

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ  
ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ**

**С. П. ПЕКАРСЬКИЙ**

**РЕЖИМ  
СЕКРЕТНОСТІ**

**НАВЧАЛЬНИЙ ПОСІБНИК**

Київ  
Дакор  
2021

УДК 351.74:005.332.5

П24

*Рекомендовано до друку та використання в освітньому процесі  
Вченою радою Донецького юридичного інституту МВС України  
(протокол № 10 від 31.03.2021 р.)*

**Рецензенти:**

*Бабенко А. М. – професор кафедри кримінального права та кримінології  
Одеського державного університету внутрішніх справ, доктор юридичних наук,  
професор;*

*Свір П. В. – начальник управління карного розшуку ГУ НП в Донецькій  
області, полковник поліції, кандидат юридичних наук.*

**Пекарський С.П.**

Режим секретності : навчальний посібник / С. П. Пекарський. – Київ:  
ВД «Дакор», 2021. 144 с.

ISBN 978-617-7679-98-0

У навчальному посібнику висвітлено сутність та правові засади режиму секретності; основні вимоги щодо дотримання режиму секретності; порядок роботи з матеріальними носіями, які містять інформацію з обмеженим доступом. Визначено особливості контролю за дотриманням режиму секретності та підстави відповідальності за порушення вимог єдиного порядку забезпечення охорони державної таємниці.

Посібник містить навчально-методичні матеріали, перелік питань для самоконтролю знань, тестові завдання, словник термінів, список рекомендованої літератури, які допоможуть здобувачам вищої освіти закладів вищої освіти системи МВС України, практичним працівникам ознайомитися з комплексом заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв.

Навчальний посібник «Режим секретності» призначений для здобувачів вищої освіти закладів вищої освіти системи МВС України, практичних працівників правоохоронних органів та науковців.

© Пекарський С. П., 2021

© ДонДУВС, 2021

© ТОВ «ВД «Дакор», 2021

## ЗМІСТ

<b>Вступ</b> .....	5
<b>§ 1. Режим секретності як навчальна дисципліна</b> .....	6
<b>§ 2. Поняття, сутність, призначення режиму секретності</b> .....	10
2.1. Поняття, сутність державної таємниці.....	10
2.2. Поняття та призначення режиму секретності.....	17
<b>§ 3. Правове регулювання режиму секретності</b> .....	20
3.1. Законодавче забезпечення режиму секретності.....	20
3.2. Звід відомостей, що становлять державну таємницю.....	22
3.3. Нормативно-правове забезпечення режиму секретності.....	27
<b>§ 4. Допуск та доступ громадян до секретних робіт і документів</b> .....	30
4.1. Підстави та порядок оформлення допуску і доступу до секретних робіт і документів.....	30
4.2. Основні обов'язки працівників, допущених до роботи, пов'язаної з державними таємницями.....	35
4.3. Основні обмеження прав для працівників, допущених до роботи, пов'язаної з державними таємницями.....	36
<b>§ 5. Організація забезпечення режиму секретності</b> .....	38
5.1. Режимно-секретні органи .....	38
5.2. Режимно-секретні підрозділи МВС України та Національної поліції України.....	43
5.3. Загальні положення щодо здійснення секретного діловодства.....	46
5.4. Загальні положення Правил пропускового режиму.....	47
<b>§ 6. Порядок роботи з документами та іншими матеріальними носіями інформації, що містять службову інформацію</b> .....	52
<b>§ 7. Віднесення інформації до державної таємниці. Засекречування та розсекречення матеріальних носіїв секретної інформації</b> .....	71
7.1. Віднесення інформації до державної таємниці.....	71

7.2. Державний експерт з питань таємниць: його права та обов'язки.....	72
7.3.Засекречування та розсекречування матеріальних носіїв секретної інформації .....	77
<b>§ 8. Сутність та порядок забезпечення контролю за режимом секретності.....</b>	<b>80</b>
8.1. Контроль за дотриманням режиму секретності.....	80
8.2. Контроль за технічним захистом інформації, яку віднесено до державної таємниці в органах і підрозділах Національної поліції України.....	83
<b>§ 9. Відповідальність за порушення режиму секретності.....</b>	<b>90</b>
9.1. Загальні підстави притягнення до відповідальності за порушення режиму секретності.....	90
9.2. Адміністративна відповідальність за порушення режиму секретності.....	93
9.3. Кримінальна відповідальність за порушення режиму секретності .....	95
<b>§ 10. Контроль успішності.....</b>	<b>102</b>
10.1. Діагностика успішності з навчальної дисципліни .....	102
10.2. Тестові завдання.....	103
10.3. Завдання для самоконтролю знань .....	118
<b>Висновки.....</b>	<b>122</b>
<b>Список використаних джерел.....</b>	<b>125</b>
<b>Додатки.....</b>	<b>129</b>

## ВСТУП

Сучасний розвиток українського суспільства характеризується впровадженням інформаційних технологій у різноманітні сфери життя. Це створює перспективи для використання інформаційних технологій і в освітньому процесі закладів вищої освіти системи Міністерства внутрішніх справ України. Розвиток та реформування всіх сторін сучасного життя суспільства супроводжується стрімким зростанням інформаційного обміну, впровадженням передових інформаційних технологій в усі його сфери. Окремий вид інформації охоплює відомості, що становлять державну таємницю. Їх розголошення може завдати шкоди національній безпеці України.

Статтею 19 Конституції України визначено, що правовий порядок в Україні ґрунтується на засадах, відповідно до яких ніхто не може бути примушений робити те, що не передбачено законодавством. Тому органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, у межах повноважень та у спосіб, що передбачені Конституцією та законами України. Отже, питання, пов'язані з охороною державної таємниці, забезпеченням режиму секретності в діяльності державних та правоохоронних органів є актуальними, особливо в період боротьби за незалежність та територіальну цілісність України. На нашу думку, зазначені процеси вимагають наукового обґрунтування і правового забезпечення захисту інформаційної, державної та національної безпеки України.

Ці аспекти необхідно враховувати під час підготовки навчально-методичних матеріалів для навчальної дисципліни «Режим секретності», яка вивчає питання, що стосуються єдиного порядку забезпечення охорони державної таємниці в практичній діяльності державних та правоохоронних органів. Навчальний посібник «Режим секретності» створено на базі чинних законодавчих актів, що регламентують суспільні відносини, пов'язані зі збереженням державної таємниці, та чинних нормативних актів, які мають відкритий характер. Це, у свою чергу, надасть можливість ознайомитися із загальними правилами забезпечення режиму секретності в повсякденній діяльності працівника Національної поліції України.

## § 1. РЕЖИМ СЕКРЕТНОСТІ ЯК НАВЧАЛЬНА ДИСЦИПЛІНА

Аналіз норм, що містяться в законодавчих та підзаконних нормативно-правових актах, які регламентують питання державної таємниці, потребують вивчення та постійного дотримання вимог зі збереження державної таємниці працівниками у їх практичній діяльності. З метою підвищення якості надання освітніх послуг зі спеціальних дисциплін, рівня підготовки фахівців необхідно створювати, розвивати та впроваджувати навчальні посібники в освітній процес (дотримуючись при цьому вимог до збереження державної таємниці) й розповсюджувати передові інформаційні технології та результати наукових досліджень серед практичних підрозділів Національної поліції України.

Перед тим як розпочати вивчення курсу «Режим секретності», необхідно наголосити на важливості цього навчального предмета. Міністерство внутрішніх справ України (далі – МВС України), Національна поліція України (далі – НП України) постійно звертають увагу працівників поліції на необхідність дотримання високої професійної пильності в цей складний для держави період розвитку, пов'язаний із захистом незалежності та територіальної цілісності. Уміння зберігати державну і службову таємниці завжди викликало повагу громадян до працівників поліції. Це пояснюється тими специфічними завданнями, які доводиться розв'язувати працівникам поліції.

У процесі службової діяльності співробітники Національної поліції України, особливо підрозділи кримінальної поліції, органи досудового розслідування, працюють з інформацією, яка не підлягає широкому розповсюдженню. Ця інформація, віднесена законодавством до категорії державної таємниці, стосується окремих форм, методів, прийомів і результатів діяльності щодо розв'язання завдань протидії кримінальним правопорушенням, зміцнення правопорядку. Розголошення, втрата такої інформації, а також відомостей про заходи, які плануються і здійснюються щодо забезпечення особистої та публічної безпеки і комплексної протидії правопорушенням, порушують їх нормальну діяльність, що значно знижує її ефективність.

З огляду на те, що злочинні елементи активно вживають заходи розвідувального характеру, спрямовані на з'ясування стратегічних і поточних планів діяльності правоохоронних органів, Міністерство внутрішніх справ України, територіальні та міжрегіональні територіальні підрозділи Національної поліції України приділяють серйозну увагу вихованню у співробітників високої пильності, здійснюють різноманітні заходи, щоб забезпечити збереження відомостей, що становлять державну таємницю. Значна роль відведена навчанню співробітників підрозділів правилам виконання секретних робіт, поводження з матеріальними носіями секретної та службової інформації. Кожен працівник поліції зобов'язаний чітко знати вимоги законів, наказів, інструкцій та інших нормативних документів, що регулюють режим секретності, а також дотримуватися у своїй діяльності з протидії правопорушенням.

