УДК 342.951

ФЕДОРЧЕНКО О.С., молодший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0009-0007-7358-7753.

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА КЛАСИФІКОВАНОЇ ІНФОРМАЦІЇ В ДЕЯКИХ ДЕРЖАВАХ ЄС ТА НАТО

Анотація. *Досліджено поняття, зміст та особливості обігу секретної (класифікованої) інформації. Визначено складові системи охорони державної таємниці та іншої інформації з обмеженим доступом. Розглянуто питання отримання, припинення та анулювання допуску та доступу для роботи із секретною інформацією та державною таємницею, особливості маркування класифікованої інформації, питання відповідальності за розголошення державної таємниці або класифікованої інформації на підставі узагальнення кращих практик зарубіжного досвіду нормативного забезпечення охорони державної таємниці у деяких країнах-членах НАТО та ЄС (Німеччини, Хорватії, Естонії). Визначено нормативні вимоги та існуючі стандарти у сфері охорони державної таємниці та секретної інформації. Деталізовано шляхи удосконалення вітчизняної системи охорони державної таємниці та службової інформації з урахуванням висвітлених основних позитивних тенденцій розвитку охорони класифікованої інформації в провідних європейських державах.*

Ключові слова: *класифікована інформація, секретна інформація, службова інформація, охорона державної таємниці, розголошення інформації з обмеженим доступом, державна політика у сфері забезпечення охорони державної таємниці, допуск до державної таємниці, криптографічний та фізичний захист секретної інформації,, НАТО, ЄС.*

Summary. *The concept, content and features of the circulation of secret (classified) information have been studied. The components of the system of protection of state secrets and other information with limited access are defined. The issue of obtaining, terminating and canceling clearance and access to work with classified information and state secrets, features of marking classified information, the issue of responsibility for disclosing state secrets or classified information based on the generalization of best practices of foreign experience in the regulatory protection of state secrets in some member states was considered NATO and the EU (Germany, Croatia, Estonia). Regulatory requirements and existing standards in the field of protection of state secrets and classified information are defined. Ways to improve the national system of protection of state secrets and official information are detailed, taking into account the highlighted main positive trends in the development of protection of classified information in the leading European states.*

Keywords: *classified information, secret information, official information, protection of state secrets, disclosure of information with limited access, state policy in the field of protection of state secrets, clearance to state secrets, access to information with limited access, NATO, EU.*

Постановка проблеми. Система охорони державної таємниці та класифікованої інформації є важливою складовою національної безпеки будь-якої країни світу. Аналіз законодавства у сфері охорони державної таємниці деяких країн НАТО та держав-членів ЄС переконливо засвідчує, що організація захисту класифікованої інформації є важливою умовою забезпечення національної безпеки, незалежно від таких факторів, як: політична система країни, її правова система або модель соціально-економічного розвитку.

Кожна держава-член ЄС має встановлені національним законодавством з урахуванням існуючих стандартів особливості щодо розроблених та запроваджених механізмів здійснення охорони державної таємниці, порядку організації допуску та доступу осіб до секретної інформації, процедур маркування інформації з обмеженим доступом, передумов та термінів засекречування та розсекречування матеріальних носіїв секретної інформації, перегляду їх грифів секретності, криптографічного та фізичного захисту секретної інформації тощо. Будь-яка країна НАТО та держава-член ЄС предметно переймається питаннями посилення правового захисту інформації у сфері забезпечення національної безпеки, які певною мірою пов'язані із несанкціонованим розголошенням державної таємниці або секретної інформації. У більшості країн НАТО та держав-членів ЄС питання охорони державної таємниці та класифікованої інформації регулюються спеціальними законодавчими та нормативними актами, присвяченими цій тематиці. Одночасно існують певні спільні риси між цими законами з точки зору обсягу та ступеня захисту державної таємниці з міркувань національної безпеки.

Для України в сучасних умовах, попри правовий режим воєнного стану, одним із важливих напрямів трансформації інституту державної таємниці та службової інформації є її реформування з метою прискорення впровадження інтеграційних вимог та нормативів Альянсу, що у свою чергу, передбачає імплементацію до національної системи охорони державної таємниці встановлених у країнах НАТО та провідних державах-членах ЄС стандартів у сфері класифікованої інформації. Вітчизняне законодавство у сфері охорони державної таємниці та службової інформації не повною мірою узгоджується з існуючими стандартами безпеки НАТО та ЄС, що може гіпотетично негативно вплинути як на міжнародні партнерські взаємовідносини за участю України у сфері захисту секретної інформації, навіть певним чином послабити процеси європейської та євроатлантичної інтеграції нашої держави. Серед європейських країн НАТО, система охорони державної таємниці та класифікованої інформації найбільш удосконалена у таких країнах, як: Німеччина, Хорватія та Польща. У цих державах ЄС діюча система охорона державної таємниці та державна політика у цій сфері найбільш узгоджуються з встановленими вимогами та стандартами, розробленими НАТО. У зв'язку із викладеним, актуальним і своєчасним є висвітлення кращих практик європейського досвіду у сфері здійснення правової регламентації та нормативного забезпечення здійснення охорони державної таємниці та класифікованої інформації (Німеччина, Хорватія, Естонія).

Результати аналізу наукових публікацій. Проблематику правової регламентації здійснення охорони державної таємниці та службової інформації досліджували у своїх працях такі вітчизняні вчені: С. Болдир [1], В. Галушка, Г. Тіхонов [2], О. Морозова [3], О. Семенюк [4] та інші. Кращі практики зарубіжного досвіду забезпечення охорони державної таємниці перебували у фокусі уваги В. Артемова [5], В. Глуховері [6], В. Олійника [7]. Охорону державної таємниці як важливу складову інформаційної безпеки вивчали: В. Павленко [8], А. Гуз, І. Касперський та С. Князєв [9]. Проте висвітлення особливостей правового регулювання охорони державної таємниці та класифікованої інформації у таких державах-членів ЄС та країнах НАТО, як Німеччина, Хорватія та Естонія, вказані фахівці не здійснювали, що зумовлює актуальність обраної тематики цієї наукової статті.

