ТЕМА 3
СИТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. МІЖНАРОДНИЙ ОБМІН ІНФОРМАЦІЄЮ. АНГЛОМОВНА ПІДГОТОВКА КАДРІВ ПРАВООХОРОННИХ ОРГАНІВ ЯК ОСНОВА ЕФЕКТИВНОЇ КОМУНІКАЦІЇ.

План

1. Повноваження правоохоронних органів у сфері забезпечення інформаційної безпеки.
2. Суб'єкти забезпечення інформаційної безпеки в Україні.
3. Кібербезпека як складова інформаційної безпеки держави.
4. Англомовна підготовка кадрів правоохоронних органів у контексті Закону України «Про застосування англійської мови в Україні» як основа ефективного міжнародного обміну інформацією, взаємодії з Інтерполом, Європолом та іншими міжнародними структурами.

Мета: систематизувати знання про правове регулювання доступу до інформації та захисту інформації з обмеженим доступом, основи кібербезпеки в діяльності органів державної влади та місцевого самоврядування, принципи відкритості та прозорості публічної інформації, види інформації та механізми їх правового захисту, а також сформувати практичні навички аналізу законності обмеження доступу до інформації та оцінки ризиків у цифровому середовищі.

Перелік ключових термінів і понять з теми: інформаційна безпека, правоохоронний орган, кібербезпека, інформація, інформаційні технології, персональні дані, суб'єкти забезпечення інформаційної безпеки, повноваження, взаємодія, відповідальність, Національний координаційний центр кібербезпеки, кібербезпека, національна безпека, кібератаки, критична інфраструктура, міжнародне співробітництво, державна політика, цифрові технології, кіберзагрози, кіберзахист, інформаційні системи.

1. Повноваження правоохоронних органів у сфері забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки є одним із ключових напрямів реалізації функцій сучасної держави та невід'ємною складовою системи національної безпеки. Особлива роль у цій сфері належить правоохоронним органам, які покликані захищати суспільство, державу та особу від протиправних

посягань, у тому числі в інформаційному та кіберпросторі. У науковій доктрині інформаційна безпека розглядається як стан захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері. Так, С. Усик визначає інформаційну безпеку суспільства й держави як ступінь їх захищеності та стійкості основних сфер життєдіяльності (економіки, науки, управління, військової сфери, суспільної свідомості тощо) від деструктивних інформаційних впливів, що загрожують національним інтересам [1, с. 271].

Захист інформації у правовому розумінні охоплює комплекс організаційних, правових, технічних і режимних заходів, спрямованих на:

- забезпечення цілісності, конфіденційності та доступності інформації;
- запобігання несанкціонованому доступу до інформації та її носіїв;
- обмеження незаконного поширення інформації з обмеженим доступом.

Як слушно зазначають С. Лихова та В. Сисоєва, саме правоохоронні органи як складова сектору безпеки і оборони відіграють провідну роль у протидії посяганням на інформаційну безпеку держави [2, с. 103].

Основоположні засади забезпечення інформаційної безпеки закріплено в Конституції України. Зокрема: ч. 1 ст. 17 Конституції України визначає захист інформаційної безпеки як одну з найважливіших функцій держави; ч. 2 ст. 34 Конституції України гарантує право кожного на вільне збирання, зберігання, використання та поширення інформації, водночас допускаючи законні обмеження з метою захисту національної безпеки.

Правовий компонент інформаційної безпеки, за визначенням Ю. Кунєва, полягає в наявності системи правових норм, які регламентують інформаційні відносини та забезпечують охоронну й регулятивну функції держави у сфері інформаційної діяльності [3, с. 98]. У науковій літературі повноваження правоохоронних органів у сфері забезпечення інформаційної безпеки доцільно класифікувати за функціональним критерієм. Таку систематизацію пропонує В. Макарчук [4, с. 325 - 326], зокрема:

Інформаційно-аналітичні. Збір, обробка, аналіз та використання інформації для виконання покладених законом завдань, тобто повноваження щодо створення та використання інформаційних систем. Так, наприклад, відповідно до ст. 24 Закону України «Про Службу безпеки України»**,** СБУ здійснює інформаційно-аналітичну діяльність в інтересах національної безпеки [6]. Національна поліція України відповідно до ст. 23 Закону України «Про Національну поліцію» має право отримувати від органів державної влади, підприємств, установ, організацій та громадян інформацію, необхідну для виконання її повноважень, а також користуватися державними інформаційними

базами даних [5]. Державна прикордонна служба України відповідно до законодавства створює та використовує інформаційні системи і банки даних щодо: осіб, які перетнули державний кордон; осіб, яким обмежено право в'їзду або виїзду; викрадених або втрачених документів [7].