Так, під час розробки методичних матеріалів необхідно враховувати, що інформаційна безпека як невід'ємний складник національної безпеки з часів незалежності України набула важливого суспільного значення, тому постійно перебуває в полі зору вчених і практиків, які займаються питаннями, пов'язаними із забезпеченням державної таємниці. Організація освітнього процесу в закладах вищої освіти зі специфічними умовами навчання, які входять до сфери управління МВС України, вимагає впровадження навчальних посібників, що можуть бути доступними для здобувачів вищої освіти та сприятимуть поліпшенню результатів їх самостійної роботи під час вивчення спеціальних навчальних дисциплін.

Освіта в системі МВС України покликана сформувати в особи в процесі здобуття вищої освіти систему професійних, світоглядних і громадянських якостей, зумовлену цілями та потребами особи й суспільства в ефективній правоохоронній та правозастосовній діяльності. Освітній процес здійснюється на підставі вимог Конституції України, законів України «Про освіту», «Про вищу освіту», «Про Національну поліцію», стандартів вищої освіти, нормативних актів Міністерства освіти і науки України, Міністерства внутрішніх справ України, Національної поліції, Служби безпеки та інших нормативно-правових актів з питань освіти.

Вивчення навчальної дисципліни надає здобувачу вищої освіти визначити:

- роль і значення відповідної навчальної дисципліни в підготовці та майбутній професійній діяльності фахівця;
- основні риси освітньої та науково-творчої діяльності, необхідні для успішної роботи фахівця;
- характер навчально-пізнавальних проблем і завдань, що сприяють формуванню цих рис;
- найважливіші світоглядні ідеї та категорії, які підлягають засвоєнню на конкретній змістовій основі;
- зміст навчання з дисципліни;
- очікувані результати навчання, тобто систему вмінь, якими повинні оволодіти курсанти та курсантки (слухачі та слухачки), а також рівні їх сформованості.

Тому загальною метою навчального курсу є підготовка фахівців для МВС України та Національної поліції України, а також інших галузей правової системи держави шляхом забезпечення умов, необхідних для здобуття особою вищої освіти. Саме тому навчальна дисципліна «Режим секретності» має три мети: загальноосвітню, правознавчу і практичну.

Загальноосвітнє значення запропонованої навчальної дисципліни пов'язане з необхідністю підвищення загальної правової культури курсантів та курсанток (слухачів та слухачок) – майбутніх правоохоронців, правознавців, фахівців у галузях права, правоохоронної діяльності та вивчення ними регламентованих правил щодо дотримання державної та службової таємниці.

Правознавча мета навчальної дисципліни полягає в здобутті юридичних знань про державну та службову таємниці, а також про організацію регулювання суспільних відносин у сфері державної та службової таємниці, у т. ч. їх правовий захист з боку держави.

Практична мета навчальної дисципліни пов'язана з вивченням режиму секретності та порядку:

- допуску та доступу до секретних робіт і документів;
- роботи з матеріалами обмеженого грифа користування;
- дотримання вимог перебування в режимних приміщеннях.

Завдання навчальної дисципліни:

- підвищити правосвідомість курсантів та курсанток (слухачів та слухачок) як представників правоохоронних органів;
- сформувати основні навички роботи з матеріалами обмеженого грифа користування;
- дати здобувачам та здобувачкам вищої освіти знання щодо дотримання режиму секретності у процесі навчання, вивчення навчальних дисциплін з обмеженим грифом користування та в подальшій практичній роботі як працівників практичних органів і підрозділів Національної поліції.

Предметом курсу є правовий механізм установаження порядку дотримання режиму секретності в органах і підрозділах Національної поліції, державний захист цих суспільних відносин, особливості поведінки працівників під час роботи в режимних приміщеннях та з матеріалами обмеженого грифа користування.

Під час вивчення навчальної дисципліни «Режим секретності» простежуються міжпредметні зв'язки з іншими дисциплінами: теорією держави та права, інформаційним правом, кримінальним правом, адміністративним правом, оперативно-розшуковою діяльністю, оперативно-розшуковим документуванням та іншими, вивчення яких спрямоване на підготовку висококваліфікованих фахівців спеціальностей 081 «Право» та 262 «Правоохоронна діяльність» першого (бакалаврського) рівня вищої освіти, здатних розв'язувати складні спеціалізовані задачі і практичні проблеми правоохоронної діяльності, що характеризуються комплексністю та невизначеністю умов.

## **§ 2. ПОНЯТТЯ, СУТНІСТЬ, ПРИЗНАЧЕННЯ РЕЖИМУ СЕКРЕТНОСТІ**

### **2.1. Поняття, сутність державної таємниці**

Конституцією України проголошено Україну правовою державою, для якої людина, її життя і здоров'я, честь і гідність, недоторканність і безпека є найвищою соціальною цінністю. Розвиток та реформування всіх сторін сучасного життя суспільства супроводжується стрімким зростанням інформаційного обміну, впровадженням передових інформаційних технологій у всі його сфери. Окремий вид такої інформації охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, що становлять державну таємницю. Розголошення цих відомостей може завдати шкоди національній безпеці України.

Зазначені процеси вимагають наукового обґрунтування й правового забезпечення проблеми оптимального співвідношення інтересів особистості, суспільства, держави, приватних і публічних засад, визначення підстав та меж втручання у сферу приватного й особистого інтересу, захисту інформаційної, державної та національної безпеки України. Інформаційна безпека як невід'ємний складник національної безпеки з часів незалежності України набула важливого суспільного значення і тому постійно перебуває у полі зору вчених і практиків, які займаються питаннями, пов'язаними із забезпеченням державної таємниці.

На важливості цього питання наголошено в Конституції України, у ст. 17 якої зазначено, що захист інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу.

Здійснюючи теоретичний аналіз досліджуваних суспільних відносин, автор дійшов висновку про закріплення в законодавчих актах та відповідне регулювання таємниць, пов'язаних з різною професійною діяльністю.

Отже, до таємниць, пов'язаних з професійною діяльністю належать:

- **адвокатська таємниця** – будь-яка інформація, що стала відома адвокату, помічнику адвоката, стажисту адвоката, особі, яка перебуває у трудових відносинах з адвокатом, про клієнта, а також питання, з яких клієнт (особа, якій відмовлено в укладенні договору про надання правової допомоги з передбачених Законом України «Про адвокатуру та адвокатську діяльність» підстав) звертався до адвоката, адвокатського бюро, адвокатського об'єднання, зміст порад, консультацій, роз'яснень адвоката, складені ним документи, інформація, що зберігається на електронних носіях, та інші документи і відомості, одержані адвокатом під час здійснення адвокатської діяльності (ст. 22 Закону України «Про адвокатуру та адвокатську діяльність»);
- **банківська таємниця** – інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам під час надання послуг банку (ст. 60 Закону України «Про банки і банківську діяльність»);
- **військова таємниця** – відомості військового характеру, предмети, документи або матеріали, що містять відомості військового характеру, які становлять державну таємницю (ст. 422 Кримінального кодексу України);
- **журналістська таємниця** – журналіст має право на збереження таємниці авторства та джерел інформації, за винятком випадків, коли ці таємниці обнародуються на вимогу суду (п. 11 ст. 26 Закону України «Про друковані засоби масової інформації (пресу) в Україні»);
- **комерційна таємниця** – інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці (ст. 505 Цивільного кодексу України);

- **лікарська таємниця** – медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків. Під час використання інформації, що становить лікарську таємницю, в навчальному процесі, науково-дослідній роботі, у тому числі у випадках її публікації у спеціальній літературі, повинна бути забезпечена анонімність пацієнта (ст. 40 Закону України «Основи законодавства України про охорону здоров'я»);
- **нотаріальна таємниця** – сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, в тому числі про особу, її майно, особисті майнові та немайнові права і обов'язки тощо (ст. 8 Закону України «Про нотаріат»);
- **публічна інформація з обмеженим доступом** – інформацією з обмеженим доступом є:
  - 1) конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов (ст. 7 Закону України «Про доступ до публічної інформації»);
  - 2) таємна інформація – інформація, доступ до якої обмежується відповідно до частини другої статті 6 Закону України «Про доступ до публічної інформації», розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю (ст. 8 Закону України «Про доступ до публічної інформації»);

3) службова інформація – відповідно до вимог частини другої статті 6 Закону України «Про доступ до публічної інформації» до службової може належати така інформація:

3.1. що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

3.2. зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці;

