ТЕМАТИЧНИЙ НАПРЯМ РОБОТИ 4.
«МІЖНАРОДНИЙ ДОСВІД ТА ШЛЯХИ ЙОГО ІМПЛЕМЕНТАЦІЇ У ДІЯЛЬНІСТЬ ВІЙСЬКОВИХ ФОРМУВАНЬ ТА ПРАВООХОРОННИХ ОРГАНІВ ПРИ ВИКОНАННІ ЗАВДАНЬ ІЗ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ»

Анашкіна-Вітченко А. А.,
здобувач другого (магістерського) рівня вищої освіти
Національна академія Служби безпеки України
(м. Київ, Україна)

АДАПТАЦІЯ СТАНДАРТІВ НАТО ТА ЄС У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

В сучасних умовах охорона державної таємниці є ключовим елементом забезпечення національної безпеки, особливо в умовах воєнних загроз та розширення міжнародного співробітництва України. Євроінтеграційний курс нашої держави зумовлює необхідність гармонізації національної системи захисту секретної інформації з вимогами НАТО та Європейського Союзу. Це дає можливість не лише зміцнити власний безпековий потенціал, але й стати надійним партнером у сфері обміну розвідувальними та службовими даними.

Адаптація стандартів НАТО та ЄС у сфері охорони державної таємниці передбачає приведення українського законодавства, інституційних механізмів і технічних рішень у відповідність до міжнародних норм. Такий процес забезпечує сумісність систем секретності, полегшує координацію у спільних операціях і підвищує рівень довіри між державами-партнерами. Одночасно він сприяє посиленню кіберзахисту, мінімізації ризиків витоку інформації та формуванню єдиного безпекового простору [1].

У процесі гармонізації української системи охорони державної таємниці важливе значення має порівняння базових стандартів НАТО та Європейського Союзу. Адже саме ці міжнародні організації встановили чіткі правила класифікації та захисту секретної інформації, які використовуються в сучасній практиці безпеки. Порівняльний аналіз дозволяє визначити спільні риси та відмінності у підходах до забезпечення інформаційної безпеки, окреслити напрями їхнього впровадження в Україні та зрозуміти, які елементи потребують найбільшої адаптації (табл. 1).

Таблиця 1

Порівняльна таблиця стандартів НАТО та ЄС у сфері охорони секретної інформації [2]

Критерії	Досвід НАТО	Досвід ЄС

Базовий документ	NATO Security Policy (C-M(2002)49), NATO Security Directives	Council Decision 2013/488/EU (Security Regulations)
Класифікаційні рівні секретності	1. COSMIC TOP SECRET (CTS) 2. NATO SECRET (NS) 3. NATO CONFIDENTIAL (NC) 4. NATO RESTRICTED (NR)	1. EU TOP SECRET (TRES SECRET UE/EU TOP SECRET). 2. EU SECRET (SECRET UE/EU SECRET). 3. EU CONFIDENTIAL (CONFIDENTIEL UE/EU CONFIDENTIA) 4. EU RESTRICTED (RESTREINT UE/EU RESTRICTED)
Основні принципи	Захист інформації незалежно від носія, обов'язковий контроль доступу та принцип «need-to-know».	Єдність стандартів для всіх інституцій ЄС, мінімізація ризику витоку та принцип «need-to-know».
Інституційна структура	NATO Office of Security (NOS), підрозділи безпеки в штабах і агенціях НАТО.	Генеральний секретаріат Ради ЄС (Security Office), підрозділи безпеки в інституціях ЄС.
Захист інформації в ІТ-системах	Політика INFOSEC, криптографічні стандарти НАТО, обов'язкова сертифікація обладнання.	EU INFOSEC Policy, використання затверджених криптосистем, обов'язкове тестування і сертифікація.
Обмін інформацією з партнерами	Лише з країнами, що мають угоди з НАТО про взаємний захист секретів.	Лише з державами або організаціями, з якими укладено угоди про захист EUCI.