Профілактично-запобіжні. Правоохоронні органи здійснюють комплекс заходів, спрямованих на попередження правопорушень у сфері інформаційної та кібербезпеки. Зокрема, СБУ відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» здійснює негласну перевірку готовності об'єктів критичної інфраструктури до кібератак [8].

Протидійно-реагувальні. Служба безпеки України протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [8]. Окрім того на неї покладено обов'язок протидіяти проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації [9].

Оперативно-технічні. СБУ здійснює технічне регулювання у сфері спеціальних технічних засобів зняття інформації з каналів зв'язку [6], а Державна прикордонна служба має повноваження щодо протидії використанню безпілотних авіаційних систем [7].

Моніторингові - спрямовані на виявлення, фіксацію та обмеження доступу до інформації, поширення якої заборонено законом, а також на застосування санкцій та обмежень у сфері інформаційної та кібербезпеки [8]. *Моніторингові*, які проводяться з метою виявлення, фіксації, обмеження доступу та/або видалення з українського сегмента мережі Інтернет інформації, розміщення якої обмежено або заборонено законом. СБУ у межах компетенції здійснює: моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та Інтернету з метою виявлення загроз національній безпеці України в інформаційній сфері; протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації. Правоохоронні органи забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління.

Правообмежуючі - правоохоронні органи мають повноваження щодо

обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави, визнані Верховною Радою України державою- агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері.

2. Суб'єкти забезпечення інформаційної безпеки в Україні.

В умовах цифровізації суспільних відносин та триваючої гібридної агресії проти України забезпечення інформаційної безпеки набуває системного, комплексного характеру та здійснюється сукупністю державних органів, об'єднаних у єдину національну систему. Правову основу функціонування цієї системи становлять Закон України «Про національну безпеку України», Закон України «Про основні засади забезпечення кібербезпеки України», а також Стратегія кібербезпеки України. Зазначені нормативно-правові акти визначають засади державної політики у сфері інформаційної та кібербезпеки, коло суб'єктів її забезпечення, їхні повноваження, а також механізми координації та взаємодії.

Національна система кібербезпеки України включає основних суб'єктів, кожен з яких виконує специфічні функції відповідно до своєї компетенції. Діяльність суб'єктів забезпечення інформаційної безпеки регулюється профільним законодавством, яке чітко окреслює межі їхніх повноважень, напрями відповідальності та форми взаємодії між собою.

1. ***Рада національної безпеки і оборони України (РНБО)*** є конституційним координаційним органом з питань національної безпеки і оборони при Президентові України. Ключова роль РНБО у сфері інформаційної безпеки реалізується через діяльність *Національного координаційного центру кібербезпеки (НКЦК),* який є її робочим органом. До основних повноважень НКЦК належать: координація та контроль діяльності всіх суб'єктів сектору безпеки і оборони у сфері кібербезпеки; аналіз стану кіберзахисту державних електронних інформаційних ресурсів та об'єктів критичної інфраструктури; прогнозування кіберзагроз; розроблення пропозицій щодо стратегічного розвитку національної системи кібербезпеки. Діяльність Центру спрямована на синхронізацію зусиль різних органів державної влади на стратегічному рівні та формування єдиної державної політики у сфері протидії кіберзагрозам.

2. ***Державна служба спеціального зв'язку та захисту інформації України*** є центральним органом виконавчої влади спеціального призначення, який забезпечує функціонування та розвиток державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, а також формування та реалізацію державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку та активної протидії агресії у кіберпросторі. До ключових повноважень цього органу належать:

а) формування та реалізація державної політики у сферах кіберзахисту, криптографічного і технічного захисту інформації;

б) забезпечення функціонування Державного центру кіберзахисту та урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;

в) проведення державних експертиз та аудитів інформаційної безпеки, зокрема на об'єктах критичної інфраструктури.

