Аналітична записка
з питань порівняльного законодавства щодо правового регулювання охорони державної таємниці та класифікованої інформації
в окремих державах-членах НАТО*

Анотація. В аналітичній записці досліджено поняття, зміст та особливості обігу секретної (класифікованої) інформації, визначено складники системи охорони державної таємниці та іншої інформації з обмеженим доступом, розглянуто питання отримання, припинення та анулювання допуску й доступу для роботи із секретною інформацією та державною таємницею, маркування класифікованої інформації, питання відповідальності за розголошення державної таємниці або класифікованої інформації на підставі узагальнення кращих практик закордонного досвіду нормативного забезпечення охорони державної таємниці в державах-членах НАТО (проаналізовано законодавство семи країн: Великобританії, Франції, Німеччини, Польщі, Естонії, Хорватії та Чехії). Визначено нормативні вимоги та наявні стандарти у сфері охорони державної таємниці та секретної інформації, які діють у НАТО та ЄС.

Розглянуто організаційно-правові засади позначення інформації з обмеженим доступом, особливості її поширення та засекречування/розсекречування, а також умови й порядок надання доступу службовим особам до державної таємниці. Окреслено пріоритети державної політики у сфері охорони державної таємниці та захисту секретної (класифікованої) інформації, розкрито компетенції національних уповноважених державних органів, на які покладені функції із забезпечення захисту державної таємниці та службової інформації. Виявлено спільні риси та національні відмінності під час організації захисту та охорони державної таємниці й класифікованої інформації.

Виявлено спільні риси та національні відмінності в підходах до організації захисту державної таємниці та класифікованої інформації.

Ключові слова: класифікована інформація, секретна інформація, службова інформація, охорона державної таємниці, розголошення інформації з обмеженим доступом, допуск до державної таємниці, доступ до інформації з обмеженим доступом, сертифікація, криптографічний та фізичний захист секретної інформації, засекречування матеріальних носіїв секретної інформації, гриф обмеження доступу, стандарти НАТО у сфері секретів та охорони державної таємниці, нормативні вимоги ЄС щодо класифікованої інформації, відповідальність за розголошення державної таємниці.

I. Вступна частина

Аналіз законодавства європейських країн (держав-членів НАТО) у сфері охорони державної таємниці переконливо засвідчує, що організація захисту класифікованої інформації є важливою умовою забезпечення національної безпеки. Це твердження є справедливим незалежно від політичної системи держави, її правової системи або моделі соціально-економічного розвитку.

Одним із напрямів трансформації інституту державної таємниці та службової інформації є його реформування з метою прискорення впровадження інтеграційних вимог та нормативів Альянсу, що, своєю чергою, передбачає імплементацію

встановлених стандартів у сфері класифікованої інформації провідних держав-членів НАТО до національної системи охорони державної таємниці.

За результатами проведеного дослідження можна констатувати, що вітчизняне законодавство у сфері охорони державної таємниці та службової інформації не повною мірою узгоджується з наявними стандартами безпеки НАТО та ЄС, що становить ризики негативного впливу на міжнародні партнерські взаємовідносини України у сфері захисту інформації, ускладнення північноатлантичних та євроінтеграційних процесів нашої держави.

Кожна держава, враховуючи стандарти НАТО та ЄС, встановлює національним законодавством особливі механізми 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 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 погляду обсягу та ступеня захисту державної таємниці з міркувань національної безпеки.

Відповідно до проведеного огляду закордонного законодавства про державну таємницю, 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 НАТО включає: поняття, порядок, умови 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. Як правило, порогові значення розкриття секретної інформації включають критерій шкоди та критерій суспільного інтересу. Уповноважені особи можуть забезпечити доступ до секретної інформації лише за умови, що вони діють на основі еквівалентних правил та стандартів у сфері забезпечення інформаційної безпеки з метою захисту інформації з обмеженим доступом. Також у кожній державі законодавчо визначено національний орган, який уповноважений здійснювати функції та повноваження у сфері охорони державної таємниці та класифікованої інформації. Серед європейських держав-членів НАТО найбільш удосконалені системи охорони державної таємниці діють у таких державах, як Великобританія, Німеччина, Франція, Польща. У цих державах

системи охорони державної таємниці та державна політика в цій сфері найбільш відповідають вимогам і стандартам НАТО.

За результатами аналізу здобутого позитивного закордонного досвіду можна визначити основні напрями державного управління у сфері охорони державної таємниці та іншої інформації з обмеженим доступом, зокрема, це:

- забезпечення національної безпеки, державних інтересів, 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;
- охорона секретної інформації здійснюється в рамках 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, які спрямовані на розроблення відповідним уповноваженим органом нормативно-правових актів з метою унормування та забезпечення охорони державної таємниці, її подальшого фактичного впровадження.

До системи організаційно-правових заходів охорони державної таємниці на рівні ЄС належать: 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; запровадження особливих правил здійснення державними органами своїх функцій щодо державних органів, органів місцевого самоврядування, установ, підприємств та організацій, діяльність яких пов’язана із секретною інформацією; розроблення та впровадження обмежень щодо поширення секретної інформації; надання допуску та доступу до державної таємниці у встановленому законодавством порядку.

Сучасні загальні тенденції розвитку системи охорони державної таємниці включають укладання та виконання угод про взаємний захист секретної інформації на рівні держав-членів НАТО та ЄС. Такі угоди між Європейським Союзом і різними країнами світу спрямовані на зміцнення безпеки через обмін секретною інформацією та запровадження механізмів для її захисту. Відповідно до зобов’язань і домовленостей, кожна зі сторін повинна забезпечувати захист секретної інформації, наданої іншою стороною.

Також сторони повинні дотримуватися процедури обміну секретною інформацією, призначати відповідальних осіб від кожної сторони з метою контролю за виконанням угоди, надавати взаємну допомогу щодо забезпечення безпеки секретної інформації (наприклад, Угода про взаємний захист секретної інформації та

процедур безпеки між ЄС та Великобританією 2021 року[1], Угода між Україною та Європейським Союзом щодо процедур безпеки обміну секретною інформацією 2005 року[2] тощо.

У зв'язку із диференційованими підходами до охорони державної таємниці та класифікованої інформації у європейських державах-членах НАТО, доцільно розглянути правове регулювання поняття, змісту та особливостей доступу до такої інформації у контексті досвіду окремих із них (Великобританії, Німеччини, Франції, Польщі, Естонії, Хорватії, Чехії).

ІІ. Основна частина

Досвід та стандарти Європейського Союзу. За законодавством ЄС секретна інформація – це відомості або матеріали, які вважаються визнаються конфіденційними й потребують захисту. Класифікація секретної інформації здійснюється з метою її захисту, дотримуючись принципу, за яким вищі класи секретності охороняють інформацію, витік якої може становити загрозу національній безпеці.

Класифікація формалізує те, що належить до категорії «державна таємниця», і визначає різні рівні захисту на основі очікуваної та вірогідної шкоди, яку інформація, відомості або матеріали можуть завдати у випадку їхнього розголошення або несанкціонованого розкриття, втрати. З метою перегляду або обробки секретних матеріалів з боку уповноважених національних органів посадовим особам надається офіційний дозвіл безпеки. Процес оформлення вимагає проведення загальних або спеціальних перевірок. Цей процес включає надання та оформлення допусків безпеки для персоналу, який працює із секретною інформацією. Дозвіл безпеки – це загальна класифікація, яка містить низку правил, що контролюють відповідний рівень, який є необхідним для перегляду певної секретної інформації, а також способи її зберігання, передачі та знищення.

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)[3]. З метою сприяння Раді ЄС та допоміжним органам (Комісія ЄС, Європейська служба зовнішніх дій (EEAS)) працювати в усіх сферах, які вимагають використання секретної інформації, «European Union classified information» (EUCI) була розроблена та схвалена комплексна система безпеки з метою захисту інформації з обмеженим доступом, яка встановлює основні принципи та мінімальні стандарти безпеки у сфері охорони класифікованої інформації з еквівалентним рівнем захисту на теренах ЄС. Стаття 2 Рішення Ради 2013/488/ЄС регламентує, що правила безпеки охоплюють декілька способів захисту цієї інформації, включаючи безпеку персоналу, фізичну безпеку, управління інформацією, промислову безпеку та способи обміну безпековою інформацією між ЄС та третіми державами й міжнародними організаціями.

---

[1] Agreement between the European Union and the United Kingdom of Great Britain and Northern Ireland concerning security procedures for exchanging and protecting classified information 30.04.2021 № 149. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L.2021.149.01.2540.01.ENG

[2] Agreement between Ukraine and the European Union on the security procedures for the exchange of classified information 13.06.2005 № 172. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A22005A0705%2801%29

[3] 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%3A32013D0488

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 Європейського Союзу або одній чи кільком державам-членам. На теренах ЄС секретна інформація класифікується на одному з таких рівнів:

- TRÈS SECRET UE/EU TOP SECRET (Цілком таємно): інформація та матеріали, несанкціоноване розголошення яких може завдати надзвичайно серйозної шкоди основним інтересам Європейського Союзу або однієї чи кількох держав-членів;
- SECRET UE/EU SECRET (Таємно): інформація та матеріали, несанкціоноване розголошення яких може завдати серйозної шкоди основним інтересам Європейського Союзу або однієї чи кількох держав-членів;
- CONFIDENTIEL UE/EU CONFIDENTIAL (Конфіденційно): інформація та матеріали, несанкціоноване розголошення яких може завдати шкоди основним інтересам Європейського Союзу або однієї чи кількох держав-членів;
- RESTREINT UE/EU RESTRICTED (Обмежено): інформація та матеріали, несанкціоноване розголошення яких може бути невигідним для інтересів Європейського Союзу або однієї чи кількох держав-членів.

На рівні законодавства ЄС встановлені стандартизовані скорочені позначки (абревіатури) класифікації секретної інформації, які можуть використовуватися для позначення рівня секретності окремих параграфів тексту документа. Скорочення не повинні замінювати повне класифікаційне маркування, водночас допускається використання таких стандартів скорочення в секретних документах ЄС для позначення рівня секретності розділів або блоків тексту, що становлять менше однієї сторінки в такому форматі:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Під час створення секретного документа в ЄС дотримуються такі нормативні вимоги: кожна сторінка має бути чітко позначена рівнем секретності; кожна сторінка має бути пронумерована; документ повинен мати контрольний номер та дату; документи з рівнем секретності SECRET UE/EU SECRET або вище повинні мати номер копії на кожній сторінці, якщо вони розповсюджуються в кількох примірниках. Компетентні органи повинні гарантувати, що класифікована інформація належним чином засекречена, визначена як секретна інформація та зберігає свій рівень секретності лише до тих пір, поки це є необхідним.

Щодо секретної інформації в ЄС, забороняється понижувати її гриф або декласифікувати. Рада ЄС затверджує стандарти політики безпеки для створення класифікованої інформації. Згідно зі статтею 5 рішення Ради ЄС (2013/488/ЄС), Стаття 5 рішення Ради ЄС (2013/488/ЄС) встановлює, що заходи безпеки з метою захисту класифікованої інформації протягом усього життєвого циклу повинні відповідати, зокрема вимогам безпеки, формі та обсягу інформації чи матеріалу,

проводити оцінку розташування та конструкції критичних об'єктів, де зберігається класифікована інформація, враховувати виклики та ризики, пов'язані із посяганнями на секретну інформацію, загрозами ймовірної або вірогідної зловмисної або злочинної діяльності, зокрема шпигунства, диверсії або проявів тероризму. У зв'язку з цим розробляються плани дій на випадок кризових ситуацій, які повинні враховувати необхідність посиленого захисту класифікованої інформації під час надзвичайних ситуацій, щоб запобігти несанкціонованому доступу, розголошенню або втраті цілісності чи доступності секретних документів.

Стаття 13 зазначеного рішення Ради ЄС регулює порядок обміну секретною інформацією з третіми державами та міжнародними організаціями. Зокрема, якщо Рада ЄС визначає, що існує потреба в обміні класифікованою інформацією із третьою державою або міжнародною організацією, для цього визначається відповідна уповноважена структура та укладаються відповідні угоди з третіми державами або міжнародними організаціями щодо процедур безпеки для обміну та захисту секретної інформації (угоди про безпеку інформації). Угоди про безпеку інформації повинні містити положення, які гарантують, що коли треті держави або міжнародні організації отримують класифіковану інформацію, то такій інформації надається захист відповідно до її рівня секретності та згідно з мінімальними стандартами безпеки секретної інформації. Рішення про передачу класифікованої інформації третій державі або міжнародній організації приймається Радою ЄС в кожному конкретному випадку відповідно до характеру та змісту такої інформації, наявних потреб одержувача. Секретна інформація ЄС, що передається з території Європейського Союзу на територію третьої держави, повинна бути упакована таким чином, щоб вона була максимально захищена від несанкціонованого розголошення. Передача інформації з класифікацією «CONFIDENTIEL UE/EU CONFIDENTIAL» і «SECRET UE/EU SECRET» з території Європейського Союзу на територію третьої держави здійснюється одним із таких засобів:

1) військовим або дипломатичним кур'єром;

2) за допомогою нарочного перевезення за умови, що:

- пакет має офіційну печатку або упакований таким чином, щоб зазначити, що він є офіційним вантажем і не підлягає митному контролю чи контролю безпеки;

- фізичні особи мають сертифікат кур'єра, що ідентифікує пакунок і дозволяє їм його перевозити;

- секретний документ не виходить з володіння розпорядника;

- секретний документ не відкривається під час транспортування та не оприлюднюється в громадських місцях;

- уповноважені особи проінструктовані щодо їхніх обов'язків у сфері забезпечення безпеки класифікованої інформації.

Секретні документи ЄС, у яких відпала необхідність, можуть бути знищені за умов виконання відповідних правил і нормативних вимог щодо їхнього архівування.

Для документів з грифом «SECRET UE/EU SECRET» або «TRÈS SECRET UE/EU TOP SECRET» знищення здійснюється у присутності свідка, який має бути допущений до рівня секретності не нижче рівня знищуваного документа. Реєстратор і свідок, якщо присутність останнього є обов'язковою, підписують акт про знищення, який підшивається до реєстру. Реєстр зберігає сертифікати про знищення документів «TRÈS SECRET UE/EU TOP SECRET» протягом щонайменше 10 років

та документів «CONFIDENTIEL UE/EU CONFIDENTIAL» і «SECRET UE/EU SECRET» протягом щонайменше 5 років. Секретні документи, включно із секретними документами «RESTREINT UE/EU RESTRICTED», повинні бути знищені методами, які відповідають відповідним стандартам ЄС або еквівалентним стандартам, або які були схвалені державами-членами відповідно до національних технічних стандартів, щоб запобігти повній чи частковій їхній реконструкції. У разі надзвичайної або форс-мажорної ситуації, якщо існує безпосередній ризик несанкціонованого розкриття, власник класифікованої інформації повинен знищити її таким чином, щоб неможливо було її відновити.

Важливим аспектом визначено управління секретною інформацією – це застосування адміністративних заходів задля контролю за класифікованою інформацією протягом усього життєвого циклу з метою організації допомоги та сприяння запобіганню випадкам навмисного чи випадкового порушення цілісності або втрати такої інформації. Такі заходи стосуються, зокрема, створення, реєстрації, копіювання, перекладу, зниження рівня секретності документів (класифікованої інформації).

На виконання нормативних вимог ЄС створюється та функціонує реєстр секретної інформації, грифованої цілком таємно «TRÈS SECRET UE/EU TOP SECRET». Секретні документи, які мають гриф «TRÈS SECRET UE/EU TOP SECRET» категорично не можна копіювати або перекладати без попередньої письмової згоди автора. Заходи безпеки, що застосовуються до оригіналу документа, аналогічно застосовуються до його копій та перекладів. Секретна інформація ЄС повинна бути закрита, щоб запобігти сторонньому спостереженню за її вмістом. Секретна інформація під грифом «TRÈS SECRET UE/EU TOP SECRET» перевозиться виключно в захищеному конверті, на якому зазначено лише ім’я адресата.

З метою здійснення унормування та оптимізації європейських стандартів у сфері охорони державної таємниці на рівні ЄС було схвалено рішення Ради ЄС «Про внесення змін та доповнень до рішення Ради ЄС «Про правила безпеки для захисту секретної інформації» від 23 вересня 2013 року (2013/488/ЄС) «Про правила безпеки та захисту секретної інформації» від 21 червня 2021 року (2021/1075/ЄС)[4]. Цим актом здійснено прив’язку національних стандартів країн ЄС у сфері охорони державної таємниці відповідно до загальновстановлених європейських нормативів (EQUIVALENCE OF SECURITY CLASSIFICATIONS).

Табл. 1

Еквівалентність національних стандартів секретної інформації деяких країн ЄС відповідно до загальноєвропейських[5]

Назва країни	**Цілком таємно TRÈS SECRET UE/EU TOP**	**Таємно SECRET UE/EU SECRET**	**Конфіденційно CONFIDENTIEL UE/EU CONFIDENTIAL**	**Для службового користування RESTREINT UE/EU RESTRICTED**

[4] 2021/1075/EU: Council Decision of 21 June 2021 amending Decision 2013/488/EU on the security rules for protecting EU classified information. URL: https://eur-lex.europa.eu/eli/dec/2021/1075/oj

[5] Еквівалентність національних стандартів секретної інформації країн світу наведено у Додатку 1.