Метою статті є узагальнення організаційно-правових засад здійснення охорони державної таємниці і класифікованої інформації для удосконалення національного законодавства у сфері охорони інформації з обмеженим доступом з урахуванням кращих практик досвіду таких держав-членів ЄС та країнах НАТО, як Німеччини, Хорватії та Естонії.

Виклад основного матеріалу. На рівні ЄС питання охорони державної таємниці регламентовані рішенням Ради ЄС "Про правила безпеки для захисту секретної інформації" від 23 вересня 2013 року (2013/488/ЄС) [10]. Відповідно до європейського законодавства "секретна інформація ЄС" (EUCI) означає будь-яку інформацію, відомості або матеріали, позначені відповідним грифом секретності ЄС, несанкціоноване розголошення яких може завдати різного ступеня шкоди інтересам ЄС або одній чи кільком державам-членам. Тобто за законодавством ЄС секретна інформація – це відомості або матеріали, які вважаються конфіденційними та які потребують посиленого захисту. Нормативно встановлено, що метою проведення класифікації таємної інформації є її посилений захист. Загалом до системи організаційно-правових заходів щодо охорони державної таємниці на рівні ЄС відносяться: розроблення та реалізація особливого режиму створення й використання матеріальних носіїв секретної інформації; надання відповідальним органам дозволів на здійснення діяльності, пов'язаної з державною таємницею; створення та забезпечення функціювання секретного режиму діяльності уповноважених органів, які провадять діяльність, пов'язану з державною таємницею; розроблення та впровадження обмежень щодо поширення секретної інформації; надання допуску та доступу до державної таємниці у встановленому законодавством порядку.

Німеччина. За німецьким законодавством державна таємниця – це термін, який використовується для позначення відомостей, інформації або матеріалів загальнодержавного значення, які підпадають під найвищий рівень секретності. До поняття "державна таємниця" належить секретна інформація, яка, зазвичай, стосується функціонування та безпеки держави, її політичних, економічних, військових і дипломатичних аспектів. До переліку відомостей та матеріалів, які підпадають під ознаки державної таємниці застосовуються особливі заходи охорони та забезпечення секретності. Охорона державної таємниці є важливим складником захисту національної безпеки та державних інтересів. Допуск та доступ до секретних матеріалів, поводження з ними, умови та процедури обігу секретних відомостей і матеріалів регламентовані федеральним Законом Німеччини "Про вимоги і порядок проходження федеральних допусків та захисту секретної інформації" (Sicherheitsüberprüfungsgesetz) [11]. Відповідно до статті 4 цього Закону секретна (класифікована) інформація означає інформацію або висновки, які вимагають дотримання конфіденційності в інтересах держави і суспільства, зокрема для захисту добробуту федерального уряду чи будь-якої адміністративно-територіальної одиниці Німеччини (землі). Секретна інформація може включати документи, а також пов'язані з ними засоби для здійснення дешифрування, шифрування, передачі інформації (за допомогою криптографічного ключа) тощо. Також цей законодавчий акт доповнює Адміністративний регламент про фізичну безпеку, якою затверджено Інструкцію щодо секретної інформації – (Verschlusssachenanweisung) [12]. Система захисту державних секретів здійснюється за трьома напрямами та передбачає: удосконалення законодавства у сфері захисту державних секретів і секретів суб'єктів підприємництва (комерційна таємниця); посилення функціоналу органів контррозвідки та надання їм повноважень, зокрема й у сфері захисту державних секретів; сприяння створенню організацій "самодопомоги" в промисловості та їх діяльності.

Відповідно до статті 1 Закону Німеччини "Про вимоги і порядок проходження федеральних допусків та захисту секретної інформації" інформація з обмеженим доступом може мати три ступені секретності: "Цілком таємно" (Streng Geheim), "Таємно" (Geheim) та "Конфіденційно" (VS-Vertraulich). Маркування секретної інформації з грифом "Цілком таємно" або "Таємно" здійснюється у верхній та нижній

частинах кожної заповненої сторінки документа, де проставляється штамп або друкований червоним кольором рівень секретності із позначкою “Офіційна таємниця”. Сторінки документа повинні бути пронумеровані, а їх загальна кількість зазначається на першій сторінці. Для матеріалів із грифом “Конфіденційно” рівень секретності з позначкою “Офіційна таємниця” має бути проставлений або надрукований чорним або синім кольором у верхній частині кожної сторінки. Слід зазначити, що у ФРН до державної таємниці належать лише відомості, які необхідно зберігати в секреті від іноземних держав з метою недопущення завдання шкоди зовнішній безпеці Німеччини. Водночас відомості, які містять інформацію про проведення оперативно-розшукових заходів, належать до службової таємниці та охороняються відповідним законодавством.

У Німеччині відповідні документи, що містять службову таємницю, позначають грифом “Конфіденційно” (VS nur fur den dienstgebrauch). Якщо документи для службового користування обробляються в автоматизованих системах, то під час таких процесів дотримуються встановлені вимоги безпеки, зокрема автоматизовану систему має бути обладнано фаєрволом (у випадку підключення до мережі Інтернет) та має бути затверджений перелік осіб, які мають право виключного доступу до відповідної автоматизованої системи, котра адмініструє документи, що містять службову інформацію. Слід зазначити, що у ФРН до державної таємниці віднесено лише документи та відомості, які необхідно зберігати в секреті від іноземних держав з метою недопущення заподіяння шкоди зовнішній безпеці Федеративної республіки. Тоді як відомості, які містять інформацію про проведення оперативно-розшукових заходів, належать до службової таємниці та охороняються відповідним законодавством. Ступінь секретності того чи іншого документа, відомостей, ступені секретності науково-дослідних, дослідно-конструкторських і проектних робіт, які виконуються в інтересах забезпечення національної безпеки та оборони держави, встановлюються офіцерами секретної безпеки або спеціально призначеними для цього співробітниками.