3. ***Служба безпеки України (СБУ)*** є головним органом у системі контррозвідувальної діяльності та протидії загрозам державній безпеці в інформаційній сфері. Повноваження СБУ у сфері забезпечення інформаційної безпеки України включають: виявлення, попередження та припинення розвідувально-підривної діяльності іноземних спеціальних служб в інформаційному просторі; боротьбу з такими протиправними діяннями, як кібертероризм та кібершпигунство; розслідування кримінальних правопорушень проти основ національної безпеки, вчинених із використанням комп'ютерних систем, інформаційно-комунікаційних мереж і технологій. Служба безпеки України зосереджує свою діяльність на виявленні та нейтралізації найбільш небезпечних загроз, що походять від іноземних спецслужб, терористичних організацій, кіберзлочинних угрупувань та інших суб'єктів, діяльність яких спрямована на підрив суверенітету, конституційного ладу, обороноздатності та інформаційної безпеки держави.

4. Одним із найбільш чисельних правоохоронних органів у системі забезпечення інформаційної безпеки є ***Національна поліція України***, у структурі якої функціонує спеціалізований підрозділ - *Департамент кіберполіції*. Він відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, а також організовує та здійснює оперативно-розшукову діяльність. До основних завдань Департаменту кіберполіції належать: участь у формуванні та реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких пов'язаний з використанням

електронно-обчислювальних машин, комп'ютерних систем, мереж і телекомунікаційних технологій; надання допомоги іншим підрозділам Національної поліції у виявленні, припиненні та розслідуванні кіберзлочинів.

Департамент кіберполіції Національної поліції України є правоохоронним органом, що спеціалізується на протидії загально кримінальній кіберзлочинності. До першочергових завдань кіберполіції належать:

а) протидія шахрайству з використанням електронно-обчислювальної техніки та несанкціонованому втручанню в роботу комп'ютерних мереж;

б) боротьба з розповсюдженням шкідливого програмного забезпечення, дитячої порнографії в мережі Інтернет та іншими видами кіберзлочинності.

При цьому слід зазначити, що кіберполіція переважно працює з кримінальними правопорушеннями загальнокримінального та інформаційного характеру, а не з політичними чи військовими загрозами.

До інших не менш важливих суб'єктів забезпечення інформаційної безпеки України належать: Міністерство оборони України та Збройні Сили України, які відповідають за кібероборону держави у військовій сфері; розвідувальні органи, що здійснюють кіберрозвідку; Національний банк України, який забезпечує кібербезпеку банківської та фінансової системи. Зважаючи на транснаціональний характер кіберзлочинності, Департамент кіберполіції Національної поліції України активно співпрацює з правоохоронними органами іноземних держав (США, Велика Британія, Франція, Німеччина, Польща, Італія тощо), а також з міжнародними правоохоронними організаціями, зокрема Європолом, Інтерполом, NCFTA та іншими, що є важливою складовою міжнародного обміну інформацією та протидії глобальним кіберзагрозам.

3. Кібербезпека як складова інформаційної безпеки держави.

Кібербезпека в сучасних умовах розвитку інформаційного суспільства та глобальної цифровізації є однією з ключових складових інформаційної безпеки держави та невід'ємним елементом системи національної безпеки. Інтенсивне впровадження інформаційно-комунікаційних технологій у сферу державного управління, економіки, фінансових відносин, оборони, енергетики, транспорту, охорони здоров'я та соціальних сервісів зумовлює істотне зростання залежності держави від стабільного та безпечного функціонування кіберпростору. За таких умов порушення роботи інформаційних систем або незаконне втручання в них може мати наслідки, співмірні з традиційними загрозами національній безпеці.

Кіберпростір сьогодні розглядається не лише як технологічне середовище обміну інформацією, а як окрема сфера суспільних відносин, у межах якої реалізуються політичні, економічні, військові та соціальні інтереси держав і

недержавних суб’єктів. Саме тому кіберзагрози мають комплексний характер і включають кібератаки на державні інформаційні ресурси, об’єкти критичної інформаційної інфраструктури, фінансові та банківські системи, системи управління технологічними процесами, а також персональні дані громадян. До найбільш небезпечних форм кіберзагроз належать кібершпигунство, кібертероризм, організована кіберзлочинність, дезінформаційні кампанії та використання кіберінструментів у гібридних війнах.