	SECRET			
Чехія	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Німеччина	STRENG GEHEIM	GEHEIM	VS – VERTRAULICH	_____
Естонія	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Франція	TRÈS SECRET TRÈS SECRET DÉFENSE	SECRET SECRET DÉFENSE	CONFIDENTIEL DÉFENSE	_____
Хорватія	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Польща	Ściśle Tajne	Tajne	Poufne	Zastrzeżone

У рамках унормування стандартів у сфері охорони державної таємниці, посилення захисту секретної інформації між Європейським Союзом та НАТО була укладена угода між ЄС та Організацією Північноатлантичного договору про безпеку інформації[6]. Ця угода складається із 18 статей та застосовується до секретної інформації, відомостей чи матеріалів у будь-якій формі (друкованій або електронній), які надаються або якими обмінюються сторони. Відповідно до статті 2 визначено, що секретна інформація визначається як будь-яка інформація (а саме, знання, які можуть бути передані в будь-якій формі) або матеріали, які потребують захисту від несанкціонованого розголошення та які мають позначку маркування «секретний».

Сторони взяли на себе зобов'язання щодо захисту та охорони секретної інформації, відомостей або матеріалів, що підпадають під дію цієї угоди й були надані або обмінювані іншою стороною; забезпечення умов для збереження рівня секретності, наданого інформації, відомостям або матеріалам стороною, яка їх надала або обміняла; використання такої інформації, відомостей чи матеріалів тільки в межах, визначених угодою, і недопущення їх використання для інших цілей; дотримання еквівалентного рівня секретності, встановленого на рівні ЄС; та заборони розголошення секретної інформації, відомостей чи матеріалів третім сторонам, будь-яким установам або організаціям ЄС, а також третім державам.

У рамках домовленостей сторони забезпечують розробку процедур перевірки секретності таким чином, щоб визначити, чи може особа, з урахуванням її лояльності, довіри та надійності, мати доступ до секретної інформації, відповідних відомостей чи матеріалів.

Досвід та стандарти НАТО. Кожна держава-член Альянсу бере на себе зобов'язання, зокрема у сфері охорони державної таємниці, що в термінології Альянсу позначається як «класифікована інформація». Охорона державної таємниці в НАТО, а також побудова й акредитація з безпеки інформаційно-комунікаційних

[6] Agreement between the European Union and the North Atlantic Treaty Organisation on the Security of Information 27.03.2003. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22003A0327%2801%29

систем, призначених для оброблення (передачі) інформації НАТО з обмеженим доступом, регулюються такими нормативними документами:

- AC/35-D/2004-REV3. Primary Directive on CIS Security. NATO Unclassified;
- AC/35-D/2005-REV3. Management Directive on CIS Security. NATO Unclassified;
- C-M(2007)0118. The NATO Information Management Policy. NATO Unclassified;
- AC/35-D/2002-REV5. Directive on the Security of NATO Classified Information. NATO Unclassified;
- C-M(2002)49-REV1. Security Within the North Atlantic Treaty Organization (NATO). NATO Unclassified;
- AC/35-D/2000-REV8. Directive on Personel Security. NATO Unclassified;
- AC/35-D/2001-REV3. Directive on Physical Security. NATO Unclassified;
- AC/35-N(2015)0022 (CISS). Rules of Engagement for Security Audits of NATO CIS. NATO Unclassified;
- AC/322-D(2021)0032. Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems. NATO Unclassified;
- AC/322-D(2019)0032-REV1 (INV). NATO Cloud Computing Directive. NATO Unclassified;
- C-M(2015)0041-REV1. NATO Cloud Computing Policy. NATO Unclassified;
- AC/322-D(2019)0041 (INV). Technical and Implementation Directive on Introducing Secure Systems and Solutions Using Commercial Off the Shelf (COTS) Products into NATO. NATO Unclassified;
- AC/322-D/0048-REV3 (INV). Technical and Implementation Directive on CIS Security. NATO Unclassified;
- AC/322-N(2014)0072. NATO Cyber Defence Taxonomy and Definitions. NATO Unclassified.

Водночас профілюючим актом законодавства Альянсу є норматив НАТО CM(2002)49[7]. Цей акт встановлює 5 основних принципів політики безпеки НАТО:

1) принцип «широти» – декларує, що держави-члени НАТО беруть на себе зобов'язання регулювати доступ до усіх видів «чутливої» інформації однаковим способом, незалежно від того, чи належить вона до діяльності НАТО. Така вимога гарантує, що кожна держава-член НАТО забезпечує високі стандарти захисту класифікованої інформації;

2) принцип «глибини» – базується на тому, що існують рівні та грифи поділу інформації з обмеженим доступом;

При цьому профільним актом законодавства Альянсу є норматив НАТО CM(2002)49.

3) принцип «централізації» – означає, що національні стандарти кожної держави-члена НАТО мають узгоджуватися зі стандартами Альянсу. Також на національному рівні кожна держава-член повинна мати державний уповноважений орган, який опікується питаннями охорони державної таємниці в контексті забезпечення національної безпеки. Центральним органом на теренах НАТО є Офіс безпеки НАТО (NOS)[8], який несе відповідальність за повну міждержавну

[7] NATO CM(2002)49. URL: https://www.freedominfo.org/documents/C-M(2002)49.pdf
[8] NATO Office of Security (NOS). URL: https://nato-intl.com/structure

координацію з питань інформаційної безпеки НАТО, проводить моніторинг національних систем з метою гарантування ефективного захисту інформації з обмеженим доступом. Офіс безпеки НАТО координує, контролює та реалізує політику безпеки НАТО, є компетентним органом НАТО для співпраці у сфері обміну та захисту секретної інформації між державами-членами Альянсу;

4) принцип «управління доступом» – ґрунтується на таких засадах: особи повинні мати доступ до інформації з обмеженим доступом тільки за наявності потреби в цій інформації для виконання своїх прямих обов'язків; інформація не може бути занижена у рівні таємності або розсекречена без згоди сторони, від якої вона була отримана;

5) принцип «персонального контролю» – передбачає встановлення правил вибору кандидатів щодо надання доступу до класифікованої інформації, водночас контроль базується на перевірці благонадійності, оцінках характеру та способу життя кандидатів на отримання допуску й доступу до класифікованої інформації.

Відповідно до цього документа в НАТО існує 4 рівні секретності: Космічно секретно (Cosmic Top Secret), Секретно (NATO Secret), Конфіденційно (NATO Confidential) та Обмежено (NATO Restricted). Класифікована інформація НАТО – це інформація, яка була створена Альянсом для нього, чи національна інформація країни-члена, яка була передана в систему безпеки НАТО. Захист цієї інформації контролюється згідно з правилами та стандартами безпеки НАТО, а доступ в межах НАТО визначається власником, якщо тільки автор не вказав обмеження у часі під час передачі відповідного документа до НАТО.

COSMIC TOP SECRET (CTS) – цей рівень секретності застосовується до інформації, несанкціоноване розголошення якої завдало б надзвичайно серйозної шкоди НАТО. Згідно з законодавством НАТО маркування «COSMIC» наноситься на матеріали «ЦІЛКОМ ТАЄМНО», щоб позначити, що вони є власністю НАТО, при цьому термін НАТО «ЦІЛКОМ ТАЄМНО» взагалі не використовується.

NATO SECRET (NS) – застосовується до інформації, несанкціоноване розголошення якої може завдати серйозної шкоди інтересам НАТО.

NATO CONFIDENTIAL (NC) — застосовується до інформації, несанкціоноване розголошення якої може завдати певної шкоди інтересам НАТО;

NATO RESTRICTED (NR) – застосовується до інформації, несанкціоноване розголошення якої було б невигідним для інтересів НАТО. Попри те, що заходи безпеки для цієї категорії матеріалів подібні до інформації «ЛИШЕ ДЛЯ ОФІЦІЙНОГО КОРИСТУВАННЯ», цей стандарт є засекреченим і повинен надсилатися виключно за допомогою секретних засобів.

З метою оперативного обміну секретною інформацією кожна держава-член НАТО є учасником Центрального реєстру забезпечення належного контролю та підзвітності секретних документів НАТО, який розташований у місті Арлінгтон, штат Вірджинія (США)[9]. Кожен секретний документ має містити відповідне маркування, яке є основним способом інформування власників інформації про особливі вимоги щодо її захисту.

У системі НАТО маркування, позначення або електронне маркування здійснюються для інформування власників про наявність секретної або

[9]The Central United States Registry (CUSR). URL: https://www.information.marines.mil/Portals/224/Docs/Newcomers/NATO-Security-Briefing.pdf

контрольованої несекретної інформації. Вони допомагають точно визначити, яка інформація потребує відповідного рівня захисту, а також надають дані про джерела й підстави для її класифікації. Окрім цього, маркування дозволяє ідентифікувати орган чи установу, що є джерелом інформації, а також автора документа, з обов'язковим зазначенням рівня секретності. Оригінальна класифікація – це первинне рішення, прийняте відповідним органом, що інформація потребує захисту від несанкціонованого розголошення в інтересах національної безпеки. Стандартні позначки є обов'язковими для всіх документів, що містять первинну секретну інформацію. До обов'язкових елементів маркування належать: банерні лінії, позначки порцій, найменування агентства, офіс походження, дата створення та блок класифікаційного органу.

Згідно з вимогами НАТО щодо розсекречення та зниження рівня секретності, секретна інформація Альянсу не підлягає зниженню або розсекреченню без попередньої згоди керівництва НАТО. Доступ до секретної інформації НАТО може бути наданий лише відповідно до встановлених нормативних вимог НАТО. Посадовій особі, яка отримала допуск до секретної інформації, видається так званий «сертифікат НАТО»; ця особа не пізніше як перед першим доступом до секретної інформації певного рівня має пройти інструктаж щодо знань своїх обов'язків при поводженні із секретною інформацією та норм законодавства НАТО в даній сфері. Документальне супроводження інструктажу передбачає підпис особою, яка його виконала (як правило, відповідальною особою або уповноваженою нею особою) та фізичною особою, яка була проінструктована. З метою встановлення нормативних вимог щодо обміну класифікованою інформацією були схвалені керівництвом НАТО STANAG 4774 та STANAG 4778. STANAG 4774 описує та деталізує синтаксис метаданих, необхідний для поміток конфіденційної інформації з метою полегшення та захисту обміну класифікованою інформацією між державами-членами Альянсу. STANAG 4778 визначає порядок як мітка конфіденційності прив'язується до даних протягом усього життєвого циклу та діє між сторонами, які надають спільний доступ. Він також описує криптографічні методи для забезпечення цілісності даних і позначень. Вимоги до маркування класифікованої інформації включають дані щодо власника інформації, стандартизації інформації, визначення рівня секретності. Держави-члени Альянсу повинні використовувати інструменти, які можуть застосовувати необхідні метадані та візуальні позначки, а також керувати доступом до конфіденційної інформації в рамках дотримання вимог STANAG 4774 та STANAG 4778.

Таким чином, НАТО створила надійну структуру сумісності для класифікації та доступу, яку держави-члени та партнерські організації повинні запровадити у своїх власних системах. Застосування технології для автоматичного застосування й забезпечення виконання класифікації інформації, візуального маркування та доступу до даних забезпечує належне застосування цих засобів контролю, і лише авторизовані сторони отримують доступ до класифікованої інформації Альянсу. Технологію класифікації та захисту даних використовують не лише для міжнародної співпраці між державами-членами НАТО та ЄС, а також як інструмент для вдосконалення національних систем за допомогою відповідного маркування та засобів контролю, що сприяє побудові більш стійкої системи класифікованої інформації, цілісному запобіганню навмисній і ненавмисній втраті даних,

розголошенню конфіденційної інформації, що може бути спричинено як навмисно, так і випадково, допомагає запобігти зламу та отриманню несанкціонованого доступу до конфіденційної критично важливої класифікованої інформації.

Великобританія. У цій країні відповідно до державної політики засекречування інформації (далі – Політика засекречування)[10] існує трирівнева система секретності (з 2014 року, Рисунок 1):

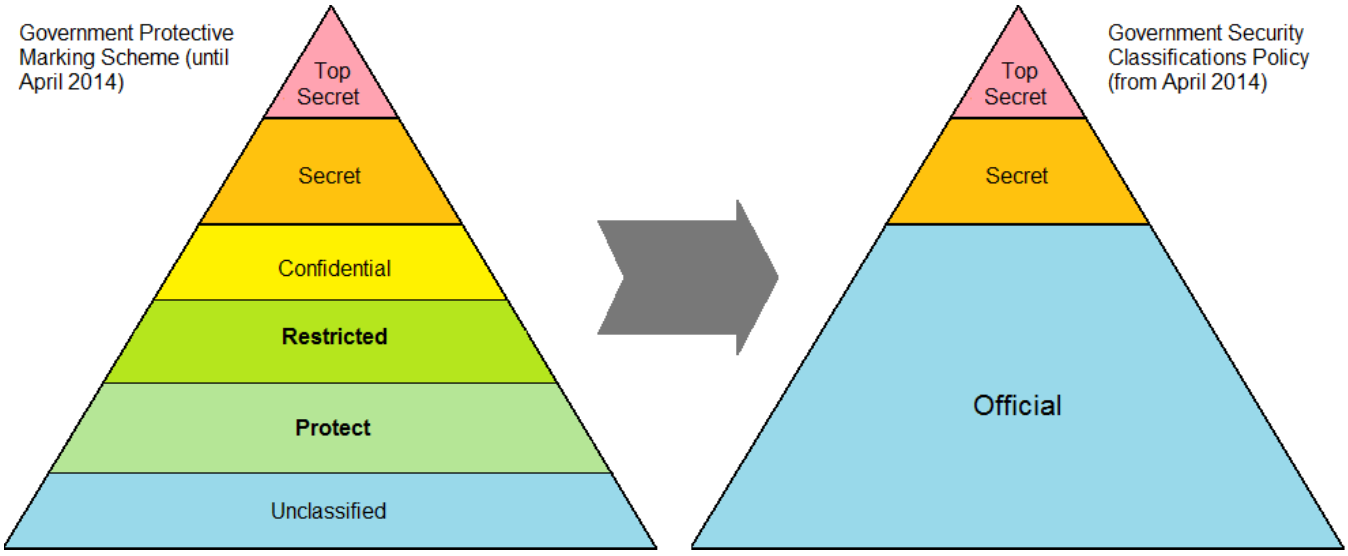
1) *«офіційна» (official)* – інформація, несанкціоноване розголошення якої може завдати незначної шкоди фізичним та юридичним особам, міжнародним відносинам, національній економіці, обороні та безпеці. До такої інформації належать: публічні повідомлення, опублікована інформація в мережі Інтернет, навчальні матеріали, документи, що не містять персональних даних та інші. У межах ступеня секретності «офіційно» також виділяють інформацію під грифом секретності *«з обмеженим доступом» (official-sensitive)*, що вимагає більш суворих протоколів поводження з нею і додаткових заходів безпеки. До неї, зокрема, належать документи, що містять персональні дані (наприклад, особові справи), загальні адміністративні документи, не призначені для опублікування, комерційні документи тощо.

2) *«таємно» (secret)* – інформація, яка потребує посилених заходів захисту, несанкціоноване розголошення якої може завдати істотної шкоди фізичним і юридичним особам, міжнародним відносинам, національній економіці, обороні та безпеці; спричинити загрозу життю, свободі або безпеці особи; зумовити погіршення ефективності держави щодо реагування на надзвичайні ситуації, протидії тероризму, шпигунству чи іншій діяльності, що підриває національну безпеку Великобританії.

3) *«цілком таємно» (top secret)* – інформація, що вимагає надзвичайно високого рівня захисту, несанкціоноване розголошення якої є вкрай небезпечним для фізичних і юридичних осіб, міжнародних відносин, національної економіки, оборони та безпеки; може спричинити значні людські втрати; зумовити тяжку шкоду ефективності реагування на надзвичайні ситуації та діяльності держави щодо боротьби з тероризмом, шпигунством або іншими діями, що підривають національну безпеку Великобританії.

[10]Government Security Classifications Policy (HTML). URL: https://www.gov.uk/government/publications/government-security-classifications/government-security-classifications-policy-html

Рис. 1[11]



Положення про державні контракти у сфері оборони та безпеки 2011 року[12] визначає секретну інформацію як будь-які відомості або матеріал, незалежно від форми, характеру або способу їх передачі, яким присвоєно гриф секретності, що в інтересах національної безпеки та згідно положень законодавства вимагає захисту від привласнення, знищення, вилучення, розкриття, втрати або несанкціонованого доступу чи будь-якого іншого виду компрометації. Уряд забезпечує організацію системи захисту секретної інформації, що впроваджена на всіх рівнях влади, об'єктах критичної інфраструктури, а також приватних підприємствах, установах і організаціях, які надають послуги державному сектору[13].

Координацію державної політики щодо питання захисту секретної інформації у Великобританії здійснює Рада національної безпеки[14], яку очолює Прем'єр-міністр. Забезпечення захисту і охорони державної таємниці у сфері національної безпеки здійснюється Управлінням військової розвідки[15] та Лабораторією оборонної науки і техніки[16]. Обидві установи підпорядковані Міністерству оборони Великобританії.

Засекречування матеріальних носіїв секретної інформації (далі – МНСІ) здійснюється шляхом нанесення на них видимого грифу секретності таким чином:

1) гриф секретності наноситься великими літерами по середині на верхню та нижню частини документа;

2) у випадку якщо секретна інформація надсилається через електронну пошту, на початку заголовку (теми) електронного листа необхідно великими літерами

---

[11] URL: https://statisticsofantarctica.com/api/

[12]The Defence and Security Public Contracts Regulations (DSPCR) 2011. URL: https://www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

[13]Controlling Classified Information in the UK Public Sector. URL: https://www.wired-gov.net/wg/images.nsf/images/DNWA-BVUP6X/$file/csw-controlling-classified-information-in-uk-public-sector-gd.pdf

[14]National Security Council. URL: https://www.gov.uk/government/groups/national-security-council

[15] Defence Intelligence. URL: https://www.gov.uk/guidance/defence-intelligence

[16] Defence Science and Technology Laboratory. URL: https://www.gov.uk/government/organisations/defence-science-and-technology-laboratory

вказати «З ОБМЕЖЕНИМ ДОСТУПОМ» (заборонено надсилати через електронну пошту секретну інформацію під грифом секретності «таємно» та «цілком таємно»);

3) гриф секретності наноситься великими літерами на титульну частину папки або швидкозшивача[17].