- **розвідувальна таємниця** – вид таємної інформації, що охоплює відомості та дані, отримані або створені розвідувальними органами України під час виконання покладених на ці органи завдань та здійснення функцій, визначених Законом України «Про розвідку», розголошення яких може завдати шкоди функціонуванню розвідки і доступ до яких обмежено відповідно до Закону України «Про розвідку» в інтересах національної безпеки України (ст. 1 Закону України «Про розвідку»);
- завдання сертифікаційної роботи зовнішнього незалежного оцінювання належить до інформації з обмеженим доступом з моменту створення набору завдань сертифікаційної роботи зовнішнього незалежного оцінювання та до моменту його санкціонованого використання особами, що проходять зовнішнє незалежне оцінювання. У разі потреби спеціально уповноважена державою установа (організація) може відносити зміст завдань сертифікаційної роботи до інформації з обмеженим доступом на більш тривалий період часу (п. 8 ст. 45 Закону України «Про вищу освіту»);
- **таємниця досудового розслідування** – відомості досудового розслідування можна розголошувати лише з письмового дозволу слідчого або прокурора і в тому обсязі, в якому вони визнають можливим. Слідчий, прокурор попереджає осіб, яким стали відомі відомості досудового розслідування, у зв'язку з участю в ньому, про

їх обов'язок не розголошувати такі відомості без його дозволу (ст. 222 Кримінального процесуального кодексу України (далі – КПК України));

- **таємниця наради суддів** – під час ухвалення вироку ніхто не має права перебувати в нарадчій кімнаті (нарадча кімната – приміщення, спеціально призначене для ухвалення судових рішень. – *Прим. автора*), крім складу суду, який здійснює судовий розгляд. Суд наділено правом перервати нараду лише для відпочинку з настанням нічного часу. Під час перерви судді не можуть спілкуватися з особами, які брали участь у кримінальному провадженні. Судді не мають права розголошувати хід обговорення та ухвалення вироку в нарадчій кімнаті (ст. 367 КПК України);
- **таємниця нарадчої кімнати** – під час ухвалення судового рішення ніхто не має права перебувати в нарадчій кімнаті, крім складу суду, який розглядає справу. Під час перебування в нарадчій кімнаті суддя не має права розглядати інші судові справи. Судді не мають права розголошувати хід обговорення та ухвалення рішення у нарадчій кімнаті (ст. 245 Цивільного процесуального кодексу України, ст. 228 Кодексу адміністративного судочинства України);
- **таємниця сповіді** – кожному громадянину в Україні гарантується право на свободу совісті, ніхто не має права вимагати від священнослужителів відомостей, одержаних ними під час сповіді віруючих (ст. 3 Закону України «Про свободу совісті та релігійні організації»);
- **таємниця усиновлення** – особа має право на таємницю перебування на обліку тих, хто бажає усиновити дитину, пошуку дитини для усиновлення, подання заяви про усиновлення та її розгляду, рішення суду про усиновлення. Дитина, яка усиновлена, має право на таємницю, в тому числі і від неї самої, факту її усиновлення (ст. 226 Сімейного кодексу України).

Визначившись з видами таємниць, пов'язаних з професійною діяльністю, перейдемо до аналізу норм, що містяться в законодавчих та підзаконних нормативно-правових актах різних міністерств та відомств, які регламентують

питання державної таємниці. Перш ніж з'ясувати значення терміна «режим секретності», необхідно дати тлумачення поняттю «державна таємниця».

Закон України «Про державну таємницю» від 21 січня 1994 року № 3855-ХІІ регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. Цим законом визначено термін «державна таємниця». Отже, державна таємниця (або секретна інформація) – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані в порядку, встановленому цим законом, державною таємницею і підлягають охороні державою.

У свою чергу, Законом України «Про інформацію» від 2 жовтня 1992 року № 2657-ХІІ розкрито загальне значення поняття інформації, інформаційної діяльності, джерел інформації і режиму доступу до неї та «таємної» інформації. Згідно з цим законом інформацію розуміють як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі. Також цим законом визначена державна інформаційна політика (ст. 6 зазначеного закону) як сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації. Головними напрямками і способами державної інформаційної політики є:

- 1) забезпечення доступу громадян до інформації;
- 2) створення національних систем і мереж інформації;
- 3) зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності;
- 4) забезпечення ефективного використання інформації;
- 5) сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів;
- 6) створення загальної системи охорони інформації;
- 7) сприяння міжнародному співробітництву в галузі інформації;
- 8) гарантування інформаційного суверенітету України;

9) сприяння задоволенню інформаційних потреб закордонних українців.

Державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції. Закон України «Про інформацію» регламентує питання, пов'язані з режимом доступу до інформації (ст. 28), який слід розуміти як передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації. За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Держава здійснює контроль за режимом доступу до інформації. Завдання контролю за режимом доступу до інформації полягає у забезпеченні додержання вимог законодавства про інформацію всіма державними органами, підприємствами, установами та організаціями, недопущенні необґрунтованого віднесення відомостей до категорії інформації з обмеженим доступом. Державний контроль за додержанням установленого режиму здійснюється спеціальними органами, які визначають Верховна Рада України і Кабінет Міністрів України. У порядку контролю Верховна Рада України може вимагати від урядових установ, міністерств, відомств звіти, які містять відомості про їх діяльність із забезпечення інформацією заінтересованих осіб (кількість випадків відмови в наданні доступу до інформації із зазначенням мотивів таких відмов, кількість та обґрунтування застосування режиму обмеженого доступу до окремих видів інформації; кількість скарг на неправомірні дії посадових осіб, які відмовили в доступі до інформації, та вжиті щодо них заходи тощо).

Стаття 29 Закону України «Про інформацію» регламентує доступ до відкритої інформації, який забезпечується шляхом:

- систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках);
- поширення її засобами масової комунікації;
- безпосереднього її надання заінтересованим громадянам, державним органам та юридичним особам.

Порядок та умови надання громадянам, державним органам, юридичним особам і представникам громадськості відомостей за запитом встановлюються законодавством України або договорами (угодами), якщо надання інформації

здійснюється на договірній основі. Обмеження права на одержання відкритої інформації забороняється законом. Переважним правом на одержання інформації користуються громадяни, яким ця інформація необхідна для виконання своїх професійних обов'язків.

## **2.2. ПОНЯТТЯ ТА ПРИЗНАЧЕННЯ РЕЖИМУ СЕКРЕТНОСТІ**

Особливої уваги потребує інформація з обмеженим доступом. Інформація з обмеженим доступом (ст. 30 Закону України «Про інформацію») за своїм правовим режимом поділяється на конфіденційну і таємну. Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ – надано статус конфіденційної. Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначається Кабінетом Міністрів України. До конфіденційної інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, не можуть бути віднесені відомості:

- 1) стосовно стану справ із правами і свободами людини і громадянина, а також фактів їх порушень;
- 2) про стан довкілля, якість харчових продуктів і предметів побуту;
- 3) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;
- 4) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

б) інша інформація, доступ до якої відповідно до законів України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути обмеженим.

Законодавець України, продовжуючи нормотворчу діяльність у Законі України «Про державну таємницю», більш детально регламентує питання, пов'язані з віднесенням інформації до державної таємниці. Під віднесенням інформації до державної таємниці слід розуміти процедуру прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу. Тому грифом секретності є реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації.

Охорона державної таємниці – це комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв. І тому «режим секретності» слід розуміти як установлений згідно з вимогами Закону України «Про державну таємницю» та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці.

Отже, «режим секретності в Національній поліції України» варто визначати як встановлений відповідно до вимог Закону України «Про державну таємницю» та інших законодавчих і нормативних актів вищих органів державної влади й управління єдиний порядок забезпечення охорони державної таємниці в процесі повсякденної діяльності органів / підрозділів Національної поліції, що включає в себе системи адміністративно-правових, організаційних, інженерно-технічних, криптографічних та інших заходів. До основних заходів забезпечення охорони державної таємниці належать:

- правила віднесення відомостей до державної таємниці;

- вимоги, що ставляться до осіб, які допускаються до особливої важливості, цілком таємних і таємних відомостей, документів, виробів і робіт;
- встановлений порядок допуску співробітників Національної поліції України до державної таємниці та іншої інформації обмеженого поширення;
- чітка нормативна регламентація (особливий режим) діяльності, пов'язаної з державною таємницею;
- певний порядок ведення таємного діловодства;
- державний і відомчий контроль за дотриманням встановленого порядку збереження і використання державних таємниць;
- відповідальність за порушення режиму секретності.

#### Призначення режиму секретності:

- обмеження доступу до державної таємниці осіб, які не мають відповідної форми;
- запобігання витоку або втраті таємної інформації;
- виховання у працівників сумлінного і пильного ставлення до виконання службових обов'язків;
- навчання працівників правил роботи з інформацією, документами, спеціальною літературою;
- забезпечення прихованості й раптовості, внаслідок чого зростає ефективність проведених оперативно-розшукових, розвідувальних, контррозвідувальних, негласних слідчих (розшукових) та інших заходів, здійснюваних правоохоронними та розвідувальними органами під час виконання покладених на них завдань.

## **§ 3. ПРАВОВЕ РЕГУЛЮВАННЯ РЕЖИМУ СЕКРЕТНОСТІ**

### **3.1. ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ РЕЖИМУ СЕКРЕТНОСТІ**

Правові засади режиму секретності становлять:

- конституційні положення про суверенітет та інформаційну безпеку України;
- міжнародні договори, згода на обов'язковість яких надана Верховною Радою України;
- кодекси України, які регламентують юридичну відповідальність – Кодекс України про адміністративні правопорушення, Кримінальний кодекс України;
- закони України;
- підзаконні нормативно-правові акти – укази Президента України, постанови Кабінету Міністрів України, нормативні акти Служби безпеки України (далі – СБУ), МВС України та НП України.