У теоретико-правовому вимірі кібербезпека розглядається як складова інформаційної безпеки, що охоплює систему правових, організаційних, технічних, управлінських і міжнародних заходів, спрямованих на захист інформації, інформаційно-комунікаційних систем та цифрових ресурсів від несанкціонованого доступу, втручання, модифікації, блокування або знищення. На відміну від традиційних підходів, сучасна доктрина підкреслює, що кібербезпека не може обмежуватися виключно технічними засобами захисту, а повинна інтегруватися у загальну систему державної безпекової політики та правового регулювання.

Проблематика кібербезпеки та її нормативно-правового забезпечення отримала широке висвітлення у вітчизняних і зарубіжних наукових дослідженнях. Теоретико-методологічну основу вивчення даного питання становлять фундаментальні положення інформаційного права, права національної безпеки, адміністративного та міжнародного права. Нормативну основу формують ключові законодавчі акти України, зокрема Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про захист інформації в інформаційно-комунікаційних системах», Закон України «Про захист персональних даних», Стратегія кібербезпеки України, а також плани заходів з її реалізації.

Вагомий внесок у формування теоретико-правових засад забезпечення кібербезпеки зроблено у працях вітчизняних науковців, зокрема Б. Кормича, А. Марущака, А. Семенченка, В. Плескача та інших. У цих дослідженнях розкриваються питання правової природи кібербезпеки, механізмів правового регулювання кіберпростору, взаємодії суб’єктів забезпечення інформаційної та кібербезпеки, а також проблеми адаптації національного законодавства до міжнародних стандартів. У сфері державного управління кібербезпекою значну увагу приділено роботам О. Потія, Д. Мялковського та С. Кравченка, які акцентують на необхідності інституційного розвитку, удосконалення системи координації та управління кіберризиками.

Особливе місце у науковій розробці проблематики кібербезпеки посідають дослідження А. Зарубенка та О. Дєгтяря (2025 р.), у яких здійснено комплексний

аналіз міжнародних і українських державних механізмів правового регулювання кібербезпеки. Науковці виходять з того, що кібербезпека має розглядатися як складова національної безпеки, яка потребує системного підходу, поєднання нормативно-правового регулювання, інституційної спроможності органів державної влади, належного фінансування та активної міжнародної співпраці. Обґрунтовують доцільність гармонізації національного законодавства з правом Європейського Союзу та міжнародними стандартами у сфері кіберзахисту [13, с. 691-704].

Національна система кібербезпеки України є багаторівневою та комплексною. Вона включає суб'єктів забезпечення кібербезпеки, сукупність правових норм, організаційних структур, технічних і криптографічних засобів, а також управлінські механізми реагування на кіберзагрози. До основних суб'єктів національної системи кібербезпеки належать Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Міністерство оборони України, Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України та інші уповноважені органи.

Координацію діяльності у сфері кібербезпеки здійснює Державний центр кіберзахисту, який забезпечує функціонування національної команди реагування на комп'ютерні інциденти CERT-UA, проводить аудит кіберзахисту об'єктів критичної інформаційної інфраструктури та бере участь у формуванні політики реагування на кіберінциденти. Подальший розвиток інституційної складової кібербезпеки пов'язаний зі створенням у 2025 році Кіберцентру UA30, який функціонує як сучасна платформа моніторингу, аналізу кіберзагроз, підготовки кадрів та координації взаємодії держави з приватним сектором і громадянським суспільством.

Нормативно-правове забезпечення кібербезпеки України має багаторівневий характер. Центральне місце в цій системі займає Закон України «Про основні засади забезпечення кібербезпеки України», який визначає принципи державної політики у сфері кібербезпеки, суб'єктів національної системи кібербезпеки, механізми координації їх діяльності та напрями захисту критичної інформаційної інфраструктури. Закон встановлює обов'язки державних органів щодо впровадження заходів кіберзахисту, управління ризиками та відновлення функціонування інформаційних систем після інцидентів.

Стратегічні орієнтири державної політики у сфері кібербезпеки визначені Стратегією кібербезпеки України, затвердженою Указом Президента України № 447/2021. У Стратегії кібербезпека визначається одним із пріоритетів

національної безпеки, а основними завданнями є формування системи кібероборони, протидія кіберзлочинності, підвищення кіберстійкості держави, розвиток кадрового та науково-технічного потенціалу, а також розширення міжнародного співробітництва. Практичну реалізацію Стратегії забезпечує План заходів на 2025 рік, який конкретизує завдання, строки їх виконання та відповідальних виконавців.