Важливо зауважити, що засекречування здійснюється виключно щодо інформації під грифом секретності «з обмеженим доступом», «таємно» та «цілком таємно». Гриф секретності інформації може надаватись відповідними посадовими особами чи органами строком до 100 років[18], проте у Великобританії не передбачено законодавчого закріплення максимального строку дії грифу секретності для засекреченої інформації[19].

Доступ до секретної інформації надається особам, які виконуватимуть посадові, службові або професійні обов'язки після проходження ними безпекової перевірки, що має такі рівні:

1) базовий стандарт кадрової безпеки (Baseline Personnel Security Standard) – для отримання доступу до секретної інформації, що має ступінь секретності «офіційна»/«з обмеженим доступом»;

2) базова перевірка (Security Check) – для отримання довготривалого, частого та неконтрольованого доступу до секретної інформації під грифом секретності «таємно» або періодичного і контрольованого доступу до інформації ступеня секретності «цілком таємно».

3) розширена перевірка (Developed Vetting) – для отримання частого і неконтрольованого доступу до секретної інформації під грифом секретності «цілком таємно».

Проходження безпекових перевірок передбачено для державних службовців, співробітників органів безпеки та розвідки, військовослужбовців збройних сил, співробітників поліції, неурядових організацій, які зобов'язані дотримуватися державних процедур безпеки та осіб, які надають товари й послуги органам державної влади. За умови успішного проходження базової та розширеної перевірок особа, яка оформлює допуск до секретної інформації (далі – заявник), отримує сертифікат допуску до секретної інформації (далі – сертифікат). Такий документ видається Службою з питань безпекових перевірок Великобританії[20]. Успішне проходження перевірки згідно з базовим стандартом кадрової безпеки не передбачає видачу сертифіката[21].

Базовий стандарт кадрової безпеки передбачає перевірку: 1) особистості; 2) освіти; 3) стажу роботи за останні 3 роки; 4) наявності непогашених судимостей; 5) наявності в особи права на працевлаштування у Великобританії[22]. Проходження такої перевірки займає від 1 до 2 днів. Результати перевірки не мають терміну дії,

---

[17]Government Classification Scheme. URL: https://security-guidance.service.justice.gov.uk/government-classification-scheme/#marking-of-information

[18]Controlling Classified Information in the UK Public Sector. URL: https://www.wired-gov.net/wg/images.nsf/images/DNWA-BVUP6X/$file/csw-controlling-classified-information-in-uk-public-sector-gd.pdf

[19]Classified Information. A review of current legislation across 15 countries & the EU. URL: https://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf

[20] United Kingdom Security Vetting. URL: https://www.gov.uk/government/organisations/united-kingdom-security-vetting

[21] Difference between BPSS and SC clearance. URL: https://bpsscost.s3.nl-ams.scw.cloud/difference-between-bpss-and-sc-clearance.html

[22] National Security Vetting Your Questions Answered. URL: https://www.parliament.uk/globalassets/mps-lords--offices/offices/pass-office/psd-national-security-vetting-booklet.pdf

окрім випадків якщо особа: 1) розпочинає роботу в іншій установі, підприємстві або організації, де проходження такої перевірки є необхідним; 2) повертається до виконання своїх посадових, службових або професійних обов'язків після 12-місячної перерви. Законом можуть бути встановлені інші випадки визначення закінчення строку дії результатів перевірки відповідно до базового стандарту кадрової безпеки[23].

Безпекова перевірка передбачає: 1) успішне проходження перевірки згідно з базовим стандартом кадрової безпеки; 2) заповнення заявником спеціальної анкети з питань безпеки; 3) перевірку особистої справи заявника, наявності погашених або непогашених судимостей, його кредитної та фінансової історії; 4) отримання інформації про заявника від Служби безпеки Великобританії на предмет причетності до дій, що спричиняють шкоду національній безпеці. Така перевірка триває 6 тижнів. Допуск до секретної інформації, отриманий на підставі її проходження, діє протягом десяти років.

Для отримання допуску до інформації ступеня секретності «цілком таємно» заявник проходить розширену перевірку, що триває 6 місяців та складається з таких етапів:

1) успішне проходження перевірки згідно з базовим стандартом кадрової безпеки;

2) заповнення особою спеціальної анкети з питань безпеки;

3) перевірка особистої справи заявника, наявності погашених або непогашених судимостей, його кредитної та фінансової історії;

4) отримання інформації про заявника від Служби безпеки Великобританії на предмет причетності до дій, що спричиняють шкоду національній безпеці;

5) перевірка матеріально-фінансового стану заявника;

6) проходження співбесіди заявником зі спеціально уповноваженою особою, що здійснює оцінку її відповідності критеріям безпеки, необхідним для отримання допуску до секретної інформації. Перегляд допуску до секретної інформації, що отриманий після проходження розширеної перевірки здійснюється через сім років з дати видачі відповідного сертифіката[24].

Перегляд грифів секретності МНСІ, розсекречування, а також передача секретної інформації до Національного архіву здійснюється виключно посадовими особами або органами, які надали відповідні грифи секретності. Фізичні та юридичні особи, зацікавлені в отриманні доступу до секретної інформації, подають запити про розсекречування згідно з Законом про свободу інформації 2000 року[25]. Передача секретної інформації до Національного архіву здійснюється згідно з Законом про державні документи 1958 року[26]. Перед передачею оригінальних

[23] UK Government Baseline Personnel Security Standard - Version 7.0 - June 2024. URL: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard/uk-government-baseline-personnel-security-standard-version-70-june-2024-html

[24] National security vetting: clearance levels. URL: https://www.gov.uk/government/publications/united-kingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels

[25] Freedom of Information Act 2000. URL: https://www.legislation.gov.uk/ukpga/2000/36/contents

[26] Public Records Act 1958. URL: https://www.legislation.gov.uk/ukpga/Eliz2/6-7/51

історичних документів до Національного архіву з них має бути вилучена чутлива інформація, яка перебуває під захистом[27].

Правовий захист і охорону державної таємниці у Великобританії забезпечено Законом про державну таємницю 1989 року (далі – Закон про державну таємницю)[28], який замінив раніше чинний закон, прийнятий ще в 1911 році. У новому законі більш чітко надані визначення відомостей, що становлять державну таємницю. Зокрема, Законом про державну таємницю передбачено, що розголошення секретної інформації:

1) у сфері національної безпеки чи розвідки співробітником (колишнім співробітником) служби безпеки;

2) у сфері оборони, вчинене державним службовцем або підрядником державної установи;

3) пов'язаної з міжнародними відносинами, а також конфіденційної інформації, отриманої від інших держав чи міжнародних організацій, вчинене державним службовцем або підрядником державної установи;

4) вчинене державним службовцем або підрядником державної установи, що може призвести до: - вчинення злочину; - втечі осіб, які перебувають під вартою; - перешкоджання запобіганню або виявленню правопорушень, а також затриманню чи переслідуванню підозрюваних у вчиненні злочинів;

5) особою, якій стала відома така інформація і така особа знає або у неї були достатні підстави вважати, що розголошена нею інформація захищена законом і що її розголошення завдасть шкоди національним інтересам держави;

6) пов'язаної з розвідкою, обороною або міжнародними відносинами та яка була конфіденційно передана урядом Великобританії іншій державі чи міжнародній організації, вчинене особою, що не мала дозволу на отримання такої інформації, і така особа знає або в неї були достатні підстави вважати, що розголошення нею інформації завдасть шкоди національним інтересам держави, – карається покаранням у вигляді позбавленням волі на строк до двох років та/або штрафом у необмеженому розмірі.

Також Законом про державну таємницю передбачено кримінальну відповідальність за недбале поводження із секретною інформацією, що сприяє її розголошенню, вчинене державним службовцем або підрядником державної установи, у вигляді позбавлення волі на строк до трьох місяців та/або штрафом у необмеженому розмірі.

Закон про національну безпеку 2023 року (далі – Закон про національну безпеку)[29] встановлює організаційно-правовий механізм, який забезпечує охорону захищеної інформації, тобто інформації до якої доступ обмежено з метою захисту безпеки та національних інтересів Великобританії, встановлюючи кримінальну відповідальність за шпигунство. Передбачено, що особа, яка отримує, копіює, записує або зберігає інформацію з обмеженим доступом, або розкриває чи надає доступ до такої інформації з метою її передачі іноземній державі, іноземній організації або їх представникам, і такі дії спрямовані на завдання шкоди безпеці

[27]Government Security Classifications Policy. URL: https://assets.publishing.service.gov.uk/media/649c38e006179b00113f745b/Government_Security_Classifications_Policy_June_2023.pdf

[28] Official Secrets Act 1989. URL: https://www.legislation.gov.uk/ukpga/1989/6/contents

[29] National Security Act 2023. URL: https://www.legislation.gov.uk/ukpga/2023/32/contents

або інтересам Великобританії, карається довічним позбавленням волі та/або штрафом у необмеженому розмірі.

Таким чином, у Великобританії захист секретної інформації здійснюється відповідно до Політики засекречування державної таємниці, згідно з якою за ступенем секретності інформація поділяється на «офіційну», «таємну» й «цілком таємну». У межах ступеня секретності «офіційно» виділяють інформацію під грифом секретності «з обмеженим доступом». Правовий захист і охорону державної таємниці у Великобританії забезпечено в рамках Законів про державну таємницю та про національну безпеку. Обов'язки із забезпечення організації системи захисту секретної інформації в Великобританії покладено на Уряд.

Нанесення грифів секретності на МНСІ є необхідним для інформації, що має ступені секретності «з обмеженим доступом», «таємно» або «цілком таємно». Державні службовці та інші особи, які уповноважені мати доступ до секретної інформації повинні пройти такі рівні перевірки:

1) базовий стандарт кадрової безпеки («офіційно»/«з обмеженим доступом»);

2) безпекова перевірка («таємно»/«цілком таємно»);

3) розширена перевірка («цілком таємно»). Рішення про перегляд грифів секретності МНСІ, розсекречування й передачі секретної інформації до Національного архіву приймається посадовими особами або органами, якими були надані відповідні грифи секретності.

У рамках налагодження взаємної охорони класифікованої інформації між ЄС та Великобританією було укладено Угоду про захист секретної інформації від 30 квітня 2021 року[30]. Це надасть можливість для спрощення процедур оперативного обміну інформацією з обмеженим доступом між сторонами.

Нарівні із законодавчим поняттям «класифікована інформація», активно використовується термін «захищена інформація». Окрім того, законодавчо встановлено, що строк надання грифу секретності інформації може становити до 100 років, проте граничний максимальний термін засекречування інформації з обмеженим доступом не визначений. Державна політика щодо питання захисту секретної інформації координується Радою національної безпеки, яку очолює Прем'єр-міністр, проте процедурні питання організації захисту та охорони державної таємниці у сфері національної безпеки здійснюються Управлінням військової розвідки та Лабораторією оборонної науки і техніки, які підпорядковані Міністерству оборони Великобританії.

Франція. Секретна інформація, яка підпадає під критерії законодавчо визначеної «таємниці національної оборони» (далі – державна таємниця) міститься у статті R2311-1 Кодексу про оборону[31], який визначає, що до неї належать відомості, матеріали, документи, інформаційні дані, комп'ютерні мережі, комп'ютеризовані дані або файли, що мають оборонне значення для національної безпеки. Особливістю французької моделі охорони державної таємниці є те, що за ступенем секретності така інформація поділялася на три рівні:

[30] Agreement between the European Union and the United Kingdom of Great Britain and Northern Ireland concerning security procedures for exchanging and protecting classified information. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.149.01.2540.01.ENG

[31] Code de la défense. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071307/2024-07-09/

1) конфіденційна оборонна (confidentiel défense) – інформація, розголошення якої може завдати шкоду національній обороні або призвести до розкриття інформації, віднесеної до вищого рівня безпеки;

2) таємна оборонна (secret défense) – інформація, розголошення якої може завдати істотної шкоди національній обороні, яка може бути поширена за умови надання дозволу уповноваженими органами влади; за виняткових ситуацій поширення такої інформації можливе без відповідного дозволу;

3) цілком таємна оборонна (très secret défense) – інформація, розголошення якої вважається вкрай небезпечним для національної оборони; зберігання, передача, відображення або знищення інформації цього рівня секретності здійснюється виключно за дозволом Прем'єр-міністра Франції або Секретаря національної оборони.

У рамках реформування, на підставі указу Прем'єр-міністра Франції від 13 листопада 2020 року (далі – Указ)[32] було введено в дію дворівневу систему секретності з наданням грифу «таємно» (secret) та «цілком таємно» (très secret). Одночасно було затверджено Загальну міжвідомчу інструкцію про охорону таємниці національної оборони № 1300 (далі – Інструкція № 1300)[33].

Згідно зі статтею R2311-2 Кодексу про оборону таємною визнається інформація, розголошення якої може завдати суттєвої шкоди національній обороні та безпеці; цілком таємною – інформація, розголошення якої може мати вкрай серйозні наслідки для національної оборони та безпеки. Згідно з Указом ступінь секретності «конфіденційна оборонна» відповідає ступеню «таємно», ступені «таємна оборонна» і «цілком таємна оборонна» – ступеню «цілком таємно».

Важливо зазначити, що гриф секретності, який був наданий у період до набуття чинності цих змін (до 01 липня 2021 р.) залишається чинним[34]. У зв'язку з цим у Рішенні Ради (ЄС) 2021/1075 від 21 червня 2021 року «Про внесення змін до Рішення 2013/488/ЄС про правила безпеки для захисту інформації ЄС що не підлягає розголошенню»[35] зазначено обидві системи засекречування – трирівнева та дворівнева. Реформа національного стандарту ступенів секретності у 2021 році мала такі завдання:

- деталізація переліку секретної інформації, що підлягає захисту як державна таємниця;
- спрощення обміну секретною інформацією з іншими країнами, міжнародними організаціями, а також приватним сектором;
- деталізація процедур поводження з дематеріалізованою секретною інформацією (правила поводження з IT-інструментами тощо);
- посилення контролю за обігом секретної інформації шляхом введення під егідою Генерального секретаріату національної оборони та безпеки[36]

[32] Arrêté du 13 novembre 2020 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale. URL: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042520705

[33] Instruction générale interministérielle sur la protection du secret de la défense nationale. URL: https://www.sgdsn.gouv.fr/files/files/Nos_missions/igi-1300-20210809%20(1).pdf

[34] Protéger le secret de la défense nationale. URL: https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-secret-de-la-defense-nationale

[35] Council Decision (EU) 2021/1075 of 21 June 2021 amending Decision 2013/488/EU on the security rules for protecting EU classified information. URL: https://eur-lex.europa.eu/eli/dec/2021/1075/oj#ntr5-L_2021233EN.01000302-E0005

[36] Secrétariat général de la défense et de la sécurité nationale. URL: https://www.sgdsn.gouv.fr/

обов'язкової щорічної інвентаризації матеріальних носіїв секретної інформації (далі – МНСІ) незалежно від ступеня їх секретності;

- посилення заходів із захисту секретної інформації на загальнодержавному рівні (моніторинг діяльності уповноважених осіб у сфері захисту секретної інформації, охорона приміщень тощо);
- роз'яснення порядку та умов доступу юридичних осіб до секретної інформації[37];
- узгодження підходів до захисту секретної інформації з іншими країнами-членами НАТО та ЄС[38].

Порядок і заходи у сфері охорони державної таємниці, що застосовуються на кожному етапі її життєвого циклу (виробництво, відтворення, маршрутизація, знищення тощо), визначені вищевказаною інструкцією й залежать від ступеня секретності класифікованої інформації. Спеціальним органом, відповідальним за управління політикою захисту державної таємниці на загальнодержавному рівні є Департамент з питань захисту таємниці національної оборони (далі також – Департамент)[39], підпорядкований Управлінню державної охорони та безпеки, що перебуває в структурі Генерального секретаріату національної оборони та безпеки.

Координація державної політики в питаннях забезпечення охорони класифікованої інформації здійснюється Генеральним секретаріатом національної оборони та безпеки, що є міжвідомчим органом, який керується Секретарем національної оборони та реалізує функцію контролю у сфері захисту секретної інформації (стаття R1132-3 Кодексу про оборону). Генеральний секретаріат підпорядкований Прем'єр-міністру Франції. У межах компетенції та відповідно до функціональності вказаний Департамент:

- надає консультації органам влади щодо питань захисту державної таємниці;
- розробляє стандарти захисту державної таємниці на національному й міжнародному рівнях;
- здійснює моніторинг і контроль за їх застосуванням;
- проводить для міністерств та відомств технічну експертизу у сфері захисту державної таємниці;
- представляє Генеральний секретаріат в ЄС, НАТО та Європейському космічному агентстві[40].