У Німеччині існують різні ступені перевірки стану безпеки. Чим вище рівень допуску, тим суворішими є необхідні перевірочні заходи для особи, яка отримує допуск до державної таємниці. Проста форма перевірки безпеки, відома як допуск Ü1, вимагається, наприклад, для осіб, які мають доступ до секретних матеріалів з позначкою безпеки VS-VERTRAULICH (“Конфіденційно”). У цьому випадку заходи включають отримання необмеженої інформації з Федерального центрального реєстру (Bundeszentralregister) та консультації з Федеральним управлінням кримінальної поліції (Bundeskriminalamt) або федеральними розвідувальними органами відповідно до нормативних вимог Закону “Про вимоги і порядок проходження федеральних допусків та захисту секретної інформації”. Розширена перевірка безпеки, відома як допуск Ü2, необхідна, наприклад, для осіб, які мають доступ до секретних матеріалів з грифом GEHEIM (“Таємно”) або до певної кількості секретних документів з позначкою VS-VERTRAULICH.

Окрім заходів, пов’язаних із допуском до категорії Ü1, ця розширена перевірка також включає консультації з відділом поліції щодо місць, де проживав суб’єкт перевірки, а також загальну перевірку особи. Розширена перевірка безпеки з розслідуваннями в питаннях безпеки, відома як допуск Ü3, процедурно необхідна, наприклад, для осіб, які мають доступ до секретних матеріалів з грифом STRENG GEHEIM (“Цілком таємно”) або до великої кількості секретних документів з грифом GEHEIM (“Таємно”), а також для осіб, які планують працювати у Федеральному розвідувальному агентстві. У цьому випадку основним доповненням до заходів щодо допуску Ü2 є консультації за участю експертів або суддів, призначених під час

перевірки, та інших осіб, які можуть надавати інформацію. Особи, які займаються діяльністю, що вимагає отримання дозволу Ü3 або, в окремих випадках, дозволу Ü2, можуть бути зобов'язані завчасно повідомити компетентний орган перед здійсненням офіційних або приватних поїздок до та через країни, до яких застосовуються спеціальні заходи безпеки.

Починаючи з жовтня 2021 року, військовослужбовці, які виконують особливо важливі завдання в інтересах держави, і до яких висуваються суворіші вимоги щодо безпеки, повинні отримати підвищений розширений допуск, який передбачає форму SÜ4. У цьому випадку особа, яка проходить перевірку, отримує свою декларацію безпеки для оновлення лише через 30 місяців, а процес перевірки повторюється кожні п'ять років. Співбесіда із суб'єктом відбору в цьому випадку є обов'язковою відповідно до статті Закону Німеччини "Про правовий статус військовослужбовців" (Soldatengesetz) [13]. Уповноваженим органом у сфері охорони державної таємниці в Німеччині є Федеральне відомство охорони конституції (Bundesamt für Verfassungsschutz), яке вважається внутрішньою спецслужбою та підпорядковано Міністерству внутрішніх справ Німеччини. У ролі допоміжних органів у сфері охорони державної таємниці виступають, у рамках своєї компетенції та відповідно до функціональності, Федеральне міністерство оборони, Військова контррозвідувальна служба (Militärischer Abschirmdienst), які також беруть участь в організації перевірок осіб щодо дотримання ними заходів безпеки як майбутніх секретоносіїв. Як правило, відповідальність за допуск до інформації з обмеженим доступом у державному секторі покладається на уповноважений федеральний орган. Федеральне відомство з охорони конституції, Федеральне міністерство оборони, Військова контррозвідувальна служба збирають та узагальнюють відповідну інформацію, пов'язану з певною особою та перевіряють і оцінюють її, надалі надаючи рекомендацію компетентному органу про те, чи підходить певна особа, яку перевіряють, для подальшої конфіденційної роботи. Однак, у кінцевому підсумку, саме відповідний компетентний орган має остаточно вирішувати, чи буде призначення цієї особи для конфіденційної діяльності загрозою безпеці. У рамках чинного федерального законодавства кожні п'ять років встановлена вимога переоформлювати допуск до державної таємниці відповідним особам. Заповнена форма декларації у сфері безпеки щодо особи повинна бути знову представлена уповноваженому суб'єкту перевірки, який зобов'язаний оновлювати її, якщо будь-які з даних змінилися. Повторна процедура скринінгу повинна бути розпочата, як правило, з інтервалом в десять років. Заходи насправді є аналогічними до тих, що застосовуються під час первинного скринінгу. (п. 2 ст. 17 Закону). Таким чином, у Німеччині державна таємниця захищена кримінальним законодавством, а процедури отримання доступу та допуску до державної таємниці є нормативно врегульованими та передбачають надання тій чи іншій особі залежно від грифу таємності інформації дозволів за класифікатором Ü1, Ü2, Ü3, Ü4. Засекречування матеріальних носіїв інформації здійснюється шляхом надання відповідному документу, виробу або іншому матеріальному носію інформації грифу секретності. У Німеччині максимальний строк дії засекречуваних відомостей та інформації, які належать до державної таємниці, складає 50 років. З 15 червня 2022 року набули чинності законодавчі зміни, якими передбачається встановлення нормативних вимог щодо загальних обмежень для усіх осіб-носіїв державної таємниці на будь-які поїздки (приватні або службові) до або через країни, що входять до сфери геополітичного та геостратегічного впливу російської федерації (Вірменія, білорусь, Казахстан, Киргизстан, Сирія, Таджикистан, Туркменістан, Узбекистан). Список таких

країн був складений та затверджений Федеральним міністерством внутрішніх справ Німеччини [14].