Під час аналізу державної таємниці, режиму секретності нами попередньо було зауважено, що вони регламентуються законами України та відомчими нормативними актами, що і становить їхню правову основу.

Основним законодавчим актом, який встановлює суспільні відносини у сфері державної таємниці, є Закон України «Про державну таємницю». Відповідно до його положень відносини у сфері охорони державної таємниці регулюються Конституцією України, законами України «Про інформацію», «Про доступ до публічної інформації», міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України та іншими нормативно-правовими актами.

Дія Закону України «Про державну таємницю» поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші державні органи, у тому числі територіальні органи центрального органу виконавчої влади, що реалізує державну митну політику, та центрального органу

виконавчої влади, що реалізує державну податкову політику, утворені як відокремлені підрозділи центрального органу виконавчої влади без статусу юридичної особи, Верховну Раду Автономної Республіки Крим, Раду міністрів Автономної Республіки Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі – державні органи, органи місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці. До того ж передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим законом. У разі, якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші, ніж передбачені цим законом, правила охорони таємниці іноземної держави чи міжнародної організації, то застосовуються правила міжнародного договору України.

Відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації регулює Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-ХІІ. Відповідно до положень цього закону основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Закон України «Про доступ до публічної інформації» від 13 січня 2011 року № 2939-VI визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим законом, та інформації, що становить суспільний інтерес. Указаний закон регламентує питання поводження з публічною інформацією з обмеженим доступом, до якої відносить конфіденційну інформація, таємну інформацію та службову інформацію.

До законів, які регламентують питання, пов'язані державною таємницею та дотриманням режиму таємності, належать такі:

- Про Національну поліцію : Закон України від 2 липня 2015 року № 580-VIII;
- Про Дисциплінарний статут Національної поліції України : Закон України від 15 березня 2018 року № 2337-VIII;

- Про Службу безпеки України : Закон України від 25 березня 1992 року № 2229-XII (редакція від 03.07.2020);
- Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 року № 2135-XII;
- Про розвідку : Закон України від 17 вересня 2020 року № 912-IX;
- Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР;
- Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23 лютого 2006 року № 3475-IV;
- Про Національну систему конфіденційного зв'язку : Закон України від 10 січня 2002 року № 2919-III;
- інші законодавчі акти.

**Кодекси України:**

- Кримінальний кодекс України (статті 328, 329, 330, 422) від 5 квітня 2001 року № 2341-III;
- Кримінальний процесуальний кодекс України (глава 40) від 13 квітня 2012 року № 4651-VI;
- Кодекс України про адміністративні правопорушення (статті 255, 212-2, 212-5, 212-6) від 07 грудня 1984 року.

### **3.2. ЗВІД ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ ДЕРЖАВНУ ТАЄМНИЦЮ**

Звід відомостей, що становлять державну таємницю (далі – ЗВДТ) – це акт, у якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених Законом України «Про державну таємницю» сферах.

Стаття 12 Закону України «Про державну таємницю» регулює питання, пов'язані з формуванням Зводу відомостей, що становлять державну таємницю. На підставі проведеного теоретичного аналізу нами встановлено, що ЗВДТ формує Служба безпеки України на підставі рішень державних експертів з питань таємниць. Зазначений Звід та зміни до нього набирають чинності з моменту опублікування в офіційних виданнях України.

Зміни до Зводу відомостей, що становлять державну таємницю, вносяться не пізніше трьох місяців з дня одержання Службою безпеки України відповідного рішення державного експерта з питань таємниць. Безпосередньо зразки форм рішень державних експертів з питань таємниць, порядок та механізм формування ЗВДТ і його опублікування визначаються Кабінетом Міністрів України.

На підставі та в межах ЗВДТ з метою конкретизації та систематизації даних про секретну інформацію державні органи створюють галузеві або відомчі розгорнуті переліки відомостей, що становлять державну таємницю, а також можуть створювати міжгалузеві або міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю.

Підприємства, установи та організації незалежно від форм власності, що провадять діяльність, пов'язану з державною таємницею, за ініціативою та погодженням із замовником робіт, пов'язаних з державною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю. Такі переліки погоджуються із Службою безпеки України, затверджуються державними експертами з питань таємниць та реєструються у Службі безпеки України.

Зазначаємо, що розгорнуті переліки відомостей, що становлять державну таємницю підприємств, установ та організацій незалежно від форм власності, що провадять діяльність, пов'язану з державною таємницею, не можуть суперечити Зводу відомостей, що становлять державну таємницю. У разі включення до ЗВДТ або до розгорнутих переліків цих відомостей інформації, яка не відповідає категоріям і вимогам, передбаченим ст. 8 Закону України «Про державну таємницю», або порушення встановленого порядку віднесення інформації до державної таємниці заінтересовані громадяни та юридичні особи мають право оскаржити відповідні рішення до суду. З метою недопущення розголошення державної таємниці судовий розгляд скарг може проводитися в закритих засіданнях відповідно до закону.

Інформація вважається державною таємницею з більш високим чи нижчим ступенем секретності або такою, що не становить державної таємниці, з часу опублікування відповідних змін до Зводу відомостей, що становлять державну таємницю.

Саме тому, відповідно до статей 10–12 Закону України «Про державну таємницю», Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого Постановою Кабінету Міністрів України від 18 грудня 2013 року № 939, наказом Служби безпеки України від 23.12.2020 № 383 затверджено Звід відомостей, що становлять державну таємницю.

ЗВДТ визначає відомості, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у встановлених законодавством сферах:

- оборони;
- економіки, науки і техніки;
- зовнішніх відносин;
- державної безпеки та охорони правопорядку.

З урахуванням парадигми правоохоронної діяльності, пов'язаної з державною таємницею, слід на прикладі сфери державної безпеки та охорони правопорядку вказати на структуру ЗВДТ.

У першій частині ЗВДТ наведена відповідна аббревіатура й терміни. У другій частині у вигляді таблиці зазначені відомості, що становлять державну таємницю, зокрема у сфері державної безпеки та охорони правопорядку.

У таблиці використано такі скорочення:

ГУР – Головне управління розвідки Міністерства оборони України;

ДБР – Державне бюро розслідувань;

ДКВС – Державна кримінально-виконавча служба України;

ДПС – Державна прикордонна служба України;

ДФС – Державна фіскальна служба України;

МВС – Міністерство внутрішніх справ України;

НАБ – Національне антикорупційне бюро України;

ОВ – «Особливої важливості»;

СБ – Служба безпеки України;

СЗР – Служба зовнішньої розвідки України;

Т – «Таємно»;

УДО – Управління державної охорони України;

ЦТ – «Цілком таємно».

<b>4. Сфера державної безпеки та охорони правопорядку</b>			
Номер статті ЗВДТ	Зміст відомостей, що становлять державну таємницю	Ступінь секретності	Суб'єкти режимно-секретної діяльності, держекспертами яких прийняті рішення
4.1.4	Відомості про зв'язок ознак особи, стосовно якої проводяться або проведено заходи відповідно до Закону України «Про державний захист працівників суду і правоохоронних органів» (зміна персональних даних або зовнішності чи місця проживання), з її попередніми індивідуальними ознаками	ЦТ	ДБР ДПС МВС НАБ НПУ СБ СЗР УДО
4.1.6	Відомості про зв'язок ознак особи, яка бере участь у кримінальному судочинстві і взята під захист згідно з чинним законодавством України у зв'язку з виникненням загрози її життю чи здоров'ю і стосовно якої проводяться або проведено заходи щодо зміни персональних даних або зовнішності чи місця проживання, з її попередніми індивідуальними ознаками	ЦТ	ДБР ДПС МВС НАБ НПУ СБ СЗР
4.1.14	Відомості про функціональні обов'язки негласних штатних співробітників (працівників) СБ; СЗР; органів внутрішніх справ; органів та підрозділів НПУ; ДПС, розвідувального органу Адміністрації ДПС; податкової міліції ДФС; ГУР; ДБР	Т	ГУР ДБР ДПС ДФС МВС НПУ СБ СЗР