Система захисту державної таємниці у Франції організована таким чином[41]:

[37] Réforme de la protection du secret de la défense nationale. URL: https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-secret-de-la-defense-nationale/reforme-de-la-protection-du-secret

[38] Les mentions «Confidentiel Défense» et «Secret Défense» seront bientôt remplacées. URL: https://www.opex360.com/2020/11/16/les-mentions-confidentiel-defense-et-secret-defense-seront-bientot-remplacees/

[39] Sous-direction de la protection et de la sécurité de défense nationale. URL: https://lannuaire.service-public.fr/gouvernement/5f04919e-04e5-4ced-91ba-b6a7f29a3b4a

[40] Avis de vacance d'un emploi de sous-directeur. URL: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047936834

[41] IGI n° 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale. URL: https://cyber.gouv.fr/instruction-generale-interministerielle-n1300

Система захисту державної таємниці у Франції

Засекречування МНСІ здійснюється шляхом нанесення на нього видимого грифа секретності. Перед наданням грифа секретності відповідна посадова особа проводить аналіз важливості інформації, беручи до уваги контекст її використання й застосовну до неї класифікацію.

До реквізитів МНСІ належать:

1) *гриф секретності*, що вказує ступінь секретності інформації і проставляється червоним чорнилом або, як виняток, кольором, який контрастує з МНСІ, посередині верхньої й нижньої частини кожної сторінки. Інформація, що має бути розкрита виключно громадянам Франції, засвідчується спеціальним штампом синього кольору, що проставляється у верхній частині кожної сторінки праворуч або під грифом секретності;

2) *термін засекречування інформації*;

3) *дані про орган і посадову особу, що надають гриф секретності*;

4) *нумерація сторінок документа:* кожний аркуш документа повинен бути пронумерованим; для документів зі ступенем секретності «цілком таємно» чисті та розділові аркуші також нумеруються. Посередині порожніх аркушів зазначено «Без тексту».

Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, визначений Кодексом про спадщину[42] та становить 50 років.

Сертифікат про допуск до державної таємниці надається виключно особам, яким необхідна така секретна інформація для виконання посадових або службових обов'язків. Особа, яка оформлює допуск до державної таємниці (далі – заявник), заповнює відповідну форму (далі також – звернення про отримання сертифіката), яку подає до співробітника служби безпеки установи, підприємства або організації. Співробітник служби безпеки перевіряє повноту і правильність заповнення форми та у разі відсутності зауважень надсилає її до Генерального секретаріату національної оборони та безпеки або Міністерства до відання якого належать відповідна установа, підприємство або організація (далі – дозвільний орган)[43]. Відповідний дозвільний орган здійснює перевірку отриманої заповненої форми та надає її для розгляду таким уповноваженим органам:

1) Управлінню розвідки та безпеки Міністерства оборони[44] – для цивільного або військового персоналу Міністерства оборони, а також установ, що належать до його відання; військового персоналу жандармерії;

2) Генеральному управлінню зовнішньої безпеки Міністерства оборони[45] – для персоналу цього управління, а також установ, що забезпечують його діяльність;

3) Головне управління внутрішньої безпеки Міністерства внутрішніх справ[46] – для підприємств, установ і організацій, які здійснюють свою діяльність у цивільній сфері (зокрема цивільний персонал жандармерії).

Для надання допуску до державної таємниці під грифом секретності «таємно» розгляд звернення про отримання сертифіката триває три місяці та шість місяців

[42] Code du patrimoine. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006074236/

[43] Fiches pratiques à destination des personnes habilitées. URL: https://www.sgdsn.gouv.fr/files/files/Nos_missions/fiches-pratiques-psdn-personnes-habilitees-num-v20211001.pdf

[44] Direction du renseignement et de la sécurité de la défense. URL: https://www.drsd.defense.gouv.fr/

[45] Direction générale de la sécurité extérieure. URL: https://www.dgse.gouv.fr/fr

[46] Direction générale de la sécurité intérieure. URL: https://www.interieur.gouv.fr/ministere/direction-generale-de-securite-interieure

щодо надання допуску до державної таємниці зі ступенем секретності «цілком таємно». Рішення про надання сертифіката ґрунтується на критеріях, які дають змогу визначити чи така особа становить загрозу державній таємниці або зазнає шантажу чи тиску, що може завдати шкоди інтересам держави. За результатами розгляду звернення відповідне управління видає висновок, що направляється дозвільному органу. Такі висновки є трьох видів:

1) позитивний висновок, що рекомендує надати допуск заявнику до державної таємниці (під час розгляду звернення й перевірки особи не виявлено жодної загрози для безпеки державної таємниці);

2) обмежувальний висновок, що вказує на наявність прямих і непрямих ризиків, пов'язаних з наданням заявнику допуску до державної таємниці; такий висновок може містити рекомендацію щодо надання лише певної частини інформації, що запитується;

3) негативний висновок, який визначає, що надання заявнику допуску становитиме загрозу для державної таємниці й не рекомендує надання такого допуску.

Дозвільний орган приймає рішення про надання допуску до державної таємниці або відмову в такому наданні незалежно від змісту рекомендацій, зазначених у висновку. Строк дії сертифіката допуску складає для ступенів секретності: 1) «таємно» – до семи років; 2) «цілком таємно» – до п'яти років. Для попередніх ступенів секретності сертифікат діє: 1) до п'яти років – для ступеня секретності «цілком таємна оборонна»; 2) до семи років – «таємна оборонна»; до десяти років – «конфіденційна оборонна»[47].

Розсекречування державної таємниці здійснюється автоматично, без необхідності прийняття офіційного рішення (нанесення грифа) про розсекречування за умови закінчення 50-річного строку. Відповідно до статті R2311-4 Кодексу про оборону питання щодо зміни рівня засекречування або розсекречування секретної інформації вирішується органом, яким було здійснено засекречування.

Під час проведення інвентаризації секретних документів орган або посадова особа, якими було надано гриф секретності, здійснюють перегляд ступеня секретності інформації і, якщо можливо, приймають рішення про її розсекречування або зниження ступеня секретності. З метою такого перегляду Міжміністерський комітет з архівів Франції (далі – Комітет), за пропозицією архівних адміністрацій, визначає перелік часто запитуваних або таких, які становлять історичний чи науковий інтерес документів. Комітет звертається до органів, якими було надано гриф секретності, щодо розв'язання питання доцільності збереження режиму секретності для відповідних документів, за результатами якого органи приймають рішення про розсекречування або відмову у розсекречуванні інформації. Під час кожного засідання Комітету готується звіт про хід розсекречування документів.

У Франції інформація, що не підлягає засекреченню, але є особливо чутливою, класифікується як інформація з обмеженим доступом (Diffusion Restreinte). Зокрема, розкриття такої інформації може завдати шкоди: 1) таємниці засідань Уряду та уповноважених органів виконавчої влади; 2) зовнішній політиці Франції; 3) державній, громадській або особистій безпеці особи; безпеці інформаційних

[47] Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale. URL: https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000033293465

систем органів державної влади; 4) національній валюті та державному кредиту; 5) розпочатим судовим провадженням; 6) розслідуванню та запобіганню правопорушень. Розкриття інформації з обмеженим доступом фізичним або юридичним особам, які не мають необхідності в отриманні доступу до такої інформації, може тягнути за собою дисциплінарну, адміністративну та, в деяких випадках, кримінальну відповідальність, зокрема, у разі порушення професійної таємниці.

Таким чином, у Франції до державної таємниці належить секретна інформація, яка підпадає під критерії законодавчо визначеної «таємниці національної оборони». До такої таємниці належать відомості, матеріали, документи, інформаційні дані, комп'ютерні мережі, комп'ютеризовані дані або файли, що мають оборонне значення для національної безпеки. З 01 липня 2021 року у Франції застосовується дворівнева система секретності інформації – «таємно» та «цілком таємно». Проте гриф секретності наданий до 01 липня 2021 року залишається чинним: ступінь секретності «конфіденційна оборонна» відповідає ступеню «таємно», ступені «таємна оборонна» і «надзвичайно таємна оборонна» – ступеню «цілком таємно». Координуючим органом у сфері забезпечення захисту державної таємниці є Генеральний секретаріат національної оборони та безпеки. Спеціальним органом, відповідальним за управління політикою захисту державної таємниці на рівні міністерств є Департамент з питань захисту таємниці національної оборони, який розробляє стандарти захисту секретної інформації та здійснює моніторинг і контроль за їх застосуванням.

Інструкція № 1300 встановлює порядок і заходи захисту державної таємниці, що застосовуються на кожному етапі її життєвого циклу (виробництво, відтворення, маршрутизація, знищення тощо). Кримінальний кодекс Франції встановлює відповідальність за низку злочинних діянь, що посягають на захист такої таємниці.

Засекречування матеріальних носіїв секретної інформації (далі – МНСІ) здійснюється шляхом нанесення на них видимого грифа секретності. До реквізитів МНСІ належать: гриф секретності; термін засекречування інформації; дані про орган і посадову особу, що надають гриф секретності; нумерація сторінок документа. Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, становить 50 років. Допуск до державної таємниці надається виключно особам, яким потрібна така секретна інформація для виконання посадових або службових обов'язків, на підставі сертифіката, виданого Генеральним секретаріатом національної оборони та безпеки або Міністерством до відання якого належать відповідна установа, підприємство або організація.

Щодо відповідальності за розголошення відомостей, які належать до секретної інформації, то законодавством Франції передбачається кримінальна відповідальність. Так, статтею 413-10 Кримінального кодексу Франції[48] передбачено, що будь-яка особа, яка у зв'язку зі своїм статусом чи професією, або в силу тимчасових або постійних повноважень чи обов'язків володіє будь-якими процесами, об'єктами, документами, інформаційними даними, комп'ютерними мережами, комп'ютеризованими даними або файлами, що мають оборонне значення, та винна у розголошенні, знищенні, викраденні, вилученні або відтворенні, або доведенні їх до відома невизначеного кола осіб чи будь-якої особи,

[48] Code pénal. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/

що не має на це права, карається позбавленням волі на строк до семи років та штрафом у розмірі 100 000 євро. Якщо злочин скоєно з необережності чи недбалості таке діяння карається позбавленням волі на строк до 3 років позбавлення волі та штрафом у розмірі 45 000 євро.

Також статтею 411-6 Кримінального кодексу Франції встановлено відповідальність за передачу або надання іноземній державі, іноземній компанії чи організації або організації, що перебуває під іноземним контролем, відомостей, матеріалів, документів, комп'ютерних даних або файлів, використання, розголошення чи збирання яких може завдати значної шкоди фундаментальним інтересам держави у вигляді позбавлення волі на строк до п'ятнадцяти років та штрафом у розмірі 225 000 євро. Таким чином, у Франції останнім часом було проведено реформування охорони державної таємниці, оптимізовано та удосконалено загальнодержавну систему класифікованої інформації, законодавчо уточнено особливості її обігу та поширення з урахуванням вимог і стандартів ЄС та НАТО.

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. Обмеження доступу до цієї інформації у просторі та за колом осіб гарантує, що виключно уповноважені особи з відповідним допуском до неї зможуть отримати доступ до неї. Порушення нормативних вимог та стандартів дотримання й охорони державної таємниці може призвести до кримінального переслідування, запровадження суворих санкцій щодо винних осіб, які допустили розголошення таких відомостей або матеріалів (як навмисно, так і з необережності).

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)[49]. Відповідно до статті 4 цього закону секретна (класифікована) інформація означає інформацію, факти, предмети 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), незалежно від форми їхнього представлення. Секретна інформація може включати документи, а також пов'язані з ними засоби для здійснення дешифрування, шифрування, передачі інформації (за допомогою криптографічного ключа) тощо.

Комерційна, наукова, операційна, винахідницька, податкова чи інша приватна таємниця або обставини особистого життя також можуть підлягати під режим секретності в суспільних інтересах та встановлюватися заборони щодо

[49]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/

публічного поширення або афішування. Також цей законодавчий акт доповнює Адміністративний регламент про фізичну безпеку, якою затверджено Інструкцію щодо секретної інформації – (Verschlusssachenanweisung)[50]. Зокрема, стаття 63 цієї Інструкції передбачає, що уповноважені посадові особи, відповідальні за безпеку секретних документів на рівні відповідних державних органів повинні через певні проміжки часу перевіряти, чи відповідає поточний стан секретних документів встановленим нормативним вимогам, визначених на законодавчому рівні.

У Німеччині система захисту державних секретів взаємопов'язана із загальною системою захисту значущих секретів у сфері промисловості й торгівлі з метою запобігання та недопущення промислового шпигунства та регулюється такими федеральними законодавчими актами як: про захист комерційної таємниці[51], про охорону даних[52] тощо.

Своєю чергою, Кримінальний кодекс Німеччини[53] містить положення про те, що державною таємницею є факти, об'єкти й інформація, доступні лише обмеженому колу осіб, які повинні зберігатися в секреті від іноземних держав з метою недопущення спричинення шкоди зовнішній безпеці ФРН.

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. Відповідальність за порушення службової таємниці встановлена у 4 розділі Кримінального кодексу ФРН (статті 93-100). Стаття 93 Кримінального кодексу Німеччини передбачає, що

[50]Verschlusssachenanweisung 24.04.2024. URL: https://www.umwelt-online.de/regelwerk/cgi-bin/suchausgabe.cgi?pfad=/allgemei/laender/bln/vsa.htm&such=Verwaltungsvorschrift%20%FCber%20die

[51]Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) 18.04.2019. URL: https://www.gesetze-im-internet.de/geschgehg/BJNR046610019.html

[52] Bundesdatenschutzgesetz. 27.01. 1977. URL: https://www.gesetze-im-internet.de/bdsg_2018/index.html

[53]Strafgesetzbuch (StGB). URL: https://www.gesetze-im-internet.de/stgb/BJNR001270871.html#BJNR001270871BJNG003902307

державна таємниця – це факти, об'єкти або висновки, які доступні лише обмеженій групі осіб і які повинні зберігатися в таємниці від іноземної держави, щоб запобігти ризику заподіяння суттєвої шкоди зовнішній безпеці Німеччині. Стаття 94 визначає перелік громадян, які мають доступ до державної таємниці та злочинні дії яких підпадають під кримінальне переслідування з боку держави: особи, які повідомляють (передають) іноземній державі або одному з її посередників таємну інформацію або іншим способом оприлюднити таку інформацію або матеріали державної таємниці на шкоду державним інтересам чи з метою надання переваги іноземній державі, що створює ризик суттєвої шкоди для зовнішньої безпеки. Частина 1 статті 95 Кримінального кодексу Німеччини встановлює відповідальність за розголошення державної таємниці та передбачає покарання у вигляді позбавлення волі на строк від шести місяців до п'яти років. Частина 3 статті 94 КК Німеччини передбачає, що в особливо тяжких випадках покаранням є позбавлення волі на строк до десяти років. Необережне розголошення державної таємниці (стаття 97), тобто службова особа, яка з необережності допустила ситуацію, коли державна таємниця, яка зберігається, за її ініціативою стала загальнодоступною та потрапила до несанкціонованого доступу, створює ризик заподіяння серйозної шкоди зовнішній безпеці Федеративної Республіки Німеччини, – карається позбавленням волі на строк до трьох років або штрафом.

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, яка адмініструє документи, що містять службову інформацію.

Слід зазначити, що у ФРН до державної таємниці належать 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, встановлених розділами 8 та 12(1)

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 відповідно до статей 9 та 12(2) Закону «Про вимоги і порядок проходження федеральних допусків та захисту секретної інформації». 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 мають 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 (статті 10 та 12(3) Закону).

Стаття 32(1) Закону передбачає, що 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. Зобов'язання також може бути накладено на період після припинення конфіденційної діяльності. 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)[54].

Уповноваженим органом у сфері охорони державної таємниці в Німеччині є Федеральне відомство охорони конституції (Bundesamt für Verfassungsschutz)[55], 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

[54] Gesetz über die Rechtsstellung der Soldaten. 30.05.2005. URL: https://www.buzer.de/gesetz/2246/index.htm
[55] Der Verfassungsschutz.URL: https://www.verfassungsschutz.de/DE/home/home_node.html

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 в Німеччині 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. (пункт 2 статті 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 грифа 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.

Табл. 2

Види дозволів залежно від грифа таємності інформації в Німеччині[56]

1. Проста перевірка – («Ü1»)
2. Розширена перевірка – («Ü2»)
3. Розширена перевірка безпеки з розслідуваннями безпеки («Ü3»)
4. Розширена перевірка з розслідуваннями безпеки щодо військовослужбовців («Ü4»)

З 15 червня 2022 року набули чинності зміни до статті 32(1), 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[57].

Польща. Перевірка безпеки та поводження з секретними матеріалами регулюються Законом від 5 серпня 2010 року «Про захист секретної інформації» (далі – Закон)[58]. Цей законодавчий акт містить визначення обробки секретної інформації (пункт 5 статті 2), порядок засекречування секретної інформації (пункти «цілком таємно», «таємно», «конфіденційно» та «з обмеженим доступом» (стаття 5)), завдання Агентства внутрішньої безпеки та Служби військової контррозвідки щодо нагляду за функціонуванням державної системи захисту секретної інформації

[56] Sicherheitsüberprüfung. URL: https://de.wikipedia.org/wiki/Sicherheits%C3%BCberpr%C3%BCfung

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

[58] Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-informacji-niejawnych-17646871

(стаття 10) та порядку надання доступу до секретної інформації та допуску до забезпечення безпеки (статті 21-34).

Рис. 2

Класифікація секретної інформації в Польщі[59]

Відповідно до статті 10 Закону Агентство внутрішньої безпеки (ABW) спільно зі Службою військової контррозвідки (SKW) мають повноваження у сфері контролю загальнодержавною системою захисту секретної інформації шляхом:

1)здійснення перевірки та контролю за обігом секретної інформації та дотримання відповідних положень;

2) виконання завдань щодо безпеки IT-систем;

3) проведення процедур перевірки та забезпечення промислової безпеки;

4) забезпечення захисту секретної інформації, якою обмінюються Республіка Польща та інші країни чи міжнародні організації;

5) проведення тренувань та навчань з питань захисту секретної інформації.