Хорватія. На державному рівні охорона державної таємниці врегульована такими законодавчими актами, як "Про конфіденційність даних" [15] та "Про інформаційну безпеку" [16]. Законодавчо визначено, що відповідно до хорватської моделі охорони та захисту державної таємниці існує 4 види грифу секретності відомостей та даних, зокрема: "Цілком таємно", "Таємно", "Конфіденційно", "Обмежено" (ст. 4 Закону Хорватії "Про конфіденційність даних"). Державні органи, які здійснюють процедуру засекречування даних, мають компетенцію у сфері розробки критеріїв визначення ступенів секретності для даних щодо їхньої діяльності. Під час проведення процедур класифікації даних власник даних зобов'язаний визначити найнижчий рівень секретності, який забезпечує захист державних інтересів. Класифікацію відомостей та даних зі ступенем секретності "Цілком таємно" та "Таємно" можуть здійснювати: Президент Республіки Хорватія, Голова Хорватського парламенту, Прем'єр-міністр Республіки Хорватія, міністри, генеральний прокурор, начальник Генерального штабу Збройних сил Республіки Хорватія, керівники органів системи національної безпеки та розвідки Республіки Хорватія та особи, уповноважені ними для здійснення цих функцій. Протягом терміну дії рівня таємності даних власник зобов'язаний постійно оцінювати рівень таємності секретних даних і проводити періодичну оцінку, на основі якої рівень секретності може бути змінений або дані розсекречені. Періодична оцінка проводиться: за рівнем секретності "Цілком таємно" – не рідше одного разу на 5 років; за рівнем секретності "Таємно" – не рідше одного разу на 4 роки; за рівнем секретності "Конфіденційно" – не рідше 1 разу на 3 роки; для рівня секретності "Обмежено" – не рідше 1 разу на 2 роки. Власник даних повинен письмово повідомити всі органи, яким надано дані, про зміну рівня секретності або їхнє розсекречення. Спосіб позначення ступенів таємності секретних даних встановлюється постановою Уряду Хорватії. Доступ до секретних даних мають особи, яким це необхідно для виконання завдань у межах їх компетенції та яким видано сертифікат перевірки безпеки. Заява про видачу сертифіката подається особою, яка оформлює допуск до державної таємниці в письмовій формі до уповноваженого державного органу – Управління Ради національної безпеки Хорватії.

Сертифікат безпеки видається за відповідними рівнями секретності загальним строком на п'ять років. Сертифікат видається Управлінням Ради національної безпеки на підставі оцінки відсутності перешкод та загроз для доступу до секретних даних. Наявність перешкод безпеки визначається на підставі перевірки безпеки, проведеної вищезазначеним компетентним органом. Перешкодами у питаннях безпеки можуть стати: неправдиве надання інформації в анкеті перевірки безпеки, факти, які можуть перешкоджати для прийняття певної особи на державну службу (непогашена судимість, накладені дисциплінарні стягнення) та інші факти, які є підставою для сумнівів щодо надійності особи для роботи із секретними даними. Особа, якій було відмовлено у видачі сертифіката, не має права подати апеляційну скаргу, але має право порушити адміністративний спір протягом 30 днів з дня отримання відповідного рішення.

Стаття 22 Закону "Про конфіденційність даних" встановлює особливості видачі сертифіката щодо доступу до таємних даних інших держав і міжнародних організацій, що надається особам, яким це необхідно для виконання завдань у межах своєї компетенції на підставі міжнародного договору або угоди про безпеку. Державні органи, органи місцевого та регіонального самоврядування, юридичні особи з публічними

повноваженнями здійснюють ведення обліку перевірок та поводження із секретною інформацією. Перевірка безпеки загалом триває 3 місяці.

Правовий порядок здійснення захисту секретних даних визначається положеннями Закону "Про інформаційну безпеку". Заходи та стандарти інформаційної безпеки встановлюються відповідно до ступеня секретності, кількості, типу та загроз секретних даних у конкретному місці. Для секретної інформації рівня секретності "Конфіденційно", "Таємно" та "Цілком таємно" постійно проводиться оцінка загроз безпеки. Стаття 5 вказаного Закону регламентує, що такі заходи та стандарти включають: нагляд за доступом і обробкою секретних даних; обробку у випадку несанкціонованого розкриття та втрати секретних даних; планування заходів у надзвичайних ситуаціях; створення спеціальних фондів даних для зберігання секретних даних, які надалі надаються іншою країною, міжнародною організацією чи установою, з якою Республіка Хорватія співпрацює. Сфери інформаційної безпеки, для яких передбачені заходи та стандарти інформаційної безпеки включають: перевірку безпеки (фізичну безпеку, безпеку даних, безпеку інформаційної системи, безпеку ділового співробітництва). Стаття 11 Закону встановлює, що безпека даних – це сфера інформаційної безпеки, для якої встановлено заходи та стандарти інформаційної безпеки, які застосовуються як загальні захисні заходи з метою запобігання, виявлення та усунення збитків внаслідок втрати або несанкціонованого розголошення секретних даних. Державні органи та юридичні особи, які використовують секретні дані у своїй діяльності, зобов'язані застосовувати процедури щодо роботи із секретними даними, щодо змісту та способу ведення записів, проведення перевірок секретних даних і моніторингу безпеки даних, передбачених заходів та стандартів інформаційної безпеки.

Основним підзаконним нормативним актом у зазначеній сфері є затверджене Урядом Хорватії "Положення про спосіб маркування секретної інформації, зміст, зовнішній вигляд свідоцтва про проведену перевірку безпеки та поводження із секретною інформацією" [17]. Це Положення поширюється на державні органи, уповноважені здійснювати засекречування та розсекречування інформації, а також на юридичних і фізичних осіб, уповноважених працювати із секретною інформацією. Позначення рівня секретності здійснюється при створенні секретних документів та інших записів таємної інформації або під час періодичної оцінки ступеня секретності даних відповідно до ст. 14 Закону Хорватії "Про конфіденційність даних". Позначення ступеня секретності таємних даних зазначається на кожній сторінці документа у верхньому правому куті великими літерами, а для інших записів секретних даних позначка про ступінь секретності має бути надрукована на видному та чіткому друкарському вигляді відповідно до вимог збереження корисної цінності секретних даних. Для цілей ведення записів щодо секретних даних можуть використовуватися абревіатури "VT" для "Цілком таємно", "T" для "Таємно", "POV" для "Конфіденційно" та "OGR" для "Обмежено". Позначення рівня секретності та додаткових відміток здійснюється при створенні секретних даних або шляхом подальшої обробки шляхом штампування, друкування, написання, склеювання або прикріпленням відповідних засобів до запису секретних даних. Кожна сторінка секретного документа повинна мати в нижньому правому куті нижнього колонтитула документа номер сторінки, зазначений стосовно загальної кількості сторінок. Номер, тип, найменування та ступінь секретності вкладень зазначаються на останній сторінці документа. Зазначення кількості примірників стосовно загальної кількості примірників секретного документа зазначається на першій сторінці документа у правому верхньому куті документа, нижче позначки про ступінь секретності. У разі використання додаткових захисних відміток,