Важливим напрямом розвитку національної системи кібербезпеки є адаптація законодавства України до директив Європейського Союзу NIS та NIS2, які встановлюють підвищені вимоги до захисту критичної інфраструктури, управління кіберризиками та відповідальності операторів ключових послуг. Імплементація цих директив сприяє інтеграції України до європейського безпекового простору та підвищенню рівня довіри до національної системи кіберзахисту.Окрему роль у забезпеченні кібербезпеки відіграє міжнародне співробітництво. Україна активно взаємодіє з Європейським Союзом, НАТО, ENISA, ООН, ОБСЄ та Інтерполом, бере участь у спільних навчаннях, програмах технічної допомоги та обміну інформацією. Такі заходи сприяють підвищенню професійного рівня фахівців, запровадженню сучасних технологій кіберзахисту та формуванню ефективних механізмів реагування на транснаціональні кіберзагрози.

Отже, кібербезпека як складова інформаційної безпеки держави є складним, багатовимірним явищем, що потребує системного правового регулювання, ефективної інституційної моделі та постійного вдосконалення з урахуванням динаміки кіберзагроз. Забезпечення належного рівня кібербезпеки є необхідною умовою захисту національних інтересів, прав і свобод людини, стабільного функціонування державних інститутів та сталого розвитку інформаційного суспільства.

4. Англомовна підготовка кадрів правоохоронних органів у контексті Закону України «Про застосування англійської мови в Україні» як основа ефективного міжнародного обміну інформацією, взаємодії з Інтерполом, Європолом та іншими міжнародними структурами.

У сучасних умовах глобалізації, інтеграції України до європейського правового простору та активної міжнародної співпраці у сфері безпеки і правопорядку зростає потреба у фахівцях, спроможних до вербальної міжнародної комунікації. Англійською мовою як другою загалом володіють 743 555 740 осіб, і їх кількість постійно зростає. У Науково-практичному коментарі Закону України «Про застосування англійської мови в Україні» (2025 р.) за заг.

ред. М. Ларкіна наголошується, що сьогодні англійська мова є офіційною де-юре у 58 зі 196 країн світу [14, с. 13]. Вона є однією з шести мов Організації Об'єднаних Націй, а також офіційною мовою Європейського Союзу, Ради Європи, Європейської комісії, Європейської асоціації вільної торгівлі та НАТО.

Наголошуючи на «особливому статусі» англійської мови як світової мови та мови сучасної науки, ділової комунікації, Конституційний Суд у справі за конституційним поданням 51 народного депутата України щодо відповідності Конституції України (конституційності) Закону України «Про забезпечення функціонування української мови як державної» від 14.07.2021 р. № 1-р/2021 у п. 6.3 мотивувальної частини зазначає, що «у нинішньому світі англійська мова відіграє роль глобального посередника в спілкуванні між народами. Такою самою є її роль у спілкуванні між представниками наукових і професійних спільнот» [15].

Англомовна підготовка кадрів у сфері безпеки набуває особливої актуальності в контексті п. 5 ст. 3 Закону України від 04.06.2024 р. «Про застосування англійської мови в Україні» [16], адже активізація професійної мобільності та міжнародної співпраці (зокрема, посилення ефективності взаємодії з міжнародними організаціями такими як Європол, Інтерпол, ОБСЄ, Місія ЄС з реформування сектору цивільної безпеки в Україні тощо), оперативний обмін інформацією, належний рівень обслуговування іноземних громадян, участь у спільних операціях, тренінгах, обмін досвідом на міжнародних конференціях, симпозіумах, нарадах та проходження професійного навчання за участю іноземних інструкторів, потребує системної модернізації традиційних підходів як до організаційних моделей, так і до фінансово-правового забезпечення такої підготовки, що дозволить підвищити ефективність виконання службових обов'язків та належно представляти інтереси України на міжнародному рівні.