Відповідно до пункту 1 статті 21 Закону допуск до роботи або служби на посадах або призначення роботи, пов'язаної з доступом до інформації з грифом «Конфіденційно» або вище, може надаватися після отримання допуску до безпеки та проходження навчання з питань захисту секретної інформації.

Допуск до державної таємниці – це документ, що підтверджує гарантію додержання вимог щодо державної таємниці особою, яка його отримує. Разом із сертифікатом, що підтверджує підготовку з питань захисту секретної інформації, він надає особі доступ до секретної інформації, тобто інформації, на яку поширюється спеціальне положення про секретність (стаття 5 Закону). Дозвіл видається тільки після того, як національний орган безпеки (ABW або SKW) або представник служби безпеки проведуть відповідні процедури перевірки. У Польщі існує 4 види грифа секретності: «Цілком таємно», «Таємно», «Конфіденційно» і «З обмеженим доступом».

Відповідно до статі 5 Закону гриф «Цілком таємно» надається, якщо несанкціоноване розголошення секретної інформації завдасть винятково серйозної шкоди Республіці Польща, оскільки:

- загрожує незалежності, суверенітету чи територіальній цілісності Польщі;

[59] URL: https://prk.men.gov.pl/uk/1uk/

- загрожуватиме внутрішній безпеці чи конституційному ладу Польщі;
- загрожуватиме міжнародному становищу Польщі;
- може послабити обороноздатність Польщі;
- призведе або може призвести до ідентифікації офіцерів, військовослужбовців або працівників служб, відповідальних за виконання розвідувальних або контррозвідувальних завдань, які виконують оперативну та розвідувальну діяльність, якщо це загрожує безпеці виконуваної діяльності або може призвести до ідентифікації осіб, які їх здійснюють;
- загрожує або може загрожувати життю чи здоров'ю осіб рядового, військовослужбовця чи службовця, які здійснюють оперативно-розвідувальну діяльність, або осіб, які надають їм у зв'язку з цим допомогу.

Секретна інформація має гриф «Секретно», якщо її несанкціоноване розголошення завдасть серйозної шкоди державним інтересам, оскільки:
- перешкоджатиме виконанню завдань щодо захисту суверенітету чи конституційного ладу Республіки Польща;
- погіршить відносини Республіки Польща з іншими країнами чи міжнародними організаціями;
- порушує оборонну підготовку держави або функціонування Збройних Сил Республіки Польща;
- перешкоджатиме проведенню уповноваженими службами чи установами оперативно-розвідувальних заходів, які здійснюються з метою забезпечення безпеки держави або притягнення до відповідальності осіб, які вчинили злочини;
- суттєво порушить функціонування правоохоронних органів та системи правосуддя;
- призведе до значної шкоди економічним інтересам Польщі.

Секретна інформація класифікується як «Конфіденційна», якщо її несанкціоноване розголошення завдає шкоди Республіці Польща, оскільки:
- ускладнить реалізацію поточної зовнішньої політики Республіки Польща;
- перешкоджатиме реалізації оборонних проектів або негативно вплине на боєздатність Збройних Сил Польщі;
- порушує громадський порядок або загрожує безпеці громадян;
- перешкоджатиме виконанню завдань службами або установами, відповідальними за захист безпеки або основних інтересів Республіки Польща;
- перешкоджатимуть виконанню завдань службами чи установами, відповідальними за охорону громадського порядку, безпеки громадян або притягнення до відповідальності осіб, які вчинили злочини та податкові правопорушення, а також судовими органами;
- загрожуватиме стабільності фінансової системи Польщі;
- негативно позначиться на функціонуванні національної економіки.

Під гриф «З обмеженим доступом» підпадає інформація з обмеженим доступом, якщо їй не встановлено підвищений рівень секретності та її несанкціоноване розголошення може негативно вплинути на виконання органами державної влади або іншими структурними підрозділами завдань у сфері оборони

країни, зовнішньої політики, громадської безпеки, дотримання прав і свобод громадян, системи правосуддя чи економічних інтересів Республіки Польща.

Згідно з пунктом 3 статті 29 Закону, допуск до інформації з грифом «Конфіденційно» є тимчасовим і видається на строк 10 років; для інформації з грифом «Секретно» – на строк 7 років; а для інформації з грифом «Цілком таємно» – на строк 5 років.

Питання грифування документів, скасування грифа, порядок й умови їхньої реєстрації в журналах обліку секретних матеріалів регулюється розпорядженням Прем'єр-міністра від 22 грудня 2011 року «Про порядок позначення матеріалів та проставлення на них грифів секретності»[60]. Зокрема нормативно встановлено, що скасування або зміна режиму секретності можлива в разі припинення або зміни встановлених законом підстав для охорони за письмовою згодою особи, яка присвоїла гриф, або її керівника. Якщо зміна або скасування грифа секретності стосується інформації з грифом «Цілком таємно», письмова згода на проведення зазначених заходів надається керівником підрозділу, в якому цьому матеріалу встановлено такий гриф. У разі припинення, скасування, ліквідації, перетворення або реорганізації організаційного підрозділу, права на скасування або зміну положення про секретність матеріалу переходять до його правонаступника. У разі відсутності правонаступника права щодо цього переходять до Агентства внутрішньої безпеки або Служби військової контррозвідки відповідно до їх підвідомчості. У разі завищення або заниження грифа секретності одержувач матеріалу може звернутися до посадової особи, яка його видала, або її керівника з вимогою внести відповідну зміну. Секретна інформація захищена, доки не буде скасовано або змінено положення про секретність. Проте особа, яка присвоїла гриф секретності, може вказати дату чи подію, після яких гриф секретності буде скасовано або змінено.

Стаття 22 Закону регулює процедуру перевірки та розширену процедуру перевірки, надаючи доступ до інформації з грифами «Цілком таємно» та «Таємно». Залежно від посади або спектру виконання дорученої діяльності, на яку претендує особа-кандидат, що перевіряється, здійснюється:

1) звичайний допуск – для посад і робіт, пов'язаних з доступом до інформації з грифом «Конфіденційно»;

2) розширений допуск на безпеку:

а) на посади та роботу, пов'язані з доступом до інформації під грифом «Таємно» або «Цілком таємно»;

б) співробітникам служби безпеки, заступникам охоронців та кандидатам на такі посади;

в) керівникам підрозділів, які обробляють інформацію з грифом «Конфіденційно» або вище;

г) особам, які звертаються за доступом до міжнародної секретної інформації або за доступом, що має бути наданий відповідно до міжнародного договору, укладеного Республікою Польща.

[60]Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20112881692

Допуск, яким надається доступ до секретної інформації, та строк його дії фіксується у відповідному наказі.

Таким чином, залежно від посади або виконання доручених заходів, проводяться регулярні або розширені процедури перевірки. Відповідно до статті 24 Закону, заповнена анкета є таємною і охороняється законом, а також підлягає захисту, передбаченому для секретної інформації з грифом «Конфіденційно» у випадку розширеної перевірки або «З обмеженим доступом» у випадку звичайної перевірки. Дані перевірки обов'язково засекречуються, а строк зберігання анкети та результатів перевірки безпеки становить 20 років.

Проведення процедури перевірки вимагає письмової згоди відповідної особи. Проста процедура перевірки проводиться представником служби безпеки (співробітником, відповідальним за питання безпеки) за письмовим клопотанням керівника відповідного підрозділу, а розширена процедура перевірки проводиться Агентством внутрішньої безпеки та Військовою контррозвідкою, на вимогу в запиті. Процедура скринінгу спрямована на визначення того, чи дає особа, яка проходить обстеження, гарантію секретності та полягає у перевірці минулого обстежуваної особи, її політичної та трудової діяльності, потенційних контактів з іноземною розвідкою, дотримання законодавства, стану психічного здоров'я, достовірності даних, наданих особою в анкеті. Під час процедури перевірки перевіряє реєстри, записи та справи, зокрема Національний реєстр судимостей. Під час процедури перевірки визначається наявність обґрунтованих сумнівів щодо: участі, співпраці чи підтримки особи, яка перевіряється, на шпигунство, тероризм, саботаж чи іншу діяльність, спрямовану проти Республіки Польща; наявні погрози щодо особи, яка перевіряється з боку іноземних спецслужб у вигляді спроб її завербувати або встановити з нею контакт; приховування або свідомо неправдиве надання особою, яка перевіряється, відомостей, що мають відношення до захисту секретної інформації; настання стосовно особи, яка перевіряється, обставин, які призводять до ризику піддатися шантажу чи тиску, встановлення фактів неналежного поводження з секретною інформацією тощо. Процедура закінчується наданням допуску, відмовою в допуску або анулюванням допуску.

Розширена процедура перевірки також може включати бесіди з родичами, сусідами, колегами та керівниками обстежуваної особи, а також перевірку її банківських рахунків. У ході процедури розширеної перевірки також визначається наявність сумнівів щодо: рівня життя, якщо встановлено факти перевищення доходів, відомості про психічну хворобу або інші порушення психічної діяльності, що обмежують розумову дієздатність і можуть негативно вплинути на здатність особи, яка перевіряється, виконувати роботу, пов'язану з доступом до секретної інформації; залежність від алкоголю, наркотичних засобів або психотропних речовин. Орган, який проводить процедуру перевірки, відмовляє у видачі допуску, якщо наявні сумніви виявлені під час проведення звичайної процедури перевірки відповідно. Орган, який проводить процедуру перевірки, відмовляє у видачі допуску, якщо особу, яку перевіряють, було засуджено остаточним вироком до позбавлення волі за умисний злочин, або за злочин, вчинений за кордоном, чи умисний фінансовий злочин.

Після завершення процедури перевірки з негативним результатом орган, що проводить процедуру, виносить рішення про відмову у видачі допуску та вручає

його особі, яка перевіряється, повідомляючи про це заявника та представника служби безпеки. Перевірка щодо особи, якій відмовлено у видачі допуску, може бути проведена не раніше, ніж через рік з дня вручення рішення про відмову у видачі допуску. Проведення перевірки припиняється у разі: смерті особи, яка перевіряється; у випадку, коли особа, яка перевіряється, за власним бажанням відмовляється від вступу на посаду чи виконання роботи, пов'язаної з доступом до секретної інформації; у випадку, коли керівник організаційного підрозділу відмовляється від призначення особи, яка перевіряється, на посаду або доручення їй роботи, пов'язаної з доступом до секретної інформації тощо.

Покарання за вчинення злочинів, пов'язаних з охороною державної таємниці, передбачені Кримінальним кодексом Польщі[61]. Пункт 1 статті 265 КК (розголошення державної таємниці) встановлює кримінальну відповідальність для фізичних осіб, які здійснили розголошення секретної інформації, класифіковану як «Таємно» або «Цілком таємно» та визначає покарання ув'язненням від 3 місяців до 5 років. Відповідно до пункту 2 у випадку, якщо секретна інформація розголошується особі, яка діє від імені або за дорученням іноземної організації або іноземної держави, винний підлягає покаранню у вигляді позбавлення волі на строк від 6 місяців до 8 років. Пункт 3 регламентує, що кожен, хто ненавмисно (з необережності) розголошує відомості, віднесені до секретної інформації, передбачені пунктом 1 цієї статті, які стали йому відомі у зв'язку з виконанням публічної функції або отриманим дозволом, підлягає штрафу, обмеженню волі або позбавленню волі на строк до одного року. Стаття 266 КК Польщі встановлює кримінальну відповідальність за розголошення службової або професійної таємниці. Пункт 2 цієї статті регламентує, що державний службовець, який розголошує сторонній особі секретну інформацію, класифіковану як «З обмеженим доступом» або «Конфіденційно», або інформацію, отриману у зв'язку із виконанням службових обов'язків, розголошення якої може поставити під загрозу охоронюваний законом інтерес, підлягає покаранню у вигляді позбавлення волі на строк до 3 років.

Естонія. Питання здійснення охорони державної таємниці регулюється профільним законом Естонії «Про державну таємницю та секретну іноземну інформацію»[62] (далі – Закон). 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 в Законі про державну таємницю та секретну іноземну інформацію та (б) вона повинна вимагати захисту від оприлюднення в інтересах забезпечення безпеки Естонії. Державною таємницею є інформація, розголошення якої поставило б під загрозу безпеку Естонії або завдало б 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 важливим складником запобігання розвідувально-підривній діяльності іноземних спецслужб проти Естонії. Метою цього

[61] Ustawa Kodeks karny z dnia 6 czerwca 1997 r. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20200001444/U/D20201444Lj.pdf

[62] Riigisaladuse ja salastatud välisteabe seadus 25.01.2007. URL: https://www.riigiteataja.ee/akt/107032023010

законодавчого акта є забезпечення безпеки та зовнішніх відносин Естонської Республіки, захист державної таємниці та секретної інформації іноземних держав 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. Перевірка безпеки має бути виправдана стосовно певної особи, оскільки передбачає звуження основних прав та подальшу високу сферу відповідальності. Дозволи на доступ до державної таємниці поділяються на два види – дозвіл для фізичної особи та дозвіл для юридичної особи. Дозвіл на доступ юридичної особи не поширюється на фізичних осіб, які там працюють. Дозвіл доступу не надає права доступу до всієї секретної інформації, але вимагає наявності дозволу відповідного рівня та реальної потреби в контакті з інформацією. Щоб отримати доступ, потрібна перевірка безпеки. Винятком є допуск до державної таємниці лише рівня «З обмеженим доступом».

За наявності обставин, що призводять до відмови у наданні допуску, посадова особа звільняється з посади. Перевірка безпеки фізичної особи зазвичай триває три місяці та може бути продовжена ще на наступні три місяці, якщо виникнуть обставини, зазначені в статті 33(4) Закону. Перевірка безпеки юридичної особи, як правило, триває шість місяців, і її також можна продовжити, якщо виникнуть обставини, зазначені в частині 4 статті 43 закону. Під час проведення перевірки безпеки контролюючий орган в особі Агентства оборонної поліції має у межах повноважень досить широкі можливості перевірити минуле особи, у тому числі обставини приватного життя. Межі перевірки особи залежать від конкретного заявника на дозвіл доступу до інформації. 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.

Положення щодо захисту секретної інформації іноземних держав, у тому числі секретної інформації НАТО, викладені у главі 3 «Таємна інформація іноземних держав» (статті 50–52). Секретна іноземна інформація визначається в § 3 п. 2 Закону про державну таємницю та секретну іноземну інформацію як «інформація, засекречена та розкрита Естонії іноземною державою, Європейським Союзом, НАТО або будь-якою іншою міжнародною організацією чи установою, створеною міжнародною угодою, та інформація, створена Естонською Республікою для виконання іноземного договору, яка повинна бути засекречена відповідно до іноземного договору». Таким чином, закон надає секретній інформації іноземної країни дві характеристики: (а) інформація спочатку належить іноземній країні, міжнародній організації чи установі, створеній міжнародною угодою, (б) видавець інформації засекретив її. Естонія обмінюється секретною інформацією з країнами, з

якими укладено угоди про захист секретної інформації, і інформація захищена відповідно до положень угоди. По-друге, у законі зазначено, що секретна іноземна інформація – це інформація, створена Естонською Республікою для виконання іноземного договору, яка повинна бути засекречена відповідно до іноземного договору. Це означає, що секретна іноземна інформація також може бути створена в Естонії – наприклад, посади, підготовлені та представлені в рамках участі в програмі НАТО, які засекречені на основі керівних принципів НАТО щодо секретності, а не Закону про державну таємницю та секретну іноземну інформацію, є секретною інформацією НАТО, а не Естонії. З метою організації захисту секретної іноземної інформації застосовуються вимоги та заходи, які встановлені для державної таємниці Естонії, виходячи із рівня секретності іноземної країни та її відповідності рівню державної таємниці Естонії, а також з урахуванням встановлених відмінностей в естонському законодавстві та договорах з іноземними державами щодо обробки секретної іноземної інформації.

Важливим додатком до цитованого закону є Порядок охорони державної таємниці та секретної іноземної інформації, затверджений Урядом Естонії, який набув чинності з 1 січня 2008 року[63]. На виконання цього нормативного акта в Естонії створено та здійснюється адміністрування реєстру носіїв секретної інформації. Вимоги до створення і обслуговування такого реєстру встановлюються Розділом 2 (статті 47-54). Так, зокрема стаття 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 прийняття-передання; 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) ознака знищення.

Опрацювання державної таємниці – це узагальнений термін, який включає будь-які операції з державною таємницею або секретною іноземною інформацією. Зокрема це складання, маркування, збирання, зберігання, збереження, перевезення, відтворення, передача, 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 п’ять 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.

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

Для позначення рівня секретності розділів тексту, менших за одну сторінку, у секретних документах Естонії (як і НАТО) можуть використовуватися такі стандартні скорочення: CTS, NS, NC, NR. Документи часто мають позначення «NATO UNCLASSIFIED». Це не секретна інформація, але вона все одно потребує захисту від розголошення, а її поширення здійснюється з урахуванням принципу «необхідності знати», подібно до інформації, призначеної для «ВИКОРИСТАННЯ В ОРГАНІЗАЦІЯХ» на території Естонії відповідно до Закону про публічну інформацію[64]. Слід зазначити, що маркування таких документів має відповідати частині 3 статті 41 Закону про державну таємницю та секретну іноземну інформацію.

У документах ЄС досить часто використовується позначка «LIMITÉ», яка засвідчує, що документ не підпадає під секретну інформацію, але все ж потребує захисту від розголошення, та її розповсюдження здійснюється з урахуванням принципу «необхідно знати», подібно до інформації, призначеної для «ВИКОРИСТАННЯ В ОРГАНІЗАЦІЇ» Маркування таких документів має ґрунтуватися на частині 3 статті 41 Закону про державну таємницю та секретну іноземну інформацію».