позначка про номер примірника проставляється нижче додаткових захисних позначок. Власник секретних даних може також позначати інформацію додатковими захисними позначками про: заборону або обмеження дублювання даних; заборону, обмеження та спосіб подальшого розповсюдження даних для інших одержувачів і встановлювати зобов'язання повернення секретних даних; закінчення строку дії секретності, який власник секретних даних надав під час їх створення. Додаткові позначки проставляються на першій сторінці документа чи іншого запису секретних даних великими літерами під знаком рівня секретності секретних даних і можуть бути розміщені на всіх сторінках документа, якщо це важливо для додаткового маркування. У рядку зі ступенем секретності секретних даних додається додаткове посилання про закінчення строку секретності шляхом позначення терміну закінчення або посилання на подію, яка має певну тривалість.

Питання конфіденційного захисту даних у Міністерстві оборони урегульовано відповідним наказом оборонного відомства Хорватії [18]. Цей наказ визначає перелік секретних даних захисту, осіб, уповноважених визначати секретні дані захисту, критерії визначення ступеня секретності даних захисту, порядок здійснення засекречування та розсекречування даних і питання доступу до секретних даних. У Міністерстві оборони Хорватії у питаннях військової таємниці використовуються загальнодержавні 4 грифи секретності: "Цілком таємно", "Таємно", "Конфіденційно", "Обмежено". Порядок та умови засекречування відомостей, створених у Міністерстві оборони, здійснюють відповідальні особи, які є розробниками секретних даних. Власником секретних даних у розумінні цього наказу є Міністерство оборони, Генеральний штаб Збройних Сил, Збройні Сили Хорватії. Класифікація здійснюється під час створення секретних даних під час якої ступінь секретності даних визначається відповідно до їх змісту. Розробники секретних даних зобов'язані постійно оцінювати ступінь їхньої секретності. Періодичне оцінювання не є необхідним, якщо створювач секретних даних після їх створення визначає та позначає крайній термін, протягом якого ступінь секретності може бути знижений. Періодична оцінка секретних даних у сфері оборони та військової системи безпеки і розвідки здійснюється у такі строки, встановлені на підставі нормативних вимог у сфері захисту секретних даних (ст. 15): за ступенем секретності "Цілком таємно", не рідше одного разу на 5 років; для рівня секретності "Таємно" не рідше одного разу на 4 роки; для рівня секретності "Конфіденційно" не рідше одного разу на 3 роки; для рівня секретності "Обмежено", не рідше одного разу на 2 роки.

Рішення про розсекречування або зміну грифу секретності даних приймає Міністр оборони щодо даних, які належать Міністерству оборони, начальник Генерального штабу Збройних Сил – щодо даних, які належать Генеральному штабу Збройних Сил. Розробники секретних даних готують письмову оцінку-обґрунтування, в якій вони викладають усі відповідні обставини, факти та події, які вимагають або призводять до захисту даних з певним ступенем секретності, і повинні обґрунтувати необхідність продовження збереження секретності даних. Рішення про розсекречення даних обов'язково визначає умови подальшої обробки або публічного використання розсекречених даних. Міністр оборони, начальник Генерального штабу Збройних Сил можуть здійснювати колективне розсекречення або зміну рівня секретності певної групи відомостей або даних. Якщо у процесі періодичної оцінки рівень секретності знижується або розсекречується, первісне позначення рівня секретності викреслюється на документі чи іншому записі секретних даних і запроваджується новий рівень секретності. Про розсекречування або зниження рівня секретності даних створювач повідомляє кожного адресата, якому надійшли дані.

Також Управління Офісу РНБО Хорватії здійснює та координує міжнародне співробітництво у сфері інформаційної безпеки і на підставі Рішення Уряду Хорватії є відповідальною структурою, яка укладає міжнародні угоди з безпеки та захисту секретної інформації від імені держави. Тобто цей державний орган має національну та міжнародну компетенцію. В межах національної компетенції: здійснює координацію і гармонізацію прийняття та впровадження заходів і стандартів у сфері інформаційної безпеки в Республіці Хорватія; на підставі рішення Уряду проводить переговори та укладає міжнародні угоди з безпеки щодо взаємного захисту та обміну секретною інформацією; здійснює навчання та координує роботу адміністраторів і координаторів з питань безпеки в державному та комерційному секторах, включаючи юридичні особи; видає допуски (сертифікати) безпеки для фізичних осіб, зокрема громадян Хорватії, які працюють з секретною інформацією та оформлює допуски (сертифікати) безпеки для юридичних осіб; здійснює нагляд за впровадженням заходів та стандартів інформаційної безпеки в державних органах і юридичних особах, які працюють з секретною інформацією тощо. У сфері міжнародної юрисдикції: опікується питаннями забезпечення безпеки секретної інформації на теренах НАТО/ЄС як в національних органах влади, так і за кордоном; видає допуски стандарту НАТО/ЄС для громадян Хорватії, які працюють із секретною інформацією НАТО/ЄС, яка має класифікацію "Конфіденційно", "Таємно" та "Цілком таємно"; адмініструє роботу Реєстру з питань міжнародної секретної інформації; здійснює акредитацію безпеки інформаційних систем Реєстру; забезпечує впровадження технічних заходів безпеки інформаційних систем та контролює роботу державних органів за цим напрямком; відповідно до правил безпеки НАТО/ЄС контролює обробку секретної інформації в інформаційно-комунікаційних системах.

Право доступу до секретних даних, створених у діяльності Міністерства оборони, Генерального штабу Збройних Сил мають особи, яким вони потрібні для виконання завдань у межах їхньої компетенції, яка визначена посадовими інструкціями. Для доступу до секретних даних особи повинні мати: свідоцтво про допуск (сертифікат) на відповідний рівень секретності; висновки щодо проведених заходів інформаційної безпеки; повноваження доступу до окремих секретних даних. Клопотання про видачу сертифіката подається особами, призначеними на виконання обов'язків відповідно до Переліку посад і робіт, перебування на яких потребує доступу до секретної інформації Міноборони або Генерального штабу Збройних Сил. Загалом в Хорватії максимальний строк дії засекречуваних відомостей та інформації, які належать до державної таємниці встановлено строком 50 років, а мінімальний – 5 років.

Таким чином, у Хорватії існують такі особливості у сфері охорони державної таємниці. По-перше, уповноваженим державним органом у сфері захисту та охорони державної таємниці визначено Управління Офісу Ради національної безпеки і оборони Хорватії. По-друге, у законодавстві Хорватії визначається на рівні з державною таємницею ще й військова таємниця, тобто є розмежування між ними. По-третє, класифікація секретної інформації здійснюється за загальноєвропейськими стандартами та передбачає 4 грифи секретності: "Цілком таємно", "Таємно", "Конфіденційно", "Обмежено". По-четверте, законодавство Хорватії регламентує особливості здійснення охорони державної таємниці, зокрема встановлює номенклатурні процедури видачі допуску (сертифікату безпеки) до державної таємниці, здійснення засекречування та розсекречування секретної інформації, надання доступу до секретних матеріалів і відомостей третім країнам або міжнародним організаціям.

Естонія. Питання здійснення охорони державної таємниці регулюється Законом Естонії "Про державну таємницю та секретну іноземну інформацію" [19]. Законодавчо визначено, що державна таємниця – інформація, яка вимагає охорони від розкриття в інтересах національної безпеки або міжнародних відносин Естонії, за винятком секретної інформації іноземних держав. Таким чином, вищезазначений стандарт визначення містить дві важливі особливості: (а) інформація має бути визначена як державна таємниця відповідно до положень закону про державну таємницю та секретну іноземну інформацію та (б) вона повинна вимагати захисту від оприлюднення в інтересах забезпечення безпеки Естонії. Формально державною таємницею є інформація, розголошення якої може поставити під загрозу безпеку Естонії або завдати шкоди міжнародним відносинам за її участю. Розкриття державної таємниці може у більш серйозних випадках завдати суттєвої шкоди загальному функціонуванню держави, її політичній, військовій або дипломатичній сферам. Захист державної таємниці є важливою складовою запобігання розвідувально-підривній діяльності іноземних спецслужб проти Естонії. Одночасно важливим завданням цього законодавчого акта є захист державної таємниці та секретної інформації від розголошення.

На законодавчому рівні залежно від ступеня секретна інформація поділяється на: "Обмежену", "Конфіденційну", "Таємну" та "Цілком таємну". Доступ до державної таємниці зазвичай надається тільки після проходження перевірки безпеки (спеціальної перевірки), при якій оцінюються надійність та індивідуальні ризики. Дозволи на доступ до державної таємниці поділяються на два види – дозвіл для фізичної особи та дозвіл для юридичної особи. Перевірка безпеки фізичної особи зазвичай триває 3 місяці та може бути продовжена ще на наступні 3 місяці. Перевірка безпеки юридичної особи, як правило, триває 6 місяців, і її також можна продовжити до 12 місяців. Під час проведення перевірки безпеки контролюючий орган в особі Агентства оборонної поліції має у межах повноважень досить широку компетенцію здійснювати перевірки минулого особи, у тому числі, обставини приватного життя. Межі перевірки особи напряму залежать від особи конкретного заявника. Усі заявники, які звернулися із вимогою отримати доступ до державної таємниці проходять співбесіду за фізичної присутності. За підсумками перевірки особа, яка пройшла перевірку безпеки отримує сертифікат допуску до державної таємниці, який видає Агентство оборонної поліції або сертифікат секретної іноземної інформації, що видає уповноважений представник органів державної безпеки, який діє при Службі зовнішньої розвідки Естонії. Після отримання сертифікатів особи, які запитують доступ, також ознайомлюються з вимогами безпеки обробки секретної зовнішньої інформації.

Важливим додатком до вказаного закону є Порядок охорони державної таємниці та секретної іноземної інформації, затверджений Урядом Естонії і який набув чинності з 1 січня 2008 року [20]. Так, зокрема ст. 51 регламентує, що до реєстру носіїв секретної інформації вносяться: 1) дані, необхідні для ідентифікації носія інформації: реєстраційний номер, дата реєстрації, дата виготовлення, назва установи, від якої надійшов носій інформації, та реєстраційний номер передавача також назву, автора та підписанта документа; 2) тип носія інформації; 3) підстави засекречування носія інформації, рівень і строк засекречування, їх зміну та підстави внесення зміни; 4) кількість і номери примірників; кількість примірників не потребує внесення до реєстру, якщо носій інформації має обмежену та конфіденційну інформацію; 5) кількість частин носія інформації і кількість сторінок документа; 6) кількість примірників; 7) найменування органу обробки, до якого передано носій секретної інформації або його копію, та час передачі; підпис одержувача або номер акта прийому-передачі; 8) відмітка

про те, коли другим блоком обробки даних надано дозвіл на передачу секретної інформації, що міститься на носії секретної інформації, до третього блоку обробки; 9) підтверджена ознака знищення носія інформації.