Одним із ключових викликів в процесі адаптації стандартів НАТО та ЄС у сфері охорони секретної інформації виступає наявність застарілої нормативно-правової бази, сформованої ще в умовах радянської системи. Чинне законодавство не повною мірою враховує новітні загрози, зокрема пов'язані з кіберпростором, і не завжди відповідає сучасним міжнародним практикам у сфері безпеки інформації. Це створює прогалини у взаємодії з партнерами та обмежує можливість обміну секретними матеріалами на рівні, необхідному для спільних операцій.

Другим важливим викликом є обмеженість фінансових і матеріально-технічних ресурсів, які потрібні для модернізації системи охорони секретної інформації. Встановлення сучасних систем криптографічного захисту, фізичного

контролю доступу, обладнання спеціальних приміщень для зберігання секретних документів вимагає значних витрат, які не завжди можуть бути забезпечені у повному обсязі. Це особливо актуально в умовах воєнних дій, коли фінансування держави спрямовується насамперед на оборонні потреби.

Додатковим ризиком є активізація кіберзагроз та діяльності ворожих спецслужб, які намагаються отримати доступ до чутливих даних шляхом хакерських атак, кібершпигунства чи вербування співробітників державних структур. Війна проти України значно загострила ці проблеми, оскільки інформаційний простір став одним із головних полів бою. Тому ефективна протидія таким викликам потребує не лише технічних рішень, а й посилення міжвідомчої координації та міжнародної співпраці.

Україна активно працює над удосконаленням системи охорони державної таємниці, щоб наблизити її до стандартів НАТО та ЄС. Одним із ключових напрямів виступає модернізація законодавчої бази. Зокрема, здійснюється перегляд Закону «Про державну таємницю» та суміжних нормативних актів для гармонізації класифікацій рівнів секретності, процедур доступу та вимог до захисту інформації. Поступово вводяться норми, які відображають міжнародні підходи до обмеження доступу за принципом «need-to-know» і взаємного визнання рівнів секретності між країнами-партнерами. Не менш важливим напрямом є розвиток інституційної структури. В Україні створені відповідальні органи за забезпечення охорони державної таємниці, серед яких ключову роль відіграють Служба безпеки України та спеціалізовані підрозділи Міністерства оборони. Водночас триває вдосконалення системи перевірки та допуску персоналу (security clearance) з урахуванням вимог НАТО та ЄС. Це сприяє формуванню більш надійної системи довіри у сфері спільного використання секретної інформації [3].

Технічна адаптація охоплює модернізацію систем захисту інформації: впроваджуються сучасні засоби шифрування, сертифіковані інформаційно-телекомунікаційні системи, удосконалюється кіберзахист державних органів та критичної інфраструктури. Важливим завданням є створення умов для безпечного функціонування спеціальних комунікаційних каналів, що використовуються для обміну даними з партнерами по НАТО та ЄС. Окремо варто відзначити кадрову та освітню складову. В Україні поступово розвивається система підготовки фахівців у сфері інформаційної безпеки, а також реалізуються програми міжнародної співпраці, що дозволяють українським спеціалістам навчатися у навчальних центрах НАТО та ЄС. Це сприяє формуванню професійних компетентностей і поширенню сучасних підходів до захисту секретної інформації.

Отже, у перспективі очікується подальша інтеграція України до євроатлантичного інформаційного простору. Це передбачає створення умов для оперативного та безпечного обміну секретними даними, участь у спільних інформаційних мережах, а також підвищення довіри з боку партнерів. Таким чином, адаптація стандартів НАТО та ЄС у сфері охорони державної таємниці не

лише зміцнює внутрішню систему безпеки України, а й сприяє її повноцінному входженню до колективних структур безпеки.

Список використаних джерел:

1. Ковалів К. Є. Правові аспекти захисту інформації з обмеженим доступом в Україні. *Інформація і право.* 2022. № 3 (38). С. 50-58.

2. Скачиляєс-Павлів О. Правові механізми забезпечення інформаційної безпеки в Україні. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки.* 2024. Том 11, № 2 (42). С. 151-158. DOI: 10.23939/law2024.42.151.

3. Izmailov Yaroslav, Yegorova Iryna. Possibilities of adapting the EU experience in information security to the conditions of Ukraine. *Economics and Technical Engineering.* 2023. Vol. 1, № 1, С. 35-43. DOI: 10.62911/ete.2023.01.01.03.