Секретний документ повинен бути позначений розробником документа, як тільки він починає підготовку документа, грифом рівнів секретності «ОБМЕЖЕНО», «КОНФІДЕНЦІЙНО», «СЕКРЕТНО» або «ЦІЛКОМ СЕКРЕТНО» у верхній або нижній частині документа великими літерами, відсортованим жирним шрифтом з висотою кегля не менше 16. Якщо неможливо додати позначку класифікації в програмі обробки текстів (наприклад, логотипи на фірмовому бланку заважають друкувати позначку або це не паперовий документ), позначку класифікації також можна додати після друку документа з копією печатки. Закон про державну таємницю та іноземну інформацію також передбачає можливість засекречувати документ додатковим знаком (наприклад, «РОЗКРИВАЄТЬСЯ ЛИШЕ АДРЕСАТУ»), що означає додатковий захід безпеки, застосований до носія інформації або визначає коло осіб з правами доступу до носія інформації. Якщо документ, що містить державну таємницю Естонії, передається іноземній державі або міжнародній організації, на документі повинні бути нанесені грифи секретності, які відповідають вимогам міжнародного договору, а в правому куті титульної сторінки має бути вказана англійською мовою позначка про те, що ця інформація є власністю Естонії.

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 зазначених країнах носіїв секретних відомостей, загрожує державним таємницям 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 від’їзду[65]. В Естонії максимальний строк дії

[64] Avaliku teabe seadus 15.11.2000. URL: https://www.riigiteataja.ee/akt/122032011010

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

засекречуваних відомостей та інформації, які належать до державної таємниці, загалом складає 50 років, а мінімальний – 5 років.

Покарання за вчинення злочинів, пов'язаних з державною таємницею, передбачені Кримінальним кодексом Естонії[66]. Зокрема стаття 63 встановлює кримінальну відповідальність за збирання відомостей, що становлять державну таємницю з метою їх подальшої передачі іноземній державі, іноземній організації, іноземцю чи особі, яка діє від імені іноземної держави, а також за збирання чи передачу іншої інформації від імені органу іноземної розвідки. Санкція покарання передбачає позбавлення волі на строк до десяти років. Стаття 73 встановлює кримінальну відповідальність за розголошення державної таємниці: розголошення або незаконне передання державної таємниці рівня «конфіденційно» або надання до неї незаконного доступу за відсутності ознак прослуховування, – караються штрафом або позбавленням волі на строк до двох років. Частина 2 статті 73 регламентує, що розголошення чи незаконне передання державної таємниці рівня «секретно» або надання незаконного доступу до неї за відсутності ознак прослуховування – караються позбавленням волі від двох до чотирьох років. Частина 3 статті 73 визначає, що розголошення чи незаконне передання державної таємниці рівня «цілком таємно» або надання до неї незаконного доступу за відсутності ознак прослуховування – караються позбавленням волі на строк від трьох до восьми років. Відповідно до статті 74 КК Естонії втрата носія інформації, що містить державну таємницю особою, якій цей носій був довірений, якщо втрата сталася внаслідок порушення законодавства про охорону державної таємниці, карається штрафом або позбавленням волі на строк до двох років. Частина 2 статті 74 КК визначає, що те саме діяння, якщо воно спричинило тяжкі наслідки передбачає покарання у вигляді позбавлення волі від одного до трьох років. Стаття 52 Закону про державну таємницю та секретну іноземну інформацію встановлює, що за скоєння проступку, пов'язаного з порушенням вимог законодавства про державну таємницю, судом або в позасудовому порядку до винного може бути застосовано як додаткове покарання позбавлення доступу до державної таємниці чи секретної іноземної інформації або заборону на обробку державної таємниці та секретної іноземної інформації на строк до одного року.

1 травня 2023 року набув чинності закон Естонії «Про внесення змін до Закону «Про державну таємницю та секретну іноземну інформацію», «Про публічну інформацію» та «Про державну службу» [67]. Підставами для ініціювання внесення змін до естонського законодавства про охорону державної таємниці стали зміни світової безпекової ситуації, масштабна військова агресія РФ проти України, виклики і потреби удосконалити захист державної таємниці в умовах глобального цифрового розвитку та епохи цифровізації. Відповідно до положень закону, вимоги обробки секретної інформації мають бути приведені у відповідність до сучасних засад управління безпекою інформації ЄС, а державна таємниця та іноземна інформація юридично краще захищені, щоб особи без права доступу до неї не отримували такі відомості жодним чином. Відповідальним державним органом у сфері забезпечення охорони державної таємниці визначено Агентство оборонної

[66] Kriminaalkoodeks 29.07.2002. URL: https://www.riigiteataja.ee/akt/184289
[67] Riigisaladuse ja salastatud välisteabe seaduse, avaliku teabe seaduse ning avaliku teenistuse muutmise seadus. 13.02.2023. URL: https://www.riigiteataja.ee/akt/107032023002

поліції, яке уповноважене захищати державну таємницю та секретну іноземну інформацію, контролювати та гарантувати безпеку у цій сфері. Агентство оборонної поліції – державна установа, яка діє під юрисдикцією Міністерства внутрішніх справ Естонії[68]. Також відповідальність за порушення вимог щодо забезпечення охорони державної таємниці несе відповідна службова особа, якій надано такі повноваження у рамках міністерств та відомств Естонії.

Хорватія. На державному рівні охорона державної таємниці врегульована такими законодавчими актами як: «Про конфіденційність даних»[69] та «Про інформаційну безпеку»[70]. 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» (стаття 4 Закону Хорватії «Про конфіденційність даних») (Рисунок 3).

Рис. 3

Класифікація секретної інформації в Хорватії[71]

Стаття 10 Закону Хорватії «Про конфіденційність даних» встановлює, що 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. Стаття 13 цитованого закону встановлює, що 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

[68] Kaitsepolitseiamet. URL: https://kapo.ee
[69] Zakon o tajnosti podataka. 07.08.2007. URL: https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka
[70] Zakon o informacijskoj sigurnosti. 30.7.2007. URL: https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti
[71] Zakoni Republike Hrvatske vezani uz informacijsku sigurnost i zaštitu podataka. URL: https://security.foi.hr/wiki/index.php/Zakoni_Republike_Hrvatske_vezani_uz_informacijsku_sigurnost_i_za%C5%A1titu_podataka.html

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 Республіки Хорватія. 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[72]. 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»[73]. Заходи та стандарти інформаційної безпеки встановлюють мінімальні критерії захисту секретних даних. Стаття 4 цього закону встановлює, що 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 регламентує, що заходи та стандарти інформаційної безпеки

[72] The Office of the National Security Council. URL: https://www.uvns.hr/en

[73] Zakon o informacijskoj sigurnosti 13.07.2007 № 79/07. URL: https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti

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 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.

Стаття 14 Закону «Про інформаційну безпеку» встановлює, що Управління Ради національної безпеки є центральним державним органом, який координує та узгоджує прийняття й застосування заходів і стандартів інформаційної безпеки в Республіці Хорватія та в обміні секретними даними між Хорватією та іноземними державами й міжнародними організаціями. При цьому, Апарат РНБО Хорватії співпрацює з відповідними установами іноземних держав та міжнародними організаціями у сфері забезпечення інформаційної безпеки та координує міжнародне співробітництво.

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»[74]. 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 статті 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

[74] 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

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.

Стаття 8 регламентує, що з метою обмеження подальшого розповсюдження секретних даних використовується позначка «ЕКСКЛЮЗИВ». У випадку обмеження розповсюдження секретних даних конкретною країною чи міжнародною організацією буде використовуватися позначка «ONLY». Якщо мітка «ISKLJUČIVO» використовується для подальшого обмеження розповсюдження секретних даних, вказується офіційна назва або абревіатура користувача, якому секретні дані можуть бути доставлені. Фізична копія всіх або частини секретних даних повинна мати гриф про ступінь секретності оригіналу та відмітку про копію. Стаття 12 Положення встановлює, що зміна рівня секретності таємних даних або їх розсекречування позначається перекресленням позначки наявного рівня секретності та проставленням нової позначки під поточною. Сертифікат на доступ до таємної інформації рівня «Цілком таємно», «Таємно», «Конфіденційно» видається Управлінням РНБО, відповідно до положень Закону «Про конфіденційність інформації» (стаття 19). З метою організації доступу до секретних даних інших країн або міжнародних організацій сертифікат видається англійською мовою. Бланки сертифікатів видаються Управлінням Ради національної безпеки відповідно до стандартів, встановлених у рамках міжнародних угод про безпеку, підписаних Республікою Хорватія з іншими державами або міжнародними організаціями.

Питання конфіденційного захисту даних у Міністерстві оборони урегульовано відповідним наказом оборонного відомства Хорватії[75]. 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. Хорватське законодавство визначає поняття військової таємниці, зокрема

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

«засекречена оборонна інформація» – це інформація, яка має один із рівнів секретності, а також інформація, яка була подана у якості засекреченої до Міністерства оборони іншою державою, міжнародною організацією чи органом з якими співпрацює Республіка Хорватія. У міністерстві оборони Хорватії у питаннях військової таємниці використовуються загальнодержавні 4 грифи секретності: «цілком таємно», «таємно», «конфіденційно», «обмежено».

Організаційні підрозділи Міноборони та Генерального штабу Збройних Сил Хорватії на рівні управлінь, секторів, служб, а також на рівні командувань або підпорядкованих підрозділів Збройних Сил можуть бути наділені правом у межах своєї компетенції ініціювати розробку спеціальних інструкцій щодо класифікації секретних даних, які охоплюватимуть сфери, групи даних у цих сферах, а також дані з діапазонами можливих рівнів секретності. Нормативно встановлено, що засекречування – це процедура, за якою для даних у сфері оборони та системи військової безпеки і розвідки визначається один із ступенів секретності, який має бути захищеним, щоб уникнути несанкціонованого розголошення даних. Порядок засекречування відомостей, створених у Міністерстві оборони, здійснюють 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. При класифікації ступінь секретності даних визначається відповідно до їх змісту. При проведенні процедури засекречування даних відповідальні уповноважені особи зобов'язані визначити найнижчий рівень секретності, який забезпечить захист інтересів оборони та системи військової безпеки і розвідки, надасть змогу запобігти шкоді, яка може виникнути через неавторизоване розкриття, використання, публікацію або втрату цих даних. При проведенні процедури засекречування розробники секретних даних можуть визначати строк секретності, якщо це дозволяє зміст даних. 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 (стаття 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.

Стаття 19 цього наказу встановлює, що процедура визначення необхідності збереження чи розсекречення секретних даних системи оборони та військової безпеки і розвідки здійснюється у разі: запиту компетентного судового органу; запиту користувача права на доступ до інформації або щодо повторного використання інформації. У разі поданого запиту користувача на право доступу до інформації та повторного використання інформації, власник секретних даних повинен, перш ніж схвалити рішення про розсекречування даних, здійснити оцінку пропорційності права на доступ до інформації та щодо повторного використання інформації у зв'язку з чим необхідно отримати позитивний висновок Управління Офісу Ради національної безпеки і оборони Хорватії, яке є уповноваженим державним органом, що координує та контролює впровадження заходів і стандартів інформаційної безпеки у сферах перевірки безпеки, фізичної безпеки, безпеки інформації, промислової безпеки, а також видає дозволи для фізичних та юридичних осіб на доступ до національної та секретної інформації НАТО та ЄС.

Також Управління Офісу РНБО 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.

Під час проведення процедури розсекречення або періодичної оцінки ступеня секретності даних розробник даних може запропонувати їхнє розсекречення повністю або частково (лише окремих частин), при цьому щодо частин даних, для яких все ще необхідно підтримувати ступінь секретності перед розсекреченням доцільно здійснити затемнення або іншим відповідним способом. В діяльності Міністерства оборони та Генерального штабу використовуються такі абревіатури для позначення ступенів секретності: «Цілком таємно» – ВТ; «Таємно» – Т; «Конфіденційно» – РОВ, «Обмежено» – OGR. Ці скорочення застосовуються з метою ведення персоналізованого обліку секретних даних і розміщуються перед грифом документа. У правому верхньому куті під грифом про ступінь секретності проставляється кількість примірників стосовно загальної кількості примірників секретного документа. Кожна сторінка секретного документа має номер сторінки в нижньому правому куті відносно загальної кількості сторінок. Розробники секретних відомостей, матеріалів та даних можуть позначати секретні дані додатковими знаками безпеки. Додатковими захисними заходами щодо секретних даних є: заборона або обмеження відтворення документів чи інших записів секретних даних; заборона, обмеження або визначення способу подальшого розповсюдження даних іншим адресатам; зобов'язання повернути секретні дані після їхньої перевірки; встановлення строку дії секретності, який визначається власником секретної інформації під час її створення. Розробник секретної інформації може заборонити або обмежити її відтворення, написавши у верхньому правому куті під грифом секретності текст «ЗАБОРОНЕНО КОПІЮВАННЯ» або «ОБМЕЖЕНО КОПІЮВАННЯ».

Стаття 29 наказу визначає, що автор секретної інформації може вимагати від одержувача повернення документа після перевірки, про що у верхньому правому куті під грифом рівня секретності робиться позначка «ПОВЕРНУТИ ПІСЛЯ ПЕРЕВІРКИ». Одержувач фіксує такий таємний документ у журналах реєстрації секретних документів певного рівня секретності. Після проведення перевірки документа у відповідний термін або протягом заздалегідь встановленого терміну секретний документ повертається його автору. У книгах обліку (реєстрах) у графі «Відмітка» робиться позначка «За перевіркою повернуто» із зазначенням дати повернення відповідного документа.

Знак «ISKLJUČIVO» використовується для заборони або обмеження подальшого розповсюдження секретних даних, коли документ доставляється одержувачам у Республіці Хорватія. При цьому до розширеної позначки «ЕКСКЛЮЗИВ» додається офіційна абревіатура органу державної влади або юридичної особи, яка отримує секретні дані. При пересиланні або зберіганні секретна інформація поміщається в непрозорі конверти або інші захисні оболонки з метою запобігання можливості прочитання та пошкодження змісту документа. У разі наявності великої кількості секретних документів або додатків до них вони запаковуються в коробки або інші відповідні захисні оболонки.

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.

Покарання за вчинення злочинів, пов'язаних із розголошенням державної таємниці передбачені Кримінальним кодексом Хорватії[76]. Стаття 347 КК встановлює відповідальність за розголошення державної таємниці та поширення секретних відомостей або матеріалів. У випадку встановлення таких фактів винна особа карається позбавленням волі на строк від шести місяців до 5 років. Отримання будь-якою особою секретної інформації з метою несанкціонованого її використання самостійно або іншою особою карається позбавленням волі на строк до 3 років. Частина 3 статті 347 КК передбачає, що той, хто розголошує державну таємницю або здійснює поширення секретних відомостей чи матеріалів з корисливих мотивів позбавляється волі на строк від одного до 10 років. Скоєння цього злочину з необережності карається тюремним ув'язненням на строк до 3 років, а в умовах воєнного стану або загрози війни – позбавлення волі на строк від 3 до 12 років. Стаття 348 КК Хорватії встановлює кримінальну відповідальність за шпигунство у формі надання або передачі незаконним шляхом таємної інформації іноземній державі, іноземній юридичній особі чи фізичній особі, яка на них працює, що є кримінально-карним діянням за яке передбачається покарання у вигляді позбавлення волі на строк від 1 до 10 років. Несанкціоноване збирання секретної інформації з метою подальшої її передачі іноземній державі, іноземній юридичній особі чи фізичній особі, яка на них працює, карається позбавленням волі на строк від шести місяців до 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.

[76] Kazneni zakon Hrvatska. URL: https://www.zakon.hr/z/98/Kazneni-zakon

Чехія. Національне законодавство Чехії у сфері охорони державної таємниці є досить розгалуженим та складається із: Закону «Про захист класифікованої інформації та безпеку»[77], Постанов Уряду: «Про встановлення переліку секретної інформації»,[78] «Про безпеку інформаційно-комунікаційних систем та інших електронних пристроїв, що обробляють секретну інформацію»[79], «Про запровадження сертифікації криптографічного захисту секретної інформації»[80], «Про адміністративну безпеку та реєстри секретної інформації»[81].

Основним актом законодавства у сфері здійснення охорони державної таємниці є закон «Про захист класифікованої інформації та безпеку», який регулює основні засади та принципи віднесення інформації до категорії секретної, визначає умови допуску та доступу до неї, інші вимоги щодо її захисту, визначає особливості обігу інформації з обмеженим доступом, регламентує сфери конфіденційної діяльності та умови її здійснення, діяльність у сфері державного управління секретами. Згідно з чеським законодавства секретна інформація – відомості, матеріали або дані, інформація в будь-якій формі, записані на будь-якому носії, який належним чином позначений, а розголошення або неправомірне поширення або використання може завдати шкоди державним інтересам Чехії. Перелік відомостей, які належать до секретної інформації затверджується Урядом країни у спеціальній постанові, яка переглядається кожні 5 років.