4.4.1	Відомості за окремими показниками про зміст, форми, методи, організаційні положення, оперативну тактику здійснення ДПС, розвідувальним органом Адміністрації ДПС, ДФС, ГУР, УДО, СЗР; органами СБ, внутрішніх справ; органами та підрозділами НПУ; органом, установою виконання покарань, слідчим ізолятором ДКВС, НАБ, ДБР оперативно-розшукової, контррозвідувальної чи розвідувальної діяльності, розголошення яких створює загрозу національним інтересам і безпеці	Т	ГУР ДБР ДКВС ДПС ДФС МВС НАБ НПУ СБ СЗР УДО
4.12.1	Відомості про зміст матеріалів дізнання (досудового слідства), якщо розголошення відомостей про це може завдати шкоди національним інтересам і безпеці. Рішення про необхідність засекречування та розсекречування (але не пізніше вступу в силу вироку суду) інформації приймає держексперт	Т	ДБР ДКВС ДПС ДФС НПУ СБ
4.12.2	Відомості про зміст матеріалів дізнання (досудового слідства) з питань, які містять інформацію, віднесenu до державної таємниці. Рішення про необхідність засекречування (відповідно до ступеня секретності відповідних матеріалів) або розсекречування інформації приймає керівник органу дізнання (досудового слідства) самостійно або за поданням зацікавленої сторони (у разі представлення інформації про наявність у матеріалах дізнання (досудового слідства) державної таємниці, але на термін, що не перевищує максимального терміну засекречування відповідних матеріалів)	ОВ ЦТ Т	ДБР ДКВС ДПС ДФС НПУ СБ

4.12.3	Відомості про факт або методи проведення негласної слідчої (розшукової) дії	Т	ГПУ ДБР ДФС МВС НАБ НПУ СБ
4.12.4	Відомості, що дають змогу ідентифікувати особу, місце або річ, щодо якої проводиться чи планується проведення негласної слідчої (розшукової) дії, розголошення яких створює загрозу національним інтересам і безпеці	Т	ГПУ ДБР ДФС МВС НАБ НПУ СБ

### 3.3. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ РЕЖИМУ СЕКРЕТНОСТІ

Розглядаючи правове регулювання режиму секретності, слід зупинитися на підзаконних нормативно-правових актах, зокрема указах Президента України, постановах Кабінету Міністрів України, нормативних актах СБУ, МВС України та НП України.

#### **Укази Президента України:**

- Про Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства : Указ Президента України від 17 липня 2006 року № 621/2006;
- Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації : Указ Президента України від 14 грудня 2004 року № 1483/2004;
- Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць, затверджений Указом Президента України від 19 травня 2020 року № 190/2020.

#### **Кабінетом Міністрів України** були затверджені положення та постанови:

- Положення про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці, затверджене Постановою Кабінету Міністрів України від 15.06.1994 року № 414;

- Порядок організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях : Постанова Кабінету Міністрів України № 939 від 18.12.2013 року (для службового користування);
- Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію : Постанова Кабінету Міністрів України № 736 від 19.10.2016 року;
- Деякі питання документування управлінської діяльності : Постанова Кабінету Міністрів України від 17 січня 2018 року № 55.

#### **Нормативно-правові акти Служби безпеки України:**

- Звід відомостей, що становлять державну таємницю: наказ СБУ № 383 від 23.12.2020 року;
- Про затвердження Інструкції про порядок погодження органами Служби безпеки України призначення особи на посаду заступника керівника підприємства, установи, організації з питань режиму, начальника РСО : наказ СБУ № 306 від 8.05.2015 року;
- Про затвердження форм звітів про стан забезпечення охорони державної таємниці та інструкції про порядок їх оформлення і подання : наказ СБУ № 6 від 17.01.2020 року;
- Інструкція про порядок оформлення та подання звіту про стан забезпечення охорони державної таємниці та узагальненого звіту про стан забезпечення охорони державної таємниці за підзвітні суб'єкти режимно-секретної діяльності, затверджена наказом СБУ № 6 від 17.01.2020 року.

#### **Нормативно-правові акти МВС України та НП України:**

- Про затвердження Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України : наказ МВС України № 1351 від 26.12.2016 року;
- Про затвердження Інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, у системі Міністерства

- внутрішніх справ України : наказ МВС України № 88 від 03.02.2017 року;
- Положення про Управління режиму та технічного захисту інформації Національної поліції України, затверджене наказом НП України № 122 від 27.11.2015 року.

## **§ 4. ДОПУСК ТА ДОСТУП ГРОМАДЯН ДО СЕКРЕТНИХ РОБІТ І ДОКУМЕНТІВ**

### **4.1. ПІДСТАВИ ТА ПОРЯДОК ОФОРМЛЕННЯ ДОПУСКУ І ДОСТУПУ ДО СЕКРЕТНИХ РОБІТ І ДОКУМЕНТІВ**

Відповідно до положень Закону України «Про державну таємницю» **допуск до державної таємниці** – це оформлення права громадянина на доступ до секретної інформації. Допуск до державної таємниці із ступенями секретності «особливої важливості», «цілком таємно» та «таємно» надається дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання, наказом чи письмовим розпорядженням керівника органу державної влади, органу місцевого самоврядування, підприємства, установи або організації, де працює, перебуває на службі чи навчається громадянин.

В окремих випадках, які визначаються міністерствами, іншими центральними органами виконавчої влади, за погодженням із Службою безпеки України громадянам України віком від 16 років може надаватися допуск до державної таємниці із ступенями секретності «цілком таємно» та «таємно», а віком від 17 років – також до державної таємниці із ступенем секретності «особливої важливості».

Залежно від ступеня секретності інформації встановлюються такі форми допуску до державної таємниці (ст. 22 Закону України «Про державну таємницю»):

форма 1 – для роботи з секретною інформацією, що має ступені секретності «особливої важливості», «цілком таємно» та «таємно»;

форма 2 – для роботи з секретною інформацією, що має ступені секретності «цілком таємно» та «таємно»;

форма 3 – для роботи з секретною інформацією, що має ступінь секретності «таємно»,

а також такі терміни дії допусків:

- для форми 1 – 5 років;
- для форми 2 – 7 років;
- для форми 3 – 10 років.

Допуск до державної таємниці керівникові органу державної влади, органу місцевого самоврядування, підприємства, установи, організації надається наказом чи письмовим розпорядженням посадової особи, що призначає його на посаду, а у разі, коли орган державної влади, орган місцевого самоврядування, підприємство, установа, організація не підпорядкована іншому органу державної влади, органу місцевого самоврядування, підприємству, установі, організації або не належить до сфери їх управління, допуск до державної таємниці надається зазначеному керівникові наказом чи письмовим розпорядженням керівника органу державної влади, органу місцевого самоврядування, підприємства, установи, організації, яка є замовником робіт, пов'язаних з державною таємницею.

Якщо потреба громадянина у відомостях, що становлять державну таємницю, не пов'язана з місцем роботи, служби або навчання, допуск може надаватися за місцем провадження діяльності, пов'язаної з державною таємницею.

Надання допуску передбачає:

- визначення необхідності роботи громадянина із секретною інформацією;
- перевірку громадянина у зв'язку з допуском до державної таємниці;
- взяття громадянином на себе письмового зобов'язання щодо збереження державної таємниці, яка буде йому довірена;
- одержання у письмовій формі згоди громадянина на передбачені законом обмеження прав у зв'язку з його допуском до державної таємниці;
- ознайомлення громадянина з мірою відповідальності за порушення законодавства про державну таємницю.

Рішення про допуск громадянина до державної таємниці приймається не пізніше 5 днів після надходження до органу державної влади, органу місцевого самоврядування, підприємства, установи, організації висновків за матеріалами його перевірки у зв'язку з допуском до державної таємниці.

Допуск до державної таємниці не надається у разі (згідно зі ст. 23 Закону України «Про державну таємницю»):

1) відсутності у громадянина обґрунтованої необхідності в роботі із секретною інформацією;

2) сприяння громадянином діяльності іноземної держави, іноземної організації чи їх представників, а також окремих іноземців чи осіб без громадянства, що завдає шкоди інтересам національної безпеки України, або участі громадянина в діяльності політичних партій та громадських організацій, діяльність яких заборонена у порядку, встановленому законом;

3) відмови громадянина взяти на себе письмове зобов'язання щодо збереження державної таємниці, яка буде йому довірена, а також за відсутності його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці;

4) наявності у громадянина судимості за тяжкі злочини, не погашеної чи не знятої в установленому порядку;

5) наявності у громадянина психічних захворювань, які можуть завдати шкоди охороні державної таємниці, відповідно до переліку, затвердженого Міністерством охорони здоров'я України і Службою безпеки України.

У наданні допуску до державної таємниці може бути відмовлено також у разі:

1) повідомлення громадянином під час оформлення допуску недостовірних відомостей про себе;

2) постійного проживання громадянина за кордоном або оформлення ним документів на виїзд для постійного проживання за кордоном;

3) невиконання громадянином обов'язків щодо збереження державної таємниці, яка йому довірена або довірялася раніше.

Перевірка громадян у зв'язку з їх допуском до державної таємниці здійснюється органами Служби безпеки України у строк до одного місяця у порядку, встановленому Законом України «Про державну таємницю» (ст. 24 ) і Законом України «Про оперативно-розшукову діяльність».

Мотивований висновок органу Служби безпеки України, який здійснював перевірку, про неможливість надання громадянину допуску до державної таємниці є обов'язковим для виконання посадовими особами, уповноваженими

приймати рішення про надання допуску до державної таємниці, але не виключає повторного запиту із цього приводу в разі зміни обставин, за яких допуск до державної таємниці визнано неможливим.

Переоформлення громадянам допуску до державної таємниці здійснюється відповідно до ст. 26 Закону України «Про державну таємницю»:

- у разі закінчення терміну дії допуску до державної таємниці за необхідності подальшої роботи з секретною інформацією;
- у разі потреби підвищення громадянину форми допуску за необхідності роботи з секретною інформацією вищого ступеня секретності;
- у разі необхідності проведення додаткової перевірки, пов'язаної з можливим виникненням обставин, передбачених пунктами 2 і 4 частини першої та частиною другою статті 23 цього закону.

Скасування раніше наданого допуску до державної таємниці можливе у разі виникнення або виявлення обставин, передбачених статтею 23 Закону України «Про державну таємницю», а також після припинення громадянином діяльності, у зв'язку з якою йому було надано допуск, втрати громадянства України чи визнання його недієздатним.

На прохання громадянина його допуск до державної таємниці скасовується протягом трьох днів з часу звернення з приводу скасування допуску. Рішення про переоформлення чи скасування допуску приймається посадовими особами, уповноваженими приймати рішення про його надання. Громадянина, якому скасовано допуск до державної таємниці, якщо виконання трудових чи службових обов'язків вимагає доступу до державної таємниці, а переміщення на інше робоче місце чи іншу посаду неможливе, може бути в передбаченому законодавством порядку переведено на іншу роботу або службу, не пов'язану з державною таємницею, чи звільнено.

Порядок надання, переоформлення та скасування громадянам допуску до державної таємниці встановлюється Кабінетом Міністрів України.

**Доступ до державної таємниці** – це надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або

ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень. Доступ до державної таємниці (ст. 27 Закону України «Про державну таємницю») надається дієздатним громадянам України, яким надано допуск до державної таємниці та які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання.

Рішення про надання доступу до конкретної секретної інформації та її матеріальних носіїв приймають у формі наказу або письмового розпорядження керівники органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, у яких виконуються роботи, пов'язані з державною таємницею, або зберігаються матеріальні носії секретної інформації.

Керівники державних органів, за винятком осіб, передбачених частиною шостою ст. 27 Закону України «Про державну таємницю», органів місцевого самоврядування, підприємств, установ та організацій доступ до державної таємниці у сфері, що стосується діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації, отримують за посадою після надання їм допуску до державної таємниці за відповідною формою.

Порядок надання доступу до державної таємниці особам, залученим до конфіденційного співробітництва з оперативними підрозділами правоохоронних та інших спеціально уповноважених органів, які проводять оперативно-розшукову, розвідувальну або контррозвідувальну діяльність, визначається керівниками зазначених органів за погодженням із Службою безпеки України. У Службі безпеки України такий порядок надання доступу до державної таємниці визначається Головою Служби безпеки України.

Відмова надати громадянину України доступ до конкретної секретної інформації та її матеріальних носіїв можлива лише у разі відсутності підстав, передбачених частиною першою цієї статті, та може бути оскаржена в порядку, встановленому частиною другою статті 25 Закону України «Про державну таємницю».

Президентіві України, Голові Верховної Ради України, Прем'єр-міністрові України та іншим членам Кабінету Міністрів України, Голові

Верховного Суду, Голові Конституційного Суду України, Генеральному прокурору, Голові Служби безпеки України, Голові та іншим членам Рахункової палати, народним депутатам України доступ до державної таємниці всіх ступенів секретності надається за посадою після взяття ними письмового зобов'язання щодо збереження державної таємниці.

У свою чергу, іноземцям та особам без громадянства доступ до державної таємниці надається у виняткових випадках на підставі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, або письмового розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України. Зокрема, про це йде мова в Указі Президента України від 17 липня 2006 року № 621 «Про Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства».

Окрім зазначеного вище, слід указати, що доступ до державної таємниці всіх ступенів секретності, ознайомлення з якою є необхідним народним депутатам України для виконання своїх повноважень у комітеті Верховної Ради України, до предмета відання якого віднесено питання забезпечення контрольних функцій Верховної Ради України за діяльністю органів спеціального призначення з правоохоронними функціями, правоохоронних органів спеціального призначення та розвідувальних органів, надається після проходження перевірки у зв'язку з допуском їх до державної таємниці.

#### **4.2. ОСНОВНІ ОBOB'ЯЗКИ ПРАЦІВНИКІВ, ДОПУЩЕНИХ ДО РОБОТИ, ПОВ'ЯЗАНОЇ З ДЕРЖАВНИМИ ТАЄМНИЦЯМИ**

Стаття 28 Закону України «Про державну таємницю» встановлює обов'язки громадянина щодо збереження державної таємниці. Так, громадянин, якому надано допуск до державної таємниці, зобов'язаний:

- не допускати розголошення будь-яким способом державної таємниці, яка йому довірена або стала відомою у зв'язку з виконанням службових обов'язків;

- не брати участі в діяльності політичних партій та громадських організацій, діяльність яких заборонена в порядку, встановленому законом;
- не сприяти іноземним державам, іноземним організаціям чи їх представникам, а також окремим іноземцям та особам без громадянства у провадженні діяльності, що завдає шкоди інтересам національної безпеки України;
- виконувати вимоги режиму секретності;
- повідомляти посадових осіб, які надали йому доступ до державної таємниці, та відповідні режимно-секретні органи про виникнення обставин, передбачених ст. 23 Закону України «Про державну таємницю», або інших обставин, що перешкоджають збереженню довіреної йому державної таємниці, а також повідомляти у письмовій формі про свій виїзд з України;
- додержуватися інших вимог законодавства про державну таємницю.

#### **4.3. ОСНОВНІ ОБМЕЖЕННЯ ПРАВ ДЛЯ ПРАЦІВНИКІВ, ДОПУЩЕНИХ ДО РОБОТИ, ПОВ'ЯЗАНОЇ З ДЕРЖАВНИМИ ТАЄМНИЦЯМИ**

Окрім обов'язків, Законом України «Про державну таємницю» встановлено й певні обмеження прав для працівників, допущених до роботи, пов'язаної з державною таємницею.

Так, стаття 31 цього закону визначає обмеження на оприлюднення секретної інформації. Зокрема, під час підготовки матеріалів для опублікування, поширення у пресі та інших засобах масової інформації або переміщення їх через державний кордон державні органи, органи місцевого самоврядування, підприємства, установи, організації та громадяни з метою охорони секретної інформації зобов'язані керуватися законами України «Про інформацію» та «Про доступ до публічної інформації», Законом України «Про державну таємницю» та іншими нормативно-правовими актами про державну таємницю.

Контроль за додержанням законодавства про державну таємницю з метою запобігання її поширенню у пресі та інших засобах масової інформації здійснює

центральний орган виконавчої влади з питань інформаційної політики.

Стаття 32 Закону України «Про державну таємницю» встановлює обмеження щодо передачі державної таємниці іноземній державі чи міжнародній організації. Тому секретна інформація до скасування рішення про віднесення її до державної таємниці та матеріальні носії такої інформації до їх розсекречування можуть бути передані іноземній державі чи міжнародній організації лише на підставі міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, або письмового мотивованого розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України.

Стаття 33 Закону України «Про державну таємницю» встановлює обмеження, пов'язані з державною таємницею, щодо перебування і діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, а також розташування та переміщення об'єктів і технічних засобів, що їм належать. Такі обмеження визначаються відповідним законодавством.

## **§ 5. ОРГАНІЗАЦІЯ ЗАБЕЗПЕЧЕННЯ РЕЖИМУ СЕКРЕТНОСТІ**

### **5.1. РЕЖИМНО-СЕКРЕТНІ ОРГАНИ**

У державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що провадять діяльність, пов'язану з державною таємницею, з метою розроблення та здійснення заходів щодо забезпечення режиму секретності, постійного контролю за їх додержанням створюються на правах окремих структурних підрозділів режимно-секретні органи (далі – РСО), які підпорядковуються безпосередньо керівнику державного органу, органу місцевого самоврядування, підприємства, установи, організації.

Відповідно до положень ст. 21 Закону України «Про державну таємницю» створення, реорганізація чи ліквідація РСО здійснюються за погодженням із Службою безпеки України. У своїй роботі РСО взаємодіють з органами СБУ. До складу режимно-секретного органу входять підрозділи режиму, секретного діловодства та інші підрозділи, що безпосередньо забезпечують охорону державної таємниці, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації. Відповідно в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях із значним обсягом робіт, пов'язаних з державною таємницею, вводиться посада заступника керівника з питань режиму, на якого покладаються обов'язки та права керівника РСО.

РСО комплектуються спеціалістами, яким надано допуск до державної таємниці із ступенем секретності «цілком таємно», якщо характер виконуваних робіт не вимагає допуску до державної таємниці із ступенем секретності «особливої важливості». Якщо державний орган, орган місцевого самоврядування, підприємство, установа або організація не провадить діяльність із секретною інформацією, що має ступені секретності «цілком таємно» та

«особливої важливості», РСО такого органу, підприємства, установи або організації комплектується спеціалістами, яким надано допуск до державної таємниці зі ступенем секретності «таємно».

Статтею 21 Закону України «Про державну таємницю» встановлено основні завдання РСО, зокрема:

а) недопущення необґрунтованого допуску та доступу осіб до секретної інформації;

б) своєчасне розроблення та реалізація разом з іншими структурними підрозділами державних органів, органів місцевого самоврядування, підприємств, установ і організацій заходів, що забезпечують охорону державної таємниці;

в) запобігання розголошенню секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодінню секретною інформацією іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуску та доступу до неї;

г) виявлення та закриття каналів просочення секретної інформації в процесі діяльності державних органів, органів місцевого самоврядування, підприємства, установи, організації;

д) забезпечення запровадження заходів режиму секретності під час виконання всіх видів робіт, пов'язаних з державною таємницею, та під час здійснення зовнішніх відносин;

е) організація та ведення секретного діловодства;

є) здійснення контролю за станом режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та на підпорядкованих їм об'єктах.

Стаття 22 Закону України «Про державну таємницю» визначає права РСО. Отже, РСО мають право:

а) вимагати від усіх працівників державного органу, органу місцевого самоврядування, підприємства, установи та організації, а також відряджених неухильного виконання вимог законодавства щодо забезпечення охорони державної таємниці;

б) брати участь у розгляді проєктів штатних розписів державного органу, органу місцевого самоврядування, підприємства, установи та організації та підвідомчих їм установ, підприємств у частині, що стосується РСО, вносити

пропозиції щодо структури та чисельності працівників цих органів;

в) брати участь у проведенні атестації працівників, що виконують роботи, пов'язані з державною таємницею, а також у розгляді пропозицій щодо виплати в установленому нормативними актами порядку компенсації за роботу в умовах режимних обмежень;

г) залучати спеціалістів державного органу, органу місцевого самоврядування, підприємства, установи та організації до здійснення заходів щодо охорони державної таємниці;

д) здійснювати перевірки стану й організації роботи з питань захисту державної таємниці і забезпечення режиму секретності у підрозділах державного органу, органу місцевого самоврядування, підприємства, установи та організації, а також у підвідомчих їм установах та підприємствах, давати відповідні рекомендації;

е) здійснювати перевірки додержання режиму секретності на робочих місцях працівників, що мають допуск до державної таємниці, вмісту спецсховищ (приміщень, сейфів, металевих шаф, спецчемоданів, спецпапок тощо), наявності документів, виробів та інших матеріальних носіїв секретної інформації;

є) порушувати перед керівником державного органу, органу місцевого самоврядування, підприємства, установи та організації питання про призначення службових розслідувань за фактами порушень режиму секретності та секретного діловодства, про притягнення осіб до відповідальності згідно з законом, а також давати рекомендації щодо обов'язкових для виконання вказівок керівникам підрозділів державного органу, органу місцевого самоврядування, підприємства, установи та організації та підвідомчих їм установ, підприємств з питань забезпечення режиму секретності;

ж) брати участь у службових розслідуваннях, у встановленому порядку вимагати від працівників державного органу, органу місцевого самоврядування, підприємства, установи та організації письмових пояснень щодо фактів розголошення ними секретних відомостей, втрати матеріальних носіїв секретної інформації, інших порушень режиму секретності;

з) вносити пропозиції керівникові державного органу, органу місцевого самоврядування, підприємства, установи та організації про

припинення робіт, пов'язаних з державною таємницею, в структурних підрозділах, якщо умови для їх виконання не відповідають вимогам режиму секретності; опечатувати приміщення, де ведуться такі роботи або зберігаються матеріальні носії секретної інформації;

и) одержувати від громадян, яким оформляються документи на допуск до державної таємниці, анкетні дані;

і) використовувати засоби зв'язку та вести в установленому порядку поштово-телеграфне листування з іншими державними органами, органами місцевого самоврядування, підприємствами, установами й організаціями та їх РСО з питань забезпечення режиму секретності;

ї) мати печатку з найменуванням РСО, а також інші печатки та штампи установленої форми.

Відповідно до положень цієї статті передача функцій РСО будь-яким іншим підрозділам державного органу, органу місцевого самоврядування, підприємства, установи та організації не допускається.

Наказом СБУ від 08.05.2015 року № 306 затверджена «Інструкція про порядок погодження органами Служби безпеки України призначення особи на посаду заступника керівника підприємства, установи, організації з питань режиму, начальника режимно-секретного органу, його заступника, працівника, на якого покладаються обов'язки щодо забезпечення режиму секретності, а також керівника секретного архівного підрозділу підприємства, установи, організації». Отже, згідно з положеннями зазначеного наказу призначення особи на посаду заступника керівника підприємства, установи, організації з питань режиму, начальника РСО, його заступника, видання наказу про покладення на окремого працівника обов'язків щодо забезпечення режиму секретності, а також керівника секретного архівного підрозділу підприємства, установи, організації здійснюється після погодження з органом СБУ та РСО підприємства, установи, організації вищого рівня або підприємства, установи, організації, що є замовником секретних робіт. Таке погодження здійснюється органом СБУ з метою з'ясування можливості виконання кандидатом на посаду обов'язків, покладених відповідно до законодавства про державну таємницю, та його функціональних обов'язків.

Цим наказом встановлено відповідні вимоги до кандидата на посаду. Так, кандидат на посаду повинен:

- 1) відповідати кваліфікаційним вимогам, а саме мати:
  - вищу освіту за освітньо-кваліфікаційним рівнем або освітнім ступенем – спеціаліст або магістр;
  - стаж роботи у сфері охорони державної таємниці не менше 1 року;
  - досвід роботи щодо управління персоналом;
- 2) бути надійним, а саме:
  - протягом останніх п'яти років йому не скасовувався допуск до державної таємниці у зв'язку з невиконанням обов'язків щодо збереження державної таємниці, яка йому довірена або довірялася раніше;
  - не має не зняті дисциплінарні стягнення;
  - не притягався до адміністративної відповідальності за корупційні правопорушення або порушення законодавства про державну таємницю за останній рік;
  - стосовно нього відсутня інформація про наявність обставин, які можуть бути використані для примушення, впливу або тиску з метою вчинення дій на шкоду національній безпеці;
  - не зловживає алкогольними напоями, не є наркозалежним;
  - не є залежним від азартних ігор;
- 3) мати достатній рівень знань законодавства про державну таємницю;
- 4) мати допуск до державної таємниці:
  - для підприємства, установи, організації, якому встановлено першу категорію режиму секретності – за формою 1 або за формою 2, якщо характер виконуваних робіт не вимагає допуску до державної таємниці із ступенем секретності «особливої важливості»;
  - для підприємства, установи, організації, якому встановлено другу категорію режиму секретності – за формою 2;
  - для підприємства, установи, організації, якому встановлено третю категорію режиму секретності – за формою 3.

Крім указаних вище вимог, кандидат на посаду складає письмовий залік з метою з'ясування його рівня знань законодавства про державну таємницю. По закінченню заліку з кандидатом на посаду членами комісії може проводитися

співбесіда з метою з'ясування його моральних та ділових якостей. За результатами перевірки рівня знань кандидата на посаду законодавства про державну таємницю уповноважений підрозділ СБУ готує висновок про погодження призначення особи на посаду заступника керівника підприємства, установи, організації з питань режиму, начальника РСО, його заступника, а також працівника, на якого покладаються обов'язки щодо забезпечення режиму секретності, або на посаду керівника секретного архівного підрозділу, або про відмову в погодженні призначення на зазначену посаду. СБУ надсилає ініціатору повідомлення про погодження призначення кандидата на посаду. У разі відмови в погодженні призначення кандидата на посаду СБУ надсилає ініціатору відповідне повідомлення. Слід зауважити, що відмова в погодженні призначення кандидата на посаду не виключає можливості повторного звернення підприємства, установи, організації з цього приводу, але не раніше ніж після зміни обставин, які були підставою для прийняття рішення про відмову в погодженні призначення кандидата на посаду.

## **5.2. РЕЖИМНО-СЕКРЕТНІ ПІДРОЗДІЛИ МВС УКРАЇНИ ТА НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ**

Серед структурних підрозділів МВС України слід провести теоретичний аналіз діяльності Департаменту з питань режиму та службової діяльності (далі – Департамент). Зазначений Департамент організовує, контролює та аналізує стан виконання в апараті МВС України, його територіальних органах, закладах вищої освіти, що входять до сфери управління МВС, інших закладах, установах і підприємствах, що належать до сфери управління МВС, вимог законодавства у сфері охорони державної таємниці, у тому числі за дотриманням установленого законодавством порядку поводження з матеріальними носіями секретної інформації, їх зберігання та транспортування та за дотриманням установленого порядку доступу до відомостей, що становлять державну таємницю, своєчасністю і правильністю засекречування, зміни грифа секретності або розсекречування матеріальних носіїв інформації.

Також Департамент забезпечує та здійснює контроль за станом пропускнуго і внутрішньооб'єктового режимів в апараті МВС, функціонування

системи технічного захисту інформації, супроводження робіт зі створення комплексних систем захисту інформації в інформаційно-телекомунікаційних, інформаційних, телекомунікаційних системах МВС України.

Окрім того, Департамент веде облік усіх документів, які надходять до апарату МВС України, здійснює їх попередній розгляд, підготовку проектів резолюцій, доповідь керівництву МВС України, тиражування та спрямування за належністю, у тому числі облік наказів, доручень МВС України, рішень колегії МВС, організовує тиражування в друкарні та на копіювально-розмножувальній техніці, видачу їх структурним підрозділам апарату МВС України, його територіальним органам, закладам вищої освіти системи МВС України, закладам, установам і підприємствам, що належать до сфери управління МВС України. Також організовує, безпосередньо здійснює роботу зі зверненнями громадян, запитами на отримання публічної інформації, адвокатськими запитами, запитами і зверненнями депутатів усіх рівнів, які надходять до МВС України. Здійснює їх розгляд у частині, що належить до компетенції Департаменту, та готує відповіді на них.

Департамент організовує роботу приймальні громадян МВС України в апараті, здійснює контроль за діяльністю приймалень громадян у територіальних органах МВС України, закладах вищої освіти системи МВС України, закладах, установах і підприємствах, що належать до сфери управління МВС України. Також засвідчує копії документів, підписані керівництвом МВС України, та забезпечує діяльність Галузевого державного архіву Міністерства внутрішніх справ України.

Серед підрозділів Національної поліції України варто виділити Управління режиму та технічного захисту інформації (далі – УРТЗІ), яке є структурним підрозділом апарату НП України, безпосередньо є режимно-секретним органом НП України. Управління режиму та технічного захисту інформації НП України підпорядковується безпосередньо Голові НП України.

Отже, Положення про Управління режиму та технічного захисту інформації Національної поліції України затверджено наказом НП України від 27.11.2015 № 122. УРТЗІ для виконання покладених на нього завдань здійснює свої функції безпосередньо або через уповноважених РСО структурних

підрозділів апарату НП України та утворених в установленому порядку РСО територіальних органів поліції, міжрегіональних територіальних органів НП України, закладів та установ, що належать до сфери управління НП України.

Завданнями УРТЗІ є:

- недопущення необґрунтованого допуску та доступу осіб до секретної інформації;
- своєчасне розроблення та здійснення разом з іншими структурними підрозділами апарату НП України заходів щодо охорони державної таємниці в органах і підрозділах поліції;
- запобігання витоку секретної інформації в органах і підрозділах поліції;
- виявлення та закриття каналів витоку секретної інформації в процесі службової діяльності органів і підрозділів поліції;
- забезпечення режиму секретності під час проведення всіх видів секретних робіт в апараті НП України;
- організація і ведення секретного діловодства в апараті НП України;
- здійснення контролю за станом режиму секретності в органах і підрозділах поліції;
- організація роботи архівних підрозділів в органах і підрозділах поліції.

Зазначаємо, що серед підрозділів Національної поліції України роботу, пов'язану з державною таємницею, виконують підрозділи кримінальної та спеціальної поліції, які уповноважені здійснювати оперативно-розшукову діяльність та органи досудового розслідування, які уповноважені здійснювати негласні слідчі (розшукові) дії. Законом України «Про оперативно-розшукову діяльність» встановлено, що під час перевірки осіб у зв'язку з допуском їх до державної таємниці, до роботи з ядерними матеріалами та на ядерних установках, у зв'язку з призначенням на посади в розвідувальних органах України або залученням до конфіденційного співробітництва з такими органами, доступом осіб до розвідувальної таємниці, а також осіб, яким надається дозвіл на перебування без супроводу в контрольованих та стерильних зонах, зонах

обмеженого доступу, що охороняються, та критичних частинах таких зон аеропортів, оперативно-розшукова справа не заводиться. До того ж цей законодавчий акт указує, що не підлягають передачі і розголошенню результати оперативно-розшукової діяльності, які відповідно до законодавства України становлять державну таємницю, а також відомості, що стосуються особистого життя, честі, гідності людини. За передачу і розголошення цих відомостей працівники оперативних підрозділів, а також особи, яким ці відомості були довірені під час здійснення оперативно-розшукової діяльності чи стали відомі по службі або роботі, підлягають відповідальності згідно з чинним законодавством, крім випадків розголошення інформації про незаконні дії, що порушують права людини.

У системі закладів вищої освіти зі специфічними умовами навчання, які готують поліцейських, курсанти та слухачі під час вивчення спеціальних дисциплін розглядають і питання, пов'язані з державною таємницею та її охороною. Саме тому в таких закладах вищої освіти та академіях поліції також діють режимно-секретні підрозділи.

### **5.3. ЗАГАЛЬНІ ПОЛОЖЕННЯ ЩОДО ЗДІЙСНЕННЯ СЕКРЕТНОГО ДІЛОВОДСТВА**

У статті 18 Закону України «Про державну таємницю» зазначено, що з метою охорони державної таємниці впроваджуються:

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;
- дозвільний порядок провадження державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею;
- обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;
- технічний та криптографічний захисти секретної інформації тощо.

У свою чергу, стаття 19 Закону України «Про державну таємницю» вказує, що єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передачі та транспортування матеріальних носіїв секретної

інформації встановлюються Кабінетом Міністрів України. А стаття 20 цього ж закону визначає, що державні органи, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов'язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею.

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, надається державним органам, органам місцевого самоврядування, підприємствам, установам, організаціям за результатами спеціальної експертизи за умови, що вони:

- відповідно до компетенції, державних завдань, програм, замовлень, договорів (контрактів) беруть участь у діяльності, пов'язаній з державною таємницею;
- мають приміщення для проведення робіт, пов'язаних з державною таємницею, сховища для зберігання засекречених документів та інших матеріальних носіїв секретної інформації, що відповідають вимогам щодо забезпечення секретності зазначених робіт, виключають можливість доступу до них сторонніх осіб, гарантують збереження носіїв секретної інформації;
- додержуються передбачених законодавством вимог режиму секретності робіт та інших заходів, пов'язаних з використанням секретної інформації, порядку допуску осіб до державної таємниці, прийому іноземних громадян, а також порядку здійснення технічного та криптографічного захисту секретної інформації;
- мають режимно-секретний орган, якщо інше не передбачено Законом України «Про державну таємницю».

Слід наголосити, що організація та ведення секретного діловодства в органах, підприємствах, установах здійснюється безпосередньо РСО.

#### **5.4. ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРАВИЛ ПРОПУСКНОГО РЕЖИМУ**

Для забезпечення належних умов охорони державної таємниці та інформації з обмеженим доступом, порядку допуску до службових приміщень адміністративних будівель, недопущення несанкціонованого проникнення на об'єкт режимно-секретної діяльності сторонніх осіб нормативними актами

визначаються відповідні Правила пропускового режиму. Так, наказом МВС України від 22.04.2016 № 318 (редакція від 26.03.2021) затверджено Правила пропускового режиму на території апарату Міністерства внутрішніх справ України. Правила розроблені з метою визначення вимог до порядку організації пропускового режиму, доступу до службових і режимних приміщень (зон, територій) та адміністративних будівель апарату Міністерства внутрішніх справ України.

Метою запровадження пропускового режиму на території, у режимних приміщеннях (зонах, територіях) апарату МВС України є запобігання:

- проникненню на територію та в режимні приміщення (зони, території) МВС України сторонніх осіб;
- відвіданню без належної на те потреби режимних приміщень (зони, території) працівниками МВС України, центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ, відрядженими особами, а також іншими відвідувачами;
- несанкціонованому доступу сторонніх осіб до матеріальних носіїв секретної інформації та приміщень, де проводяться секретні роботи;
- несанкціонованому винесенню (вивезенню) за межі території апарату МВС України або режимних приміщень (зони, території), а також унесенню (увезенню) до них матеріальних носіїв секретної інформації;
- внесенню (ввезенню) на територію апарату МВС України аудіо-, відео-фотоапаратури, інших технічних засобів без відповідного дозволу.

Правилами пропускового режиму на території апарату Міністерства внутрішніх справ України визначено, що вхід на територію та вихід з території апарату МВС України здійснюється виключно через його контрольні-пропускні пункти (далі – КПП) за перепустками встановленого зразка. Особам, яким видано магнітні перепустки, забороняється здійснювати їх передачу іншим особам для використання з метою входу на територію (виходу з території) апарату МВС України та пересування в адміністративних будівлях. Магнітні перепустки не

дають права їх володільцям проводити через турнікети та двері зі зчитувачами інших осіб, крім тих, яких вони супроводжують.

Охорона території апарату МВС України здійснюється шляхом забезпечення пропускового режиму та підтримання публічної (громадської) безпеки і порядку на території апарату МВС України відповідно до Табеля постів роти охорони території апарату МВС за добовим розрахунком, затвердженим командиром роти охорони. Поліцейський роти охорони несе службу з вогнепальною зброєю в повсякденному однострої поліцейського.

Окрім того, варто вказати наказ МВС України від 31.07.2019 № 636 (редакція від 09.03.2021), яким затверджені Правила з організації пропускового режиму на території та до будівель закладів вищої освіти із специфічними умовами навчання, що належать до сфери управління МВС. Правилами встановлено порядок організації пропускового режиму на території, до будівель, службових та режимних приміщень (далі – території та об'єