extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ena.lpnu.ua:8443/server/api/core/bitstreams/45c0396f-cf07-47d5-be9c-1058b6dfe98a/content (дата звернення: 18.10.2025).

15. Eurostat. Assistive technologies for communication: EU benchmark report. Brussels, 2023. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Disability_statistics_-_access_to_information_and_communication_technologies (дата звернення: 18.10.2025).

Кочин Владислав Дмитрович,
курсант навчально-наукового інституту № 4 Харківського національного університету внутрішніх справ
Науковий керівник:
Онищенко Юрій Миколайович,
заступник директора з освітньої та науково-дослідної діяльності навчально-наукового інституту № 4 Харківського національного університету внутрішніх справ, кандидат наук з державного управління, доцент

ЩОДО ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ ІНШОМОВНОГО ПРОФЕСІЙНОГО СПІЛКУВАННЯ ПРАЦІВНИКАМИ КІБЕРПОЛІЦІЇ

Сьогодні кіберзлочинність не знає кордонів, що вимагає ефективної міжнародної співпраці між правоохоронними органами. Одним з ключових аспектів такої співпраці є володіння професійною термінологією іноземною мовою. Знання англійської мови є особливо важливим, оскільки більшість міжнародних стандартів і комунікацій здійснюються саме цією

мовою [1, 2]. Знання професійної термінології дозволяє працівникам кіберполіції більш точно формулювати завдання, складати звіти та документацію, а також уникати двозначностей під час спільних операцій із закордонними партнерами. Систематичне вивчення та практичне застосування термінів сприяє підвищенню професійної кваліфікації та швидкості реагування на кіберзагрози.

Іноземна термінологія в кіберполіції є основою для міжнародного співробітництва: спільних розслідувань, обміну інформацією, участі в міжнародних організаціях [1, 3]; для участі в міжнародних тренінгах і конференціях: обміну досвідом, ознайомлення з новітніми технологіями та методами боротьби з кіберзлочинністю [2]; для розробки та впровадження міжнародних стандартів, таких як спільна розробка протоколів, стандартів безпеки та методів розслідування [1, 4]. Крім того, правильне використання термінології іноземної мови допомагає уникнути помилок у процесі обробки інформації та підвищує ефективність міжвідомчої співпраці. Це також сприяє підвищенню довіри міжнародних партнерів до української кіберполіції, що є важливим для успішної реалізації спільних проектів.

У сфері кібербезпеки виділяють кілька основних категорій термінів, таких як: технічні терміни, пов'язані з технологіями, програмним забезпеченням, мережами [1]; юридичні терміни, пов'язані з правовими аспектами кіберзлочинності, законодавством, правами людини [2, 4]; оперативні терміни, пов'язані з методами та процедурами розслідування, реагуванням на інциденти [3]. Вивчення категорій термінів допомагає структурувати знання та ефективно застосовувати їх у конкретних ситуаціях. Знання технічних, юридичних та оперативних термінів є критично важливим для підготовки фахівців, які можуть швидко реагувати на нові загрози.

Незважаючи на надзвичайну важливість оволодіння іноземною термінологією, працівники кіберполіції стикаються з низкою проблем, що ускладнюють її практичне використання. Однією з проблем є відсутність точних перекладів, оскільки деякі спеціалізовані терміни не мають прямого відповідника в українській мові [3]. Швидкий розвиток технологій створює додаткову проблему: нові поняття з'являються швидше, ніж їх можна офіційно перекласти та закріпити в науковій і професійній літературі [2]. Крім того, одне й те саме явище в різних країнах може позначатися різними термінами, що часто призводить до непорозумінь у міжнародному спілкуванні [1, 4]. Ще одним важливим бар'єром є різниця в контекстуальному вживанні термінів, що іноді значно ускладнює переклад і тлумачення міжнародних документів. Все це вимагає постійного вдосконалення мовних навичок працівників кіберполіції та вимагає від них уважності до деталей і гнучкості у використанні професійної лексики іноземної мови.

Щоб ефективно використовувати термінологію іноземної мови, працівники кіберполіції повинні дотримуватися низки рекомендацій. Перш за все, важливо регулярно оновлювати свої знання, оскільки нові терміни та поняття в галузі кібербезпеки з'являються надзвичайно швидко, тому необхідно постійно стежити за їх перекладом та адаптацією [2]. Іншим важливим аспектом є використання офіційних джерел, зокрема міжнародних стандартів та авторитетних глосаріїв, які забезпечують єдність і точність у використанні професійної лексики [1, 4]. Співпраця з перекладачами та фахівцями відіграє важливу роль у запобіганні неточностям та забезпеченні правильного тлумачення складних термінів [3]. Крім того, участь у міжнародних форумах та конференціях створює можливості для обміну досвідом та узгодження термінології з іноземними колегами [2]. Особливу увагу слід приділяти створенню внутрішніх глосаріїв та довідників для працівників кіберполіції,

які систематизують необхідні терміни та полегшують підготовку нових кадрів. Постійне використання таких матеріалів у професійній діяльності сприяє підвищенню ефективності роботи та якості міжвідомчої та міжнародної комунікації.

Таким чином, володіння професійною термінологією іноземною мовою є важливою складовою ефективної кіберполіції. Це забезпечує високий рівень міжнародної співпраці, ефективне реагування на кіберзагрози та розслідування кіберзлочинів. Незважаючи на існуючі виклики, систематичне вдосконалення знань та співпраця з міжнародними партнерами допоможуть подолати ці труднощі. Акцент на професійній мовній підготовці та правильному використанні термінології сприяє підвищенню престижу української кіберполіції на міжнародній арені. Це також створює умови для швидкого та ефективного реагування на глобальні кіберзагрози.

Список використаних джерел

1. Національний інститут стандартів і технологій (NIST). Глосарій термінів з кібербезпеки. URL: https://niccs.cisa.gov/resources/glossary

2. Спеціальна служба зв'язку та захисту інформації України (Держспецзв'язок). Основні принципи кібербезпеки в Україні. URL: https://www.dsszzi.gov.ua

3. Комп'ютерна група реагування на надзвичайні ситуації України (CERT-UA). Діяльність CERT-UA та методи реагування. URL: https://cert.gov.ua

4. Міністерство юстиції США. Глосарій термінів з кібербезпеки.
URL: https://www.fortinet.com/resources/cyberglossary/definitions-of-jargon