в межах політики конфіденційності**

Кожен з виробників спеціального програмного забезпечення дбає про захист інформації в межах політики конфіденційності. Але, всі онлайн-перекладачі збирають контент, який перекладають користувачі. Насамперед його використовують як матеріал для навчання комп'ютерних перекладачів. Крім того, подібні дані – це величезне джерело знань, що дозволяє отримувати корисну інформацію для реклами, маркетингу і навіть шпигунства. Також онлайн додатки залишають за собою право використовувати контент на свій розсуд. Тому завантажувати в систему онлайн перекладачів конфіденційну чи важливу інформацію компанії не варто, оскільки це може спровокувати відкриття її у загальному доступі і виникненню проблем.

Застосування під час машинного чи автоматизованого перекладу навіть ліцензійних та перевірених електронних перекладачів та електронних словників дозволяє убезпечити себе та замовників від неточностей в перекладі, але наражає на небезпеку поширення конфіденційної інформації та системи даних.

Альтернативним рішенням машинного і автоматизованого перекладу конфіденційної інформації компаній та особистих даних є корпоративні сервери та програмні засоби, які надають доступ до всієї інформації лише в межах компанії. Сервіс автоматичного перекладу, що працює в локальній мережі компанії, має бути такою самою нормою, як і корпоративна пошта. До таких сервісів належать SDL, Systran, PROMT. Ці рішення відповідають усім вимогам безпеки та мають багато переваг у порівнянні з перекладацькими онлайн-сервісами.

Провідні міжнародні компанії використовують передові підходи в галузі безпеки для посилення захисту від кіберзагроз<sup>18</sup>:

– Кожен офіс повинен мати захищене VPN-підключення та бути захищений міжмережевими екранами.

– Персонал повинен мати доступ тільки до тих програм, за які він відповідає, а також мати обмежений доступ всередині програми.

– Кожен сервер необхідно розташовувати у сертифікованому відповідно до ISO 27001 центрі обробки даних і мати власний мережевий екран та антивірус.

– Весь трафік, що входить і виходить із корпоративної мережі, необхідно шифрувати і постійно відстежувати. Під час виявлення незвичайної поведінки повинні вживатися негайні заходи.

Для забезпечення інформаційної безпеки в перекладацькій діяльності в середовищі компаній фахівці рекомендують застосування стратегії ешелонованої оборони Defense in Depth (DiD), що включає набір

---

<sup>18</sup> Geisser Daniel The Impact of Technology on Translation Quality. *The Journal of Specialised Translation*. 2018. № 29. P. 107–126.

багатошарових та дублюючих процедур та засобів фізичного та адміністративного контролю, а також технічний захист від різних загроз, такі як:

– Брандмауер. Фахівці з безпеки інформації використовують брандмауери, які фокусуються на виявленні та блокуванні шкідливої активності, націленої на конкретну програму або всю мережу.

– Сегментація мережі. Можливо розділили внутрішні корпоративні мережі на логічні підмережі на основі бізнес-процесів, з якими працює перекладач. Ці мережі не в змозі взаємодіяти безпосередньо один з одним, що забезпечує захист інформації навіть у тому випадку, якщо частина мережі зазнала атаки.

– Управління оновленнями. Профільні спеціалісти мають стежити за станом інформаційного середовища та проводити регулярне оновлення програмного забезпечення, операційних систем та мережного обладнання, для усунення ураження небезпечними програмами та користувачами, які можуть призвести до небажаного доступу до комп'ютерних систем або мереж.

– Моніторинг система (IDS/IPS). Доцільним для збереження безпеки інформації є застосування системи виявлення та запобігання вторгненням, яка попереджає утворення потенційно шкідливого мережевого трафіку та блокує шкідливу активність у мережі або на робочому столі користувача.

– Система DLP. Міжнародні компанії часто впроваджують систему запобігання витоку інформації, щоб запобігти передачі кінцевими користувачами (зокрема перекладачами) конфіденційної та важливої інформації неавторизованим користувачам за межами компанії.

– Антивірусне програмне забезпечення повинне бути встановлено на всіх комп'ютерах користувачів в мережі компанії, в тому числі на ноутбуках і мобільних пристроях користувачів, і забезпечувати антивірусний захист.

– Управління привілейованим доступом (PAM). Паролі мають зберігатися та поширюватися у безпечному сховищі, регулярно перевірятися. Під час роботи перекладача з електронними ресурсами варто застосовувати багатофакторну авторизацію в усій системі і доступу до даних. Відповідно до принципу найменших привілеїв користувачам, системам та процесам повинен надаватися доступ лише до тих ресурсів, які необхідні для виконання поставлених завдань (перекладу).

Підбір сучасного програмного забезпечення для моніторингу безпеки інформації забезпечується комплексністю його введення<sup>19</sup>:

---

<sup>19</sup> Ferrara Gabriela Data Protection for Translators: A Practical Guide to Secure Translation. Routledge, 2019. 211 p.

– Антивірусні програми – програми, які борються з комп’ютерними вірусами та відновлюють заражені файли.

– Хмарний антивірус (CloudAV) – одне з хмарних рішень інформаційної безпеки, що передбачає застосування зручного програмного забезпечення на захищеному комп’ютері, вивантажуючи велику частину аналізу інформації в інфраструктуру провайдера. CloudAV – це також рішення для ефективного сканування вірусів на пристрої з невисоким обчислювальним діапазоном. Серед найпоширеніших хмарних антивірусних програм можна виділити Panda Cloud Antivirus, CrowdStrike, Cb Defense та Immundet.

– DLP (Data Leak Prevention) – це захист від витоку інформації. Запобігання витоку даних (DLP) сформовано набором технологій, спрямованих на запобігання втраті конфіденційної інформації, яка міститься на підприємствах по всьому світу. Успішна реалізація цієї технології потребує значної підготовки та ретельного технічного обслуговування. Підприємства, які бажають інтегрувати та впроваджувати DLP, мають бути готовими до значних зусиль, які, якщо вони будуть виконані правильно, можуть значно знизити ризик викрадення інформації для організації.

– Криптографічні системи сприяють перетворенню інформації таким чином, що її розшифрування стає можливим лише за допомогою певних кодів або шифрів (DES – Data Encryption Standard, AES – Advanced Encryption Standard). Криптографія забезпечує захист інформації і включає покращені методи автентифікації, дайджести повідомлень, цифрові підписи та зашифровані мережеві комунікації. Старі, менш безпечні програми, наприклад Telnet і протокол передачі файлів (FTP), частково замінюються безпечнішими програмами (Secure Shell (SSH)), які використовують зашифровані мережеві комунікації. Бездротовий зв’язок може бути зашифрований за допомогою таких протоколів, як WPA/WPA2 або WEP. Дротові комунікації (ITU-T G.hn) захищені з використанням AES для шифрування та X.1035 для автентифікації та обміну ключами. Програмні програми, такі як GnuPG або PGP, можуть застосовуватись для шифрування інформаційних файлів та електронної пошти.

– Міжмережеві екрани (брандмауери або файрволи) – пристрої контролю доступу до мережі, призначені для блокування та фільтрації мережного трафіку. Брандмауери зазвичай класифікуються як мережеві чи хост-сервери. Мережеві брандмауери на базі мережі розташовані на шлюзових комп’ютерах LAN, WAN та інтрамережах. Це або програмні пристрої, що працюють на апаратних засобах загального призначення, або апаратні пристрої брандмауера. Брандмауери пропонують інші

функції для внутрішньої мережі, яку вони захищають, наприклад, є сервером DHCP або VPN для цієї мережі. Одним із найкращих рішень як для малих, так і для великих підприємств є міжмережні екрани CheckPoint.

– VPN (Virtual Private Network). Віртуальна приватна мережа (VPN) дає можливість визначити та використовувати для передачі та отримання інформації приватну мережу в рамках загальнодоступної мережі. Таким чином, програми, що працюють за VPN, є надійно захищеними. VPN дозволяє підключитися до внутрішньої мережі на відстані. За допомогою VPN можна створити спільну мережу для територіально віддалених підприємств. Окремі користувачі мережі також мають свої переваги використання VPN, тому що можуть захищати власні дані за допомогою VPN, а також уникати територіальних обмежень та використовувати проксі-сервери, щоб приховати своє місцезнаходження.

– Proxy-server (Проксі-сервер) – це конкретний комп'ютер або комп'ютерна програма, яка є зв'язуючою ланкою між двома пристроями (комп'ютер та інший сервер). Проксі-сервер можна встановити на одному комп'ютері разом із сервером брандмауера, або на іншому сервері. Плюси проксі-сервера в тому, що його кеш може служити всім користувачам. Інтернет-сайти, на які є найчастіший запит, найчастіше знаходяться в кеші проксі, що зручно для користувача. Фіксування своїх взаємодій проксі-сервером є корисною функцією для виправлення неполадок в роботі електронних ресурсів.

– Системи моніторингу та управління інформаційною безпекою, SIEM. Щоб виявляти та реагувати на загрози інформаційної безпеки, використовується рішення SIEM, яке виконує збір та аналіз подій з різних джерел, таких як міжмережні екрани, антивіруси, IPS, оперативні системи тощо. Завдяки системі SIEM у компанії з'являється можливість централізовано зберігати журнали подій та корелювати їх, визначаючи відхилення, потенційні загрози, збої у роботі IT-інфраструктури, кібератаки тощо.

Сучасні навчальні платформи дозволяють перекладачеві освоїти спеціальні курси з інформаційної безпеки. В мережі Інтернет вони представлені широким колом курсів, де можна переглядати навчальні відеоматеріали, аудіо супровід, текстові лекції, проходити тексти з отриманням сертифікату про підвищення кваліфікації чи освоєння курсу. Зокрема, корисні ресурси для перекладачів пропонує онлайн платформа Prometheus: «Інформаційна безпека», «Основи інформаційної безпеки» «Інформаційна гігієна під час війни», які покликані навчити користувача правильно диференціювати інформацію та застосовувати лише перевірені електронні ресурси.



Курси містять комплекс відео-виступів провідних спікерів в цій галузі, лекційні текстові та аудіо матеріали, текстовий супровід лекцій, набір практичних завдань, що сприяють ґрунтовному засвоєнню теоретичних матеріалів, а також поточні та прикінцеві тести, що допомагають визначити рівень засвоєння навчальних матеріалів та за їх результатами генерується сертифікат.

Серед тем, які були розглянуті в середовищі курсів з інформаційної безпеки, що можна застосовувати перекладачеві в ході професійної діяльності були: «Як захистити свій гаджет від вірусів і зовнішніх посягань?», «Стратегії захисту від інформаційних загроз», «Перевірка достовірності джерел інформації», «Як забезпечити безпечну комунікацію через е-мейл та соціальні мережі?», «Сучасні загрози інформаційної безпеки», «Загрози для мобільних пристроїв», «Принципи поведіння з фінансовою інформацією» тощо.

Комплекс курсів з інформаційної безпеки дозволить перекладачеві вільно орієнтуватися в широкому колі пропонованої в мережі Інтернет інформації та доцільно застосовувати професійне програмне забезпечення.

## **ВИСНОВКИ**

Сучасний етап інформатизації суспільства пов'язаний із застосуванням інформаційно-комунікаційних технологій, телекомунікаційних систем, створенням комп'ютерних мереж трансляції. Проте недотримання правил інформаційної безпеки може призвести до негативного впливу Інтернет-ресурсів на роботу спеціалістів з перекладу та ускладнень перекладацької діяльності, пов'язаних із втратою важливої інформації. Незважаючи на зростаючу потребу в розробці та впровадженні ефективних рішень в інформаційній індустрії, інформаційна безпека є однією з найважливіших складових взаємодії перекладачів з електронними ресурсами, які полегшують їх професійну діяльність.

До основних напрямків забезпечення захисту інформації, що необхідні під час роботи перекладачів та здобувачів вищої освіти перекладацьких спеціальностей в середовищі вищого навчального закладу відносяться:

- розробляють внутрішню документацію, яка встановлює правила роботи з комп'ютерною технікою та конфіденційною інформацією;

- проводять інструктаж та періодичні перевірки персоналу; ініціюють підписання додаткових угод до трудових договорів, де зазначено відповідальність за розголошення або неправомірне використання відомостей, які стали відомими по роботі;

– розмежують зони відповідальності, щоб унеможливити ситуації, коли масиви найважливіших даних перебувають у розпорядженні одного зі співробітників; організують роботу в загальних програмах документообігу та стежать, щоб критично важливі файли не зберігалися поза мережевими дисками;

– впроваджують програмні продукти, що захищають дані від копіювання чи знищення будь-яким користувачем, у тому числі топ-менеджментом організації;

– складають плани відновлення системи у разі виходу з ладу з будь-яких причин.

Лише системний та комплексний підхід до захисту інформації під час роботи перекладачів з іншомовними текстами в інформаційному електронному середовищі може забезпечити інформаційну безпеку. У системі інформаційної безпеки слід враховувати всі актуальні та ймовірні загрози та ризики. Майбутнім перекладачам необхідно детально ознайомитися з сучасними перекладацькими електронними ресурсами в інформаційному середовищі вищого навчального закладу та в подальшій професійній діяльності застосовувати лише перевірені програмні засоби, які сприятимуть захисту особистої та конфіденційної інформації.

Гострота проблеми інформаційної безпеки зростатиме з подальшим поширенням сучасних інформаційно-комунікаційних технологій, які є технологічною основою глобалізації, у всіх сферах життєдіяльності сучасного суспільства, розвитком електронних систем управління, освіти, бізнесу тощо.

## **АНОТАЦІЯ**

В публікації розглянуто особливості захисту інформації під час роботи перекладачів з електронним професійним програмним середовищем; виокремлено та диференційовано систему сучасних онлайн ресурсів перекладацького призначення, які забезпечують безпечну взаємодію з іншомовною інформацією в ході професійної діяльності. Автором висвітлено ризики, з якими стикається сучасний перекладач, виконуючи машинний чи автоматизований переклад; схарактеризовано шляхи їх усунення та запобігання в ході перекладацької діяльності. Незважаючи на істотні загрози, що породжує перекладацька діяльність в мережі Інтернет, в сучасному інформаційному просторі можливо створити систему безпеки, що ефективно захищає всю необхідну інформацію. Необхідно провести попередню перевірку безпеки даних, підключити сучасне програмне забезпечення, яке здійснює постійний моніторинг проблем з запозиченням інформаційних даних, застосовувати лише перевірені та ліцензійні онлайн ресурси, що дозволяють зберегти конфіденційну чи важливу інформацію.

## Література

1. Віблій В. М., Смотр О. О. Безпека інформації у хмарних сховищах : thesis. 2019. URL: <http://hdl.handle.net/123456789/6228> (дата звернення: 20.03.2023).
2. Долинський Є. В., Скиба К. М. Інформаційні технології у професійній діяльності перекладача : навчальний посібник. Хмельницький : ХНУ, 2016. 75 с.
3. Заплотинський Б. А. Основи інформаційної безпеки. Конспект лекцій. КПВіП НУ «ОЮА», кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.
4. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. *Ефективна економіка*. 2015. № 4. URL: <http://www.economy.nayka.com.ua/?op=1&z=5514>
5. Яфтумова А. А. Системи машинного перекладу як складова підготовки майбутніх перекладачів. *Діалог мов і культур у сучасному освітньому просторі* : І Всеукраїнська наукова інтернет конференція. Суми, 2017. С. 573–576.
6. Ferrara Gabriela Data Protection for Translators: A Practical Guide to Secure Translation. Routledge, 2019. 211 p.
7. Katan David Translation as Intercultural Communication: Towards a Theory of Translating. Routledge, 2018. 132 p.
8. Geisser Daniel The Impact of Technology on Translation Quality. *The Journal of Specialised Translation*, №. 29, 2018, pp. 107–126.
9. Novak B. Machine Translation URL: Advantages and Disadvantages : <http://dlsdc.com/blog/machinetranslation-advantages-and-disadvantages>.
10. The five best free translation programs URL: [https://its.at.ua/publ/programni\\_zasobi/p\\_jat\\_krashhikh\\_bezkoshtovnikh\\_program\\_dlja\\_per ekladu/2-1-0-27](https://its.at.ua/publ/programni_zasobi/p_jat_krashhikh_bezkoshtovnikh_program_dlja_per ekladu/2-1-0-27) (дата звернення: 04.03.2023).
11. Translator program: pros and cons. URL: <https://taskforce.ua/uk/programa-perekladachplyusy-i-minusy> (дата звернення: 16.03.2023).
12. Williams P., Sennrich R., Post M., Koehn P. Syntax-based Statistical Machine Translation. 2016. 208 с.

### Information about the author:

**Matviienko Lesia Hryhorivna,**

Candidate of Pedagogical Sciences,

Associate Professor

at the Department of Humanities and Social Disciplines

Poltava State Agrarian University

1/3, Skovorody Str., Poltava, 36003, Ukraine