Відповідно до п. 5 ч. 1 ст. 3 ЗУ та «Про застосування англійської мови в Україні» вимога щодо обов'язковості володіння англійською мовою встановлюється до осіб, які претендують на заняття посад поліцейських середнього і вищого складу Національної поліції України, посад начальницького складу інших правоохоронних органів, посад начальницького складу служби цивільного захисту, перелік яких встановлюється Кабінетом Міністрів України (*набирає чинності через чотири роки з дня припинення або скасування воєнного стану в Україні, введеного Указом Президента України «Про введення воєнного стану в Україні» від 24 лютого 2022 року № 64/2022, затвердженим Законом України «Про затвердження Указу Президента України «Про введення воєнного стану в Україні» від 24 лютого 2022 року № 2102-IX*) [16].

Постановою КМУ від 24.12.2024 р. № 1488 затверджено перелік посад поліцейських середнього і вищого складу Національної поліції, посад начальницького складу інших правоохоронних органів, посад начальницького складу служби цивільного захисту, кандидати на зайняття яких зобов'язані володіти англійською мовою (*п. 2 зазначеної Постанови встановлено, що ця постанова набирає чинності через чотири роки з дня припинення або скасування воєнного стану в Україні*) [17]. Слід підкреслити, що зазначеною Постановою затверджено перелік відповідних посад без конкретизації рівня мовленнєвої компетенції володіння англійською мовою, що слід визнати суттєвим недоліком, який потребує усунення (більш виправданим вбачається підхід у Постанові КМУ від 27.12.2024 р. № 1522 при визначенні переліків посад військовослужбовців офіцерського складу, сержантського і старшинського складу, кандидати на зайняття яких з числа військовослужбовців за контрактом зобов'язані володіти англійською мовою, також прийнятою на виконання ЗУ «Про застосування англійської мови в Україні», в якій не лише затверджено перелік відповідних посад, але й передбачено рівень мовленнєвої компетенції) ї. Такий підхід є більш виправданим, з огляду на те, що створює підґрунтя для розробки концепції та практичної реалізації оптимального варіанта організаційно-правового забезпечення англомовної підготовки правоохоронців. Доцільно також звернути увагу на впровадження стимулюючих інструментів - Постанова КМУ від 7 березня 2025 р. № 257 «Про затвердження Порядку встановлення надбавки за володіння англійською мовою деяким категоріям осіб» [19].

Отже, англомовна підготовка правоохоронців професійно орієнтована та спрямована на формування практичних навичок використання мови у службовій діяльності. Йдеться не лише про загальне володіння англійською мовою, а про здатність працювати зі спеціалізованою правовою, кримінологічною та оперативною термінологією, складати службові документи, аналізувати інформаційні повідомлення, звіти та аналітичні матеріали, а також ефективно комунікувати в міжкультурному середовищі. У системі міжнародного обміну інформацією англійська мова відіграє ключову роль у забезпеченні оперативності та точності передавання даних. Недостатній рівень мовної підготовки може призводити до затримок у реагуванні на запити, помилок у тлумаченні інформації, обмеження доступу до міжнародних інформаційних ресурсів і, як наслідок, зниження ефективності правоохоронної діяльності. Важливе значення англомовна підготовка має у сфері інформаційно-аналітичної діяльності правоохоронних органів. Здатність аналізувати англомовні джерела інформації, у тому числі звіти міжнародних організацій, матеріали іноземних

правоохоронних органів, судову практику та рекомендації експертних структур, сприяє підвищенню якості управлінських і процесуальних рішень.

Прийняття Закону України «Про застосування англійської мови в Україні» стало імпульсом для оновлення підходів до мовної підготовки кадрів правоохоронних органів у контексті їх професійної діяльності та міжнародної взаємодії [20, с. 366]. Системна модернізація нормативно-правових, організаційних та фінансових механізмів зазначеного процесу, а саме: конкретизація вимог до рівнів англомовної компетентності, інтегрування англомовної підготовки до системи професійної освіти та підвищення кваліфікації, впровадження сучасних освітніх моделей**,** зокрема на основі концепцій ESP (англійської для спеціальних цілей) з урахуванням специфіки службових обов'язків та реальних потреб правоохоронців у міжнародному комунікативному просторі, впровадження стимулюючих механізмів (надбавок за підтверджений рівень володіння), міжвідомча координація та створення єдиної інформаційно-освітньої платформи для системної підготовки та тестування дозволить забезпечити ефективну англомовну підготовку кадрів у сфері безпеки і правопорядку.

Використана література:

1. Усик С. Дослідження правового механізму забезпечення інформаційної безпеки в умовах надзвичайних ситуацій. *Науковий вісник: «Державне управління»*. 2020. № 4 (6). С. 266 - 280.
2. Лихова С. Я., Сисоєва В. П. Діяльність правоохоронних органів України у сфері забезпечення інформаційної безпеки. *Наукові праці Київського авіаційного інституту. Серія: Юридичний вісник «Повітряне і космічне право»*. 2022. № 1(64). С. 102-107.
3. Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право».* 2021. № 1(58). С. 95-102.
4. Макарчук В.В. Повноваження правоохоронних органів при реалізації державної політики щодо забезпечення інформаційної безпеки. *Юридичний науковий електронний журнал*. 2022. № 8. С. 324 - 326.
5. Про затвердження Положення про Національну поліцію : Постанова Кабінету Міністрів України від 28.10.2015 № 877. URL: https://zakon.rada.gov.ua/laws/show/877-2015-п#Text (дата звернення: 26.12.2025).
6. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 26.12.2025).

7. Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV. URL: https://zakon.rada.gov.ua/laws/show/661-15#Text (дата звернення: 26.12.2025).

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 26.12.2025).

9. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 26.12.2025).

10. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 26.12.2025).

11. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. URL:https://zakon.rada.gov.ua/laws/show/3475-15#Text6 (дата звернення: 29.12.2025).

12. Насонов М.І. Суб'єкти забезпечення інформаційної безпеки в Україні: повноваження, взаємодія, відповідальність. *Наука і техніка сьогодні*. *Серія Право*. 2025. № 8 (49). С. 149-157.

13. Зарубенко А.О., Дєгтяр О..А. Міжнародні та українські державні механізми правового регулювання кібербезпеки. *Успіхи і досягнення у науці.* 2025. № 11 (21). С. 691-704.

14. Закон України «Про застосування англійської мови в Україні»: науково-практичний коментар / В. І. Бояров та ін.; за заг. ред. М. О. Ларкіна. Київ : Юрінком Інтер, 2025. 164 с.

15. Рішення Конституційного Суду України від 14.07.2021 № 1-р/2021 у справі за конституційним поданням 51 народного депутата України щодо відповідності Конституції України (конституційності) Закону України «Про забезпечення функціонування української мови як державної». URL: https://zakon.rada.gov.ua/laws/show/v001p710-21#Text (дата звернення: 30.12.2025).

16. Про застосування англійської мови в Україні : Закон України від 04.06.2024 № 3760-IX. URL : https://zakon.rada.gov.ua/laws/show/3760-20#Text (дата звернення: 30.12.2025).

17. Про затвердження переліку посад поліцейських середнього і вищого складу Національної поліції, посад начальницького складу інших правоохоронних органів, посад начальницького складу служби цивільного

захисту, кандидати на зайняття яких зобов’язані володіти англійською мовою: Постанова Кабінету Міністрів України від 24.12.2024 № 1488. URL: https://zakon.rada.gov.ua/laws/show/1488-2024-%D0%BF#Text (дата звернення: 30.12.2025).

18. Про переліки посад військовослужбовців офіцерського складу, сержантського і старшинського складу, кандидати на зайняття яких з числа військовослужбовців за контрактом зобов’язані володіти англійською мовою : Постанова Кабінету Міністрів України від 27.12.2024 № 1522. URL: https://www.kmu.gov.ua/npas/pro-pereliky-posad-viiskovosluzhbovtsiv-ofitserskoho-skladu-serzhantskoho-i-starshynskoho-skladu-t271224 (дата звернення: 26.07.2025).

19. Порядок встановлення надбавки за володіння англійською мовою деяким категоріям осіб : Постанова Кабінету Міністрів України від 07.03.2025 № 257. URL: https://zakon.rada.gov.ua/laws/show/257-2025-%D0%BF#Text (дата звернення 09.06.2025).

20. Пирожкова Ю.В., Ларкін М.О. Англомовна підготовка кадрів правоохоронних органів у контексті Закону України «Про застосування англійської мови в Україні»: організаційні моделі та фінансово-правове забезпечення. *Науковий вісник Ужгородського національного університету*. *Серія: Право.* 2025. Випуск 90. Ч. 3. С. 360 - 366.