Опрацювання державної таємниці – це загальний термін, який включає будь-які операції з державною таємницею або секретною іноземною інформацією, що включає складання, маркування, збирання, зберігання, перевезення, відтворення, передачу, знищення, виготовлення витягів з них, ознайомлення з ними або будь-які інші дії, що здійснюються з інформацією чи носієм інформації незалежно від способу виконання дії або використаних засобів. У рамках вимог законодавства кожні 5 років треба переоформлювати допуск до державної таємниці відповідним особам – носіям державної таємниці. Заповнена форма декларації безпеки щодо особи повинна бути знову представлена уповноваженому суб'єкту перевірки, який зобов'язаний оновлювати її, якщо будь-які із даних змінилися. Для позначення рівня секретності розділів тексту, менших за одну сторінку, у секретних документах як Естонії, так і НАТО можуть використовуватися наступні стандартні скорочення: CTS, NS, NC, NR. Документи часто мають позначення NATO UNCLASSIFIED. Це несекретна інформація, але вона все одно потребує захисту. В Естонії максимальний строк дії засекречуваних відомостей та інформації, які відносяться до державної таємниці загалом складає 50 років, а мінімальний – 5 років.

У жовтні 2023 року Міністр внутрішніх справ Естонії розширив перелік країн, відвідування яких для осіб, що мають доступ до державної таємниці є загрозливим та небажаним. Список, куди раніше занесли рф, білорусь і кндр, тепер поповнили Вірменія, Азербайджан, Китай (включно з Макао і Гонконгом), іран, Казахстан, Киргизстан, Таджикистан, Туркменістан і Узбекистан. За офіційним повідомленням МВС Естонії перебування у вказаних країнах носіїв секретних відомостей загрожує державним секретам через діяльність органів безпеки зазначених держав. Особи-носії державної таємниці мають повідомляти про такі поїздки до перелічених країн не пізніше ніж за п'ять днів до їх початку [21]. Національним органом у сфері забезпечення охорони державної таємниці визначено Агентство оборонної поліції, яке уповноважене захищати державну таємницю, контролювати та гарантувати безпеку у цій сфері. Одночасно відповідальність за порушення вимог щодо забезпечення охорони державної таємниці несе відповідна службова особа, якій надано такі повноваження у рамках діяльності міністерств та відомств Естонії.

Висновки.

Аналіз законодавства деяких європейських країн (Німеччини, Хорватії, Естонії) у сфері охорони державної таємниці переконливо засвідчує, що організація захисту класифікованої інформації є важливою умовою забезпечення національної безпеки. Кожна проаналізована держава, враховуючи стандарти НАТО та ЄС встановлює у рамках вітчизняного законодавства національні особливості щодо організаційно-правового механізму охорони державної таємниці. Це стосується організації допуску та доступу осіб до секретної інформації, процедур маркування інформації з обмеженим доступом, умов та строків засекречування/розсекречування матеріальних носіїв секретної інформації, перегляду грифів секретності, а також криптографічного і фізичного захисту секретної інформації тощо. У більшості європейських держав питання охорони державної таємниці та класифікованої інформації регулюються спеціальними законодавчими й нормативними актами, що стосуються цієї сфери в різних юрисдикціях. Водночас існують певні спільні риси між цими нормативно-

правовими приписами з огляду на обсяг та ступень захисту державної таємниці з міркувань національної безпеки.

Відповідно до проведеного аналізу зарубіжного законодавства у сфері державної таємниці, можна виділити три основні аспекти, пов'язані із національною безпекою: 1) класифікація державної таємниці; 2) маркування та поріг її розкриття; 3) наслідки розкриття інформації з обмеженим доступом. Тобто національне законодавство у сфері охорони державної таємниці тієї чи іншої держави-члена ЄС включає: поняття, порядок, передумови та особливості класифікації секретної інформації, порогові критерії її розкриття або розголошення; визначення порядку та умов надання допуску та доступу до інформації з обмеженим доступом; встановлення відповідальності за її несанкціоноване розголошення або оприлюднення, співвідношення державної таємниці та секретної інформації із кластерами інформаційної безпеки держави та її криптографічним і фізичним захистом. Законодавство у сфері державної таємниці може встановлювати певні граничні порогові значення для розкриття секретної інформації, які часто є невіддільною частиною прийнятого методу класифікації або винятком з режиму захисту державної таємниці.

За результатами узагальнення здобутків позитивного іноземного досвіду можна визначити основні напрями у сфері охорони державної таємниці та іншої інформації з обмеженим доступом, зокрема це: забезпечення національної безпеки, гарантування державних інтересів, підтримання обороноздатності країни; недопущення витоку або розголошення державних секретів, конфіденційних даних або класифікованої інформації; пошук оптимальних шляхів з метою недопущення або мінімізації шкоди, яка може бути завдана державним інтересам внаслідок розголошення або оприлюднення інформації з обмеженим доступом; встановлення підвищених вимог щодо перевірки безпеки та ретельний відбір осіб-носіїв секретної інформації; посилення заходів у сфері охорони секретної інформації шляхом реалізації організаційно-правових заходів, які забезпечують фізичний і матеріальний захист секретної інформації, включно з криптографічним.

Суттєвий вплив на ефективність охорони державної таємниці мають організаційно-правові заходи, спрямовані на розроблення відповідним уповноваженим органом нормативно-правових актів з метою унормування та забезпечення охорони державної таємниці, її подальшого фактичного впровадження. Закріплення на законодавчому рівні встановлених політикою безпеки НАТО та ЄС стандартів і процедур щодо застосування системи ступенів обмеження доступу до інформації дозволяє значно демократизувати цей процес, забезпечивши його прозорість, що сприятиме оптимізації роботи з визначення ступенів секретності матеріальних носіїв інформації, а також гармонізації та адаптації національного законодавства країн НАТО і держав-членів ЄС до вимог спільної політики безпеки євроатлантичного та європейського співтовариства. Адже політика безпеки НАТО та ЄС у частині регулювання інформації з обмеженим доступом залишає досить широкі рамки, в яких можуть варіюватися конкретні норми національного законодавства тієї чи іншої країни.

Для України в умовах правового режиму воєнного стану та анонсованого реформування вітчизняної системи охорони державної таємниці та службової інформації з урахуванням висвітлених основних позитивних тенденцій розвитку охорони класифікованої інформації в провідних європейських державах, актуальним залишаються: об'єднання державної таємниці та службової інформації в єдину категорію інформації, доступ до якої обмежується виключно в інтересах, передбачених статтею 6 Закону України "Про доступ до публічної інформації", та яка підлягає охороні державою; здійснення заходів щодо впровадження нових комплексних підходів та створення

уніфікованої системи безпеки як державної таємниці, так і службової інформації, яка б забезпечувала в усіх сферах надійний та ефективний захист чутливих відомостей, спеціальний режим доступу до яких встановлюється, виходячи із пріоритетних інтересів держави; закріплення на законодавчому рівні встановлених політикою безпеки НАТО та ЄС стандартів та процедур щодо застосування системи ступенів та грифів обмеження доступу до інформації; визначення у вітчизняному законодавстві у сфері охорони державної таємниці Служби безпеки України як національного органу безпеки класифікованої інформації; запровадження нової моделі функціонування системи охорони державної таємниці, системного підходу до безпеки секретної інформації, створення державної системи охорони секретної інформації на основі втілення єдиної категорії інформації з обмеженим доступом – класифікованої інформації; адаптація законодавства у цій сфері з урахуванням загальноприйнятих стандартів та кращих практик держав-членів ЄС та країн НАТО.

Виходячи із викладеного, необхідним є прискорення схвалення на законодавчому рівні законопроекту "Про безпеку класифікованої інформації" [22], яким передбачається перехід на 4-ох ступеневу систему обмеження доступу до інформації, запровадження системного підходу до безпеки секретної інформації, створення державної системи охорони секретної інформації на основі втілення єдиної категорії інформації з обмеженим доступом з урахуванням загальноприйнятих стандартів НАТО, імплементації сучасної моделі функціонування системи безпеки класифікованої інформації (державної таємниці та службової інформації) та гармонізації у вітчизняне законодавство вимог та стандартів НАТО та ЄС у сфері безпеки класифікованої інформації.

Використана література

1. Болдир С.В. Перспективи реформування системи охорони державної таємниці та службової інформації. *Інформація і право.* № 4(23)/2017. С. 79-85.

2. Галушка В., Тіхонов Г. Особливості правового регулювання захисту державної таємниці в Україні та за її межами. *Підприємництво, господарство і право.* 2021. № 1. С. 205-209.

3. Морозова О.О. Правова охорона державної таємниці в Україні. *Науковий часопис Національного педагогічного ун-ту ім. М.П. Драгоманова. Серія 18: Право*. 2017. Вип. № 32. С. 101-105.

4. Семенюк О.Г. Державна політика та стратегія у сфері охорони державної таємниці. *Інформаційна безпека людини, суспільства, держави*. 2017. № 2. С. 142-149.

5. Артемов В.Ю. Класифікація захисту інформації з обмеженим доступом НАТО. *Захист інформації.* 2008. № 1. С. 80-84.

6. Глуховеря В.А. Іноземний досвід адміністративно-правового регулювання захисту інформації з обмеженим доступом. *Право і суспільство.* 2015. № 4. С. 67-73.

7. Олійник В.І. Досвід кримінально-правового забезпечення охорони державної таємниці країн близького зарубіжжя. *Юридична наука.* 2020. № 12 (114). С. 114-152.

8. Павленко В.С. Охорона державної таємниці у механізмі інформаційної безпеки. *Юридичний науковий журнал.* 2021. № 4. С. 255-258.

9. Гуз А.М., Касперський І.П., Князєв С.О. Охорона державної таємниці в Україні: навч. посіб. Київ: Нац. акад. СБУ, 2017. 216 с.

10. 2013/488/EU: Council Decision of 23 September 2013 on the security rules for protecting EU classified information. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013D04 88

11. Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen. (SÜG). 20.04.1994. URL: https://www.gesetze-im-internet.de/s_g

12. Verschlusssachenanweisung 24.04.2024. URL: https://www.umwelt-online.de/regelwerk/cgi-vsa. htm&such=Verwaltungsvorschrift%20%FCber%20die

13. Gesetz über die Rechtsstellung der Soldaten. 30.05.2005. URL: https://www.buzer.de/gesetz/2246/index.htm

14. Staatenlisten im Sinne von § 32 SÜG (Reisebeschränkungen). URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/staatenliste-para-32-anleitung-sicherh eitserklaerung.pdf?__blob=publicationFile&v=6

15. Zakon o tajnosti podataka. 07.08.2007. URL: https://www.zakon.hr/z/217/Zakon-o-tajnosti-pod ataka

16. Zakon o informacijskoj sigurnosti. 30.7.2007. URL: https://www.zakon.hr/z/218/Zakon-o-infor macijskoj-sigurnosti

17. Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu Uvjerenja o obavljenoj sigurnosnoj provjeri i Izjave o postupanju s klasificiranim podacima. 04.10.2007. URL: https://www.zakon.hr/cms.htm?id=1530

18. Pravilnik o tajnosti podataka obrane. 25.07.2018. № 67/18. URL: https://www.zakon.hr/cms.htm?id=45445

19. Riigisaladuse ja salastatud välisteabe seadus 25.01.2007. URL: Riigisaladuse ja salastatu dvälistea beseadus–Riigi Teataja

20. Riigisaladuse ja salastatud välisteabe kaitse kord 20.12.2007. URL: https://www.riigiteataja.ee/akt/ 12903659

21. Eestis on täiendatud riikide nimekirja, kuhu riigisaladuse kandjad peavad oma visiitide kohta teatama. URL: https://www.err.ee

22. Про безпеку класифікованої інформації: проект закону України від 27.01.23 р. № 8394. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/41249

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~