Під час оцінки секретної інформації державні інтереси Чехії розуміються як підтримання її конституційності, суверенітету й територіальної цілісності, забезпечення внутрішнього правопорядку, виконання та забезпечення виконання міжнародних зобов'язань у сфері безпеки і оборони, захисту економіки. Шкода інтересам Чеської Республіки в розумінні закону означає збитки або загрозу інтересам Чеської Республіки, при цьому відповідно до тяжкості шкоди або загрози інтересам Чехії поділяється на: надзвичайно серйозну, звичайну, просту. Відповідно до статті 4 цього законодавчого акта секретна інформація в Чехії класифікується за критеріями ступеня на такі категорії:

«Цілком таємно»	розголошення інформації сторонній особі або її неправомірне використання може завдати надзвичайно або винятково серйозної шкоди інтересам Чеської Республіки	«Přísně tajné», скорочено PT
«Таємно»	розголошення сторонній особі або її неправомірне використання може завдати серйозної шкоди інтересам Чеської	«Tajné», скорочено T

[77]Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: 21.09.2005 № 412/2005. URL: https://www.zakonyprolidi.cz/cs/2005-412

[78]Nařízení vlády, kterým se stanoví seznam utajovaných informací 07.12.2005 № 522/2005. URL: https://www.zakonyprolidi.cz/cs/2005-522

[79]Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi 29.12.2005 № 523/2005. URL: https://www.zakonyprolidi.cz/cs/2005-523

[80]Vyhláška o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací 29.12.2005 № 525/2005. URL: https://www.zakonyprolidi.cz/cs/2005-525

[81]Vyhláška o administrativní bezpečnosti a o registrech utajovaných informací 22.09.2022 № 275/2022. URL: https://www.zakonyprolidi.cz/cs/2022-275

	Республіки	
«Конфіденційно»	розголошення сторонній особі або її неправомірне використання може завдати шкоди інтересам Чеської Республіки	«Důvěrné», скорочено D
«Обмежено»	розголошення сторонній особі або неправомірне використання може завдати певної шкоди інтересам Чеської Республіки	«Vyhrazené», скорочено V

Секретна інформація, надана іноземною державою Чеській Республіці, також класифікується за вказаними рівнями, навіть якщо вона надана іноземною державою або міжнародною організацією.

Забезпечення захисту секретної інформації здійснюється у таких формах:

1) кадрова безпека, яка полягає у відборі фізичних осіб, які можуть мати санкціонований допуск до секретної інформації, перевірці умов їх доступу до секретної інформації, їх навчанні та захисті;

2) промислова безпека, яка складається із системних заходів з метою встановлення та перевірки передумов доступу суб'єкта господарювання (підприємця) до секретної інформації та забезпечення поводження із секретною інформацією відповідно до норм чинного законодавства Чехії;

3) адміністративна безпека, яка складається із системи заходів під час створення, отримання, реєстрації, обробки, відправлення, транспортування, передачі, зберігання, знищення, архівування чи іншого поводження із секретною інформацією;

4) фізична безпека, яка складається із системи заходів, призначених для запобігання або ускладнення доступу неавторизованої особи до секретної інформації, або для фіксації доступу чи спроби доступу до неї та яка включає такі режимні заходи та технічні засоби;

5) безпека інформаційних або комунікаційних систем, яка складається із системи заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності секретної інформації, яка обробляється цими системами, а також відповідальності адміністрації та користувачів за їхню діяльність у сфері захисту інформації з обмеженим доступом;

6) криптографічний захист, який складається із системи заходів щодо охорони секретної інформації шляхом використання криптографічних методів і матеріалів під час обробки, передачі чи зберігання секретної інформації.

Доступ до державної таємниці зазвичай надається тільки після проходження перевірки безпеки, під час якої оцінюються благонадійність та індивідуальні ризики для кожної особи. Перевірка безпеки має бути виправдана стосовно певної особи, оскільки передбачає звуження основних прав і подальшу високу сферу відповідальності. Дозволи на доступ до державної таємниці поділяються на два види: дозвіл для фізичної особи та дозвіл для юридичної особи (підприємця). Дозвіл на доступ юридичної особи не поширюється на фізичних осіб, які там працюють. Дозвіл доступу не надає права доступу до всієї секретної інформації, але вимагає наявності дозволу відповідного рівня та реальної потреби в контакті з інформацією. Щоб отримати доступ, потрібна перевірка безпеки. Винятком є допуск до державної

таємниці лише рівня «З обмеженим доступом». За наявності обставин, що призводять до відмови у наданні допуску посадова особа звільняється з посади. Перевірка безпеки фізичної особи як правило триває до 6 місяців. За чеським законодавством особа, яка отримала допуск до державної таємниці вважається такою, що отримала охоронну кваліфікацію, тобто є власником чинного сертифіката допуску до державної таємниці. Якщо фізична особа має дійсний національний сертифікат фізичної особи та проходить первинний інструктаж, а згодом фізичній особі видається «сертифікат НАТО», то ця фізична особа повинна пройти повторний інструктаж із зазначенням номера національного сертифіката фізичної особи та перевіряється, чи ця фізична особа дійсно ознайомлена із нормативними документами НАТО у цій сфері.

Стаття 55 вказаного закону встановлює терміни дії свідоцтва (допуску) фізичної особи за ступенем секретності: «Цілком таємно» – 5 років; «Таємно» – 7 років; «Конфіденційно» – 9 років. Посадові особи, які мають доступ до інформації з обмеженим доступом всіх рівнів секретності без наявного свідоцтва: Президент країни; депутати та сенатори парламенту; члени уряду; громадський захисник прав та представник громадського захисника прав; судді; президент, віцепрезидент і члени Вищої аудиторської палати Чехії.

Стаття 78 Закону регламентує, що надання секретної інформації, класифікованої як секретна або конфіденційна, між Чеською Республікою та державами-членами ЄС або між Чеською Республікою та владою Європейського Союзу, яка стосується взаємної співпраці держав-членів Європейського Союзу здійснюється через реєстр, який веде Міністерство закордонних справ Чехії.

У Чехії існують певні особливості маркування даних та реєстрації секретної інформації. Так, на інформації, яка внесена до переліку секретної інформації, автор зобов'язаний вказати своє ім'я, ступінь її секретності, її реєстраційне позначення та дату її створення. У секретній інформації, наданій Чеській Республіці іноземною державою, державним органом, юридичною чи фізичною особою, яка веде бізнес, якщо вони першими зареєстрували цю секретну інформацію обов'язково зазначається ступінь таємності відповідно до міжнародної угоди, якою зобов'язана Чеська Республіка і на основі якої надається секретна інформація, включаючи будь-яке скорочення відповідно до цієї угоди (наприклад використовуються абревіатури «ЄС», «ЄВРО» або «НАТО»), або відповідно до вимог іноземної держави або зі ступенем секретності іноземною державою секретної інформації, наданої призначеній особі; не зазначається найменування автора та дата створення секретної інформації.

Для секретної інформації, яка потребує суворіших умов для забезпечення окремих видів захисту секретної інформації у сферах, визначених, зокрема, міжнародним договором або правилами міжнародної організації, членом якої є Чеська Республіка, також вказується відповідне додаткове позначення (наприклад, позначення «KRYPTO», якщо це секретна інформація зі сфери криптографічного захисту, і позначення «ATOMAL», якщо це секретна інформація зі сфери зброї масового знищення). Ступінь секретності зазначається та відповідним чином маркується під час створення документа. Позначення ступеня секретності повинно зберігатися протягом усього терміну дії підстав секретності.

Ступінь секретності негайно скасовується або змінюється, якщо буде встановлено, що строки збереження класифікованої інформації пройшли, при цьому підстави для секретності не відповідають встановленому рівню секретності. Розпорядник секретної інформації зобов'язаний не рідше одного разу на 5 років перевіряти, чи зберігаються підстави для збереження інформації в таємниці з дня його створення. Якщо розробник або автор скасував або змінив рівень секретності, він повідомляє про цей факт негайно в письмовому вигляді адресатам секретної інформації. Одержувачі секретної інформації повинні негайно повідомити про цей факт у письмовій формі всіх інших адресатів, для яких він є конфіденційним. Адресат після отримання повідомлення про анулювання або зміну класифікації секретної інформації наноситься відповідний гриф про скасування або зміну рівня секретності на відомостях, матеріалах або документах.

Ступінь секретності зазначається прописним словом або відбитком штампа, а саме для секретної інформації відповідними словами: «Цілком таємно», «Таємно», «Конфіденційно», «Обмежено». На секретному документі в паперовій формі посередині верхнього та нижнього країв кожної сторінки секретного документа має бути відмітка про ступінь секретності. Ступінь секретності може зазначатися також для окремих параграфів або частин секретного документа відповідно до ступеня секретності конфіденційної інформації, яка в них міститься. Якщо рівень секретності позначено для параграфа, відповідний рівень секретності повинен бути позначений на одній сторінці секретного документа для всіх параграфів, що містять секретну інформацію. Якщо неможливо позначити ступінь секретності безпосередньо на секретному документі в непаперовій формі, він повинен бути позначений на описовій етикетці або іншим способом. Також нормативно передбачається процедура обмеження чинності ступеня секретності відповідно до пункту 3 розділу 22 Закону «Про захист класифікованої інформації та безпеку», що включає позначку шляхом написання слів «Засекретити до» та вказується проміжок часу, протягом якого секретний документ буде засекречений.

Розділ 9 Постанови уряду «Про адміністративну безпеку та реєстри секретної інформації» встановлює, що зміна або скасування рівня секретності має бути позначена у файлі, секретному документі, частині або абзаці шляхом викреслення початкового рівня секретності, щоб наданий рівень секретності залишався розбірливим. У разі зміни новий рівень класифікації має бути позначений поряд з вихідним рівнем класифікації. Здійснення зміни або скасування грифа підтверджується записом у справі, секретному документі, частині чи абзаці із зазначенням причини, дати вчинення, прізвища, імені та підпису особи, яка поставила позначку про зміну чи скасування грифу секретності. Позичений файл або секретний документ необхідно негайно повернути до протоколу наради для внесення запису про скасування або зміну рівня секретності. Запис про зміну рівня секретності відповідного документа або файлу, що складається з секретних документів, зареєстрованих у єдиному документі (збірнику), повинен бути зроблений у відповідному протоколі, а секретний документ або файл повинен бути перереєстровано за новим рівнем класифікації інформації. У разі зміни ступеня секретності обов'язкове посилання на номер провадження, під яким секретний документ було взято на новий облік. У разі, якщо одним протоколом зареєстровано секретні документи чи справи за першим реченням різних рівнів секретності, зміна

рівня секретності повинна бути проведена шляхом закреслення абревіатури рівня секретності, позначення абревіатури нового рівня секретності та занесення до протоколу засідання. Так само зміна ступеня секретності провадиться за допомогою протоколу, в якому також має бути зроблено запис про розсекречування секретного документа. Якщо відбувається зміна або скасування ступеня секретності таємного документа в електронній формі, який було створено в електронній системі служби файлів, що є частиною сертифікованої інформаційної системи, то його необхідно зазначити іншим способом, наприклад за допомогою засобів електронної системи файлового сервісу.

Державна політика у сфері охорони державної таємниці реалізується через Агенцію національної безпеки[82], яка є центральним адміністративним органом сфери охорони секретної інформації та здійснює державне управління у цій сфері. У своїй діяльності Агенція національної безпеки керується чинним законодавством Чехії та здійснює такі функції: системний захист секретної інформації; організація та проведення державного нагляду у сфері державної таємниці; ведення реєстрів секретної інформації; управління безпекою класифікованою інформацією; схвалення рішень про видачу допуску (свідоцтва) для фізичних осіб, визначеної чинним законодавством та видача документів про анулювання свідоцтва для фізичних осіб тощо. Також Агенція національної безпеки є адміністратором Центрального реєстру, який являє собою банк даних, поділений на центральні та додаткові файли, що використовуються з метою обліку та надання конфіденційних документів, класифікованих як конфіденційні, таємні та цілком таємні.

Секретні документи, що надаються в міжнародних відносинах, обліковуються і зберігаються у допоміжному журналі Центрального реєстру, який використовується у міжнародних відносинах між Чеською Республікою та Організацією Північноатлантичного договору, Європейським Союзом, іншими державами та міжнародними організаціями. При цьому Центральний реєстр виконує функцію центральної картотеки та є головним пунктом приймання та оформлення секретних документів, які використовуються у міжнародному спілкуванні.

У кожному державному органі питання охорони державної таємниці доручається відповідній уповноваженій посадовій особі. Так, наприклад, захист секретної інформації в Міністерстві внутрішніх справ (включно з Головним управлінням пожежно-рятувальної служби Чехії та поліції) здійснює міністр внутрішніх справ. На виконання статті 36а Закону Чехії «Про «Про захист класифікованої інформації та безпеку» державне управління у сфері захисту секретної інформації, а саме електронних документів, матеріалів і відомостей здійснює Національне управління з питань кібернетичної та інформаційної безпеки[83]. У рамках компетенції та відповідно до функціональності ця державна установа здійснює криптографічний захист секретної інформації, вивчає і попереджає кібернетичні ризики й загрози щодо секретної інформації недрукованого (електронного) виду. Контроль за діяльністю Агенції національної безпеки як адміністратора Центрального реєстру секретних даних, так і Національного управління з питань кібернетичної та інформаційної безпеки здійснює Палата депутатів, яка створює для цього спеціальний контрольний орган.

[82] Národní bezpečnostní úřad. URL: https://www.nbu.cz
[83] Národní úřad pro kybernetickou a informační bezpečnost. URL: https://nukib.gov.cz/

Відповідно до чеського законодавства передача, отримання або інше переміщення секретної інформації фіксується в спеціальних адміністративних довідках. Опис, копія чи переклад секретної інформації або витяг з неї можуть бути зроблені лише на підставі письмової згоди автора або розробника. Якщо це секретна інформація з грифом «Таємно» або «Конфіденційно», то це може бути зроблено лише за письмовою згодою безпосереднього керівника відповідного підрозділу або державного органу. Секретна інформація може транспортуватися або передаватися лише в спеціальних переносних ящиках або в закритій упаковці залежно від її ступеня секретності та носія інформації; його можна транспортувати лише через кур'єрську (фельд'єгерську) службу. В обов'язковому порядку одержувач повинен підтвердити отримання секретної інформації шляхом відповідного документального супроводження. Секретна інформація може перебувати в обігу протягом усього терміну її дії. Розсекречування або знищення секретної інформації здійснюється відповідно до спеціального порядку, який регламентований нормативними актами Чехії, який є обмежений у загальному доступі.

Стаття 65 Закону Чехії «Про захист класифікованої інформації та безпеку» визначає, що кожна особа зобов'язана негайно передати (повернути) знайдену секретну інформацію або секретну інформацію, отриману з порушенням нормативного порядку. Кожен, хто мав або має доступ до секретної інформації, зобов'язаний зберігати її таємницю та не допускати доступу до неї сторонніх осіб. Статті 148-156 вказаного закону встановлюють адміністративні заходи покарання для осіб, які скоїли правопорушення під час використання секретних документів або конфіденційних матеріалів, зокрема це: порушення зобов'язання зберігати конфіденційність секретної інформації; недотримання (порушення) правил криптографічного захисту інформації; сприяння в ознайомленні із секретною інформацією неуповноважених (сторонніх) осіб; здійснення експлуатаційного технічного обслуговування криптографічного пристрою для обробки секретної інформації без дотримання встановлених нормативних вимог тощо. За фактом встановлення вищевказаних правопорушень на винну особу може бути накладено адміністративний штраф у розмірі від 50 тис. до 5 млн чеських крон.

Покарання за вчинення злочинів, пов'язаних з державною таємницею, передбачені Кримінальним кодексом Чехії[84]. Стаття 230 КК встановлює покарання у вигляді позбавлення волі на строк до 3 років за несанкціонований доступ до комп'ютерної системи та несанкціоноване втручання в комп'ютерну систему чи носій інформації, зокрема який є секретним (з обмеженим доступом). Стаття 316 КК Чехії встановлює кримінальну відповідальність за шпигунство у формі перехоплення або несанкціонованого доступу до класифікованої інформації або її неправомірне використання, що може серйозно загрожувати або завдати суттєвої шкоди конституційному ладу, суверенітету, територіальній цілісності, обороні та безпеці Чеської Республіки чи іншої держави, або обороні та безпеці міжнародній організації, щодо захисту інтересів якої в зазначених вище областях опікується Чеська Республіка; за збір даних, що містять секретну інформацію або хто навмисно

[84] Zákon trestní zákoník 09.02.2009 №40/2009. URL: https://www.zakonyprolidi.cz/cs/2009-40

розкриває таку секретну інформацію іноземній державі тощо передбачається покарання у вигляді позбавлення волі на строк від 2 до 8 років.

Частина 3 статті 316 КК регламентує, що особа карається позбавленням волі на строк від 8 до 15 років у випадках, якщо: 1) особа вчинила вищевказані дії як член організації, метою якої є отримання доступу до секретної інформації; 2) таке діяння стосується секретної інформації, віднесеної до грифа «Цілком таємно»; 3) за наслідками такого діяння особа отримує істотну вигоду для себе чи іншої особи; 4) винна особа вчинила таке кримінально-карне діяння, хоча на неї спеціально покладено захист секретної інформації як уповноваженої посадової особи. Особа карається позбавленням волі на строк від 12 до 20 років, якщо вона вчинила вказані дії під час стану загрози державі або у стані війни.

Стаття 317 КК (загрози секретній інформації) передбачає кримінальну відповідальність у випадку встановлення фактів збирання класифікованої інформації з метою подальшого її розголошення або розкриття неуповноваженій (сторонній) особі, або навмисного оприлюднення (розкриття) секретної інформації карається позбавлення волі на строк до 3 років. Особа карається позбавленням волі на строк від 2 до 8 років, якщо навмисно розголошує неуповноваженій особі інформацію, яка має гриф «Цілком таємно» або «Таємно»; якщо винна особа вчинила розголошення секретної інформації, хоча її захист був спеціально покладений на неї або якщо внаслідок такого діяння винна особа одержує собі чи для іншої особи істотну вигоду або заподіює істотну шкоду державним інтересам. Частина 3 статті 317 КК встановлює, що особа карається позбавленням волі на строк від 5 до 12 років, якщо дії стосуються секретної інформації зі сфери оборонної безпеки Чеської Республіки, яка відповідно до інших правових норм має статус «Цілком таємно», або якщо вона вчиняє таке діяння в стані загрози державі або в стані війни. Стаття 318 КК встановлює, що у випадку, якщо винна особа саме з необережності скоїла розголошення секретної інформації, яка має гриф «Цілком таємно» або «Таємно», її дії карається позбавленням волі на строк до 3 років або встановленням заборони займатися певною діяльністю.

III. Висновки

Проведений аналіз демонструє, що відповідно до стандартів та нормативів НАТО і ЄС запроваджено чотирирівневу систему обмеження доступу до секретної інформації, ступені якої розподіляються за рівнем шкоди, яку може бути заподіяно інтересам країн-членів у разі розголошення класифікованих відомостей (навмисно або з необережності). 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 держав-членів НАТО і ЄС до вимог спільної політики безпеки євроатлантичного та європейського співтовариства. З цією метою на теренах НАТО і ЄС державна таємниця та службова інформація об’єднані в єдину категорію «Класифікована інформація». У стандартах безпеки НАТО та ЄС понятійно-категоріальному терміну «Класифікована інформація» еквівалентне визначення, що відповідає належному його розумінню з урахуванням традиційних та сталих форм застосування (наприклад «Засекречена інформація», «Секретна

інформація», «Інформація з обмеженим доступом»). Практична реалізація норм безпеки у внутрішньодержавному праві європейських країн відбувається шляхом інкорпорації основних принципів політики безпеки Альянсу та Євросоюзу в правове поле цих держав. 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.

Відповідно до стандартів безпеки НАТО та ЄС однією із важливих умов інтеграції держав-партнерів в загальноєвропейську систему обміну інформацією з обмеженим доступом є створення національного органу безпеки, на який покладаються функції та повноваження із забезпечення охорони державної таємниці і службової інформації. Згідно з вимогами стандартів безпеки НАТО та ЄС у державах-учасницях створюються національні органи безпеки, основною функцією яких є впровадження стандартів безпеки інформації, здійснення інспектувань умов захисту інформації з обмеженим доступом в усіх національних організаціях на всіх рівнях, забезпечення проведення перевірки з визначення надійності громадян, які потребують доступу до секретної інформації, видачу дозволів на провадження діяльності, пов'язаної з інформацією з обмеженим доступом.

Правове становище та підпорядкованість такого національного органу визначаються самостійно європейськими державами з урахуванням традиційних підходів та практики забезпечення охорони інформації з обмеженим доступом. Поширеною є також практика створення національних органів безпеки при окремих державних органах (при Міноборони – Великобританія, Естонія, Франція; при МВС – Німеччина, при РНБО – Хорватія). У деяких країнах функції національних органів безпеки покладаються на національні спецслужби (Польща, Чехія – законодавство гармонізовано зі стандартами НАТО та ЄС) (Додаток 2).

Відповідно до стандартів безпеки, окрім забезпечення виконання усіх заходів і процедур безпеки, а також контролю за охороною інформації, обмін якою здійснюється, передбачено наділення національного органу безпеки функціями з комунікаційно-інформаційної безпеки, у т.ч. і з питань технічного та криптографічного захисту інформації. Особливістю законодавства розглянутих держав є те, що не передбачається грошової компенсації особам за роботу в умовах режимних обмежень.

У кожній державі питання охорони державної таємниці та класифікованої інформації регулюються спеціальними законодавчими та підзаконними нормативними актами, які переважно засновані на вимогах та нормативах НАТО і ЄС, а також на рівні законодавства імперативно встановлено строки для організації й проведення перевірок безпеки, які коливатимуться від 3 до 6 місяців, як виключення – до одного року. Важливим аспектом є строки проведення безпекової перевірки, від яких безпосередньо залежить якість результатів перевірочних заходів. Також на власний розсуд кожна держава визначає ступені та грифи секретності.

Так, наприклад у Великобританії і Німеччині інформація з обмеженим доступом може мати *три* ступені секретності. У Франції в рамках реформування з 2021 року було введено в дію *дворівневу* систему секретності. А у Польщі, Естонії, Хорватії та Чехії існують класичні *чотири* види грифа секретності.

Узагальнення щодо строків засекречування матеріалів і даних; дії сертифіката про допуск до державної таємниці; строків здійснення перевірки для одержання допуску до державної таємниці наведено у Таблиці 3.

Табл. 3

Країна	Мінімальний строк засекречуваних відомостей та інформації, які відносяться до державної таємниці	Максимальний строк засекречуваних відомостей та інформації, які відносяться до державної таємниці	Строк дії сертифіката про допуск до державної таємниці за грифом «Цілком таємно»	Максимальний строк проведення перевірки безпеки для отримання допуску до секретної інформації
Великобританія	20 років	100 років і більше	7 років	До 6 місяців
Франція	20 років	50 років	5 років	До 6 місяців
Німеччина	5 років	50 років	5 років	До 6 місяців
Польща	5 років	довічно	5 років	До 3 місяців
Естонія	5 років	50 років	5 років	До 3 місяців
Хорватія	5 років	50 років	5 років	До 3 місяців
Чехія	5 років	довічно	5 років	До 6 місяців

Важливим питанням залишаються заходи покарання за розголошення державної таємниці або інформації з обмеженим доступом. Аналізуючи розміри й види покарання за порушення законодавства щодо розголошення державної таємниці або класифікованої інформації необхідно зробити акцент, що найсуворіші покарання передбачені Кримінальним кодексом Франції (до 15 років позбавлення волі та штраф у розмірі 225 000 євро) і Кримінальним кодексом Чехії (позбавлення волі на строк від 12 до 20 років).

Для України в умовах правового режиму воєнного стану та анонсованого реформування вітчизняної системи охорони державної таємниці та службової інформації з урахуванням висвітлених основних тенденцій розвитку охорони класифікованої інформації в 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;
- встановлення диференційованого обсягу (що відповідатиме вимогам стандартів НАТО та ЄС) безпекової перевірки громадян залежно від ступеня секретності класифікованої інформації;
- запровадження нових удосконалених підходів до визначення повноважень державних органів з функцій контролю за технічним та фізичним захистом інформації залежно від наданого грифа обмеження доступу до інформації у сфері охорони державної таємниці, що надасть змогу запобігти, своєчасно виявляти, перешкоджати протиправній діяльності іноземних спеціальних служб, спрямованій на здобування секретних відомостей, посяганням на інформацію з боку окремих недружніх країн, організацій, нелояльних співробітників чи їхніх груп;
- підвищення рівня захисту державної таємниці, а також приведення законодавства України у зазначеній сфері діяльності у відповідність до стандартів безпеки НАТО та ЄС;
- потребують перегляду підходи до забезпечення функціонування допускної системи поряд із дозвільним порядком провадження діяльності, пов'язаної з державною таємницею;
- 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 НАТО та ЄС.

Дослідницька служба
Верховної Ради України

Додаток 1

Таблиця еквівалентних класифікаційних позначень у різних країнах

(State)	Top Secret	Secret	Confidential	Restricted
Albania	Teper Sekret	Sekret	Konfidencial	I Kufizuar
Argentina	Estrictamente Secreto y Confidencial	Secreto	Confidencial	Reservado
Australia	Top Secret	Secret	Confidential	For Official Use Only
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Belgium	Zeer Geheim / Très Secret	Geheim / Secret	Vertrouwelijk / Confidentiel	Beperkte Verspreiding / Diffusion restreinte
Bolivia	Supersecreto or Muy Secreto	Secreto	Confidencial	Reservado
Bosnia and Herzegovina	Strogo povjerljivo	Tajno	Konfidencialno	Restriktivno
Brazil	Ultrassecreto	Secreto	Confidencial	Reservado
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Cambodia	Sam Ngat Bamphot	Sam Ngat Roeung	Art Kambang	Ham Kom Psay
Canada	Top Secret/Très secret	Secret/Secret	Confidential/Confidentiel	Protected A, B or C / Protégé A, B ou C
Chile	Secreto	Secreto	Reservado	Reservado
China, People's Republic of	Juémì (绝密)	Jīmì (机密)	Mìmì (秘密)	Nèibù (内部)
Colombia	Ultrasecreto	Secreto	Confidencial	Reserva del sumario
Costa Rica	Alto Secreto	Secreto	Confidencial	
Croatia	Vrlo tajno	Tajno	Povjerljivo	Ograničeno
Czech Republic	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	Yderst Hemmeligt	Hemmeligt	Fortroligt	Til Tjenestebrug Foreign Service: Fortroligt (thin Black border)
Ecuador	Secretisimo	Secreto	Confidencial	Reservado
Egypt	Sirriy lil-Ġāyah سري للغاية	Sirriy Ğiddan سري جداً	Khāṣ خاص	Maḥẓūr محظور
El Salvador	Ultra Secreto	Secreto	Confidencial	Reservado
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ethiopia	Yemiaz Birtou Mistir	Mistir	Kilkil	
European Union (EU)	TRES SECRET UE / EU TOP SECRET	SECRET UE / EU SECRET	CONFIDENTIEL UE / EU CONFIDENTIAL	RESTREINT UE / EU RESTRICTED
European Union (Western)	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED

(WEU)				
Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Finland	Erittäin salainen (TLL I)	Salainen (TLL II)	Luottamuksellinen (TLL III)	Viranomaiskäyttö (TLL IV)
France	Très secret défense	Secret défense	Confidentiel défense	Diffusion restreinte
Germany	Streng Geheim	Geheim	VS-Vertraulich	VS-Nur für den Dienstgebrauch
Greece	Άκρως Απόρρητον	Απόρρητον	Εμπιστευτικόν	Περιορισμένης Χρήσης
Guatemala	Alto Secreto	Secreto	Confidencial	Reservado
Haiti	Top Secret	Secret	Confidential	Reserve
Honduras	Super Secreto	Secreto	Confidencial	Reservado
Hong Kong	Top Secret, 高度機密	Secret, 機密	Confidential, 保密	Restricted, 內部文件/限閱文件
Hungary	Szigorúan Titkos	Titkos	Bizalmas	Korlátozott Terjesztésű
India (Hindi)	परम गुप्त (Param Gupt)	गुप्त (Gupt)	गोपनीय (Gopniya)	प्रतिबंधित/सीमित (Pratibandhit/seemit)
India (English)	Top Secret	Secret	Confidential	Restricted
Indonesia	Sangat Rahasia	Rahasia	Rahasia Dinas	Terbatas
Iran	Tabagheh-bandi-shodeh طبقه بندی شده	Mahramaneh محرمانه	Sar-be-moher سَر به مُهر	Sarbaste سَربسته
Iraq	Sirriy lil-Ġāyah سري للغاية	Sirriy سري	Khāṣ خاص	Maḥdūd محدود
Iceland	Algert Leyndarmál	Leyndarmál	Trúnaðarmál	Þjónustuskjal
Ireland (Irish language)	An-sicreideach	Sicreideach	Runda	Srianta
Israel	Sodi Beyoter סודי ביותר	Sodi סודי	Shamur שמור	Mugbal מוגבל
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Japan	Kimitsu, 機密	Gokuhi, 極秘	Hi, 秘	Toriatsukaichuui, 取り扱い注意
Jordan	Maktūm Ǧiddan مكتوم جداً	Maktūm مكتوم	Sirriy سري	Maḥdūd محدود
Korea, South	I(Il)-geup Bimil, 1급비밀	II(I)-geup Bimil, 2급비밀	III(Sam)-geup Bimil, 3급비밀	Daeoebi, 대외비
Laos	Lup Sood Gnod	Kuam Lup	Kuam Lap	Chum Kut Kon Arn
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lebanon	Tres Secret	Secret	Confidentiel	
Lithuania	Visiškai Slaptai	Slaptai	Konfidencialiai	Riboto Naudojimo
Malaysia	Rahsia Besar	Rahsia	Sulit	Terhad
Mexico	Ultra Secreto	Secreto	Confidencial	Restringido
Montenegro	Strogo Tajno	Tajno	Povjerljivo	Interno
Netherlands[30]	STG. Zeer Geheim	STG. Geheim	STG. Confidentieel	Departementaal Vertrouwelijk
New Zealand	Top Secret	Secret	Confidential	Restricted
Nicaragua	Alto Secreto	Secreto	Confidencial	Reservado

Norway	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELT	BEGRENSET
Pakistan (Urdu)	Intahai Khufia	Khufia	Sigh-e-Raz	Barai Mahdud Taqsim
Pakistan (English)	Top Secret	Secret	Confidential	Restricted
Paraguay	Secreto	Secreto	Confidencial	Reservado
Peru	Estrictamente Secreto	Secreto	Confidencial	Reservado
Philippines (English) Philippines (Tagalog)	Top Secret Matinding Lihim	Secret Mahigpit na Lihim	Confidential Lihim	Restricted Ipinagbabawal
Poland	Ściśle tajne	Tajne	Poufne	Zastrzeżone
Portugal	Ultrassecreto	Secreto	Confidencial	Reservado
Romania	Strict Secret de Importanţă Deosebită	Strict Secret	Secret	Secret de serviciu
Saudi Arabia	Saudi Top Secret	Saudi Very Secret	Saudi Secret	Saudi Restricted
Serbia	Latin: Državna tajna Cyrillic: Државна тајна	Latin: Strogo poverljivo Cyrillic: Строго поверљиво	Latin: Poverljivo Cyrillic: Поверљиво	Latin: Interno Cyrillic: Интерно
Singapore	Top Secret	Secret	Confidential	Restricted
Slovak Republic	Prísne tajné	Tajné	Dôverné	Vyhradené
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Spain	Secreto	Reservado	Confidencial	Difusión Limitada
Sweden	Kvalificerat Hemlig (KH); Hemlig/Top Secret (H/TS)	Hemlig (H); Hemlig/Secret H/S)	Hemlig/Confidential (H/C)	Hemlig/Restricted (H/R)
Switzerland		GEHEIM / SECRET	VERTRAULICH / CONFIDENTIEL	INTERN / INTERNE
Taiwan (Republic of China)	"Absolutely" Secret (絕對機密)	"Extremely" Secret (極機密)	Secret (機密)	no direct equivalent
Tanzania (Swahili)	SIRI KUU	SIRI	STIRI	IMEZUILIWA
Thailand	Lap thi sut (ลับที่สุด)	Lap mak (ลับมาก)	Lap (ลับ)	Pok pit (ปกปิด)
Turkey	Çok Gizli	Gizli	Özel	Hizmete Özel
South Africa (English)	Top Secret	Secret	Confidential	Restricted
South Africa (Afrikaans)	Uiters Geheim	Geheim	Vertroulik	Beperk
Ukraine	Особливої важливості	Цілком таємно	Таємно	Для службового користування
United Kingdom	TOP SECRET	SECRET	OFFICIAL (formerly CONFIDENTIAL)	OFFICIAL (formerly RESTRICTED)

United States	Top Secret	Secret	Confidential	For Official Use Only
Uruguay	Ultra Secreto	Secreto	Confidencial	Reservado
Vietnam	Tuyệt Mật	Tối Mật	Mật	Phổ Biến Hạn Chế

Додаток 2

Країна	Уповноважений орган, на який покладено функції із забезпечення державної таємниці та службової інформації		Джерело
	Назва українською мовою	**Назва мовою оригіналу**	
Великобританія	Рада національної безпеки	National Security Council	https://www.gov.uk/government/groups/national-security-council
	Управління військової розвідки	Defence Intelligence	https://www.gov.uk/guidance/defence-intelligence
	Лабораторія оборонної науки і техніки	Defence Science and Technology Laborator	https://www.gov.uk/government/organisations/defence-science-and-technology-laboratory
Франція	Генеральний секретаріат національної оборони та безпеки	Secrétariat général de la défense et de la sécurité nationale	https://www.sgdsn.gouv.fr/
	Національне агентство безпеки інформаційних систем	Agence nationale de la sécurité des systèmes d'information	https://cyber.gouv.fr/
	Управління державної охорони та безпеки	La direction de la protection et de la sécurité de l'Etat	https://www.sgdsn.gouv.fr/notre-organisation/composantes/protection-et-securite-de-letat
	Департамент з питань захисту таємниці національної оборони	Sous-direction de la protection et de la sécurité de défense nationale	https://lannuaire.service-public.fr/gouvernement/5f04919e-04e5-4ced-91ba-b6a7f29a3b4a
Німеччина	Федеральне відомство охорони конституції	Bundesamt für Verfassungsschutz	https://www.verfassungsschutz.de/DE/home/home_node.html
	Федеральне міністерство оборони	Bundesministerium der Verteidigung	https://www.bmvg.de/de
	Військова контррозвідувальна служба	Der Militärische Abschirmdienst	https://www.bundeswehr.de/de/organisation/weitere-bmvg-dienststellen/mad-bundesamt-fuer-den-militaerischen-abschirmdienst
Польща	Агентство внутрішньої безпеки	Agencję Bezpieczeństwa Wewnętrznego	https://www.abw.gov.pl/
	Служба військової контррозвідки	Służbę Kontrwywiadu Wojskowego	https://www.skw.gov.pl/

Естонія	Агентство оборонної поліції	Kaitsepolitseiamet	https://kapo.ee/
Хорватія	Управління Офісу Ради національної безпеки і оборони	Ured Vijeća za nacionalnu sigurnost	https://www.uvns.hr/hr
Чехія	Агенція національної безпеки	Národní bezpečnostní úřad	https://www.nbu.cz/
	Національне управління з питань кібернетичної та інформаційної безпеки	Národní úřad pro kybernetickou a informační bezpečnost	https://nukib.gov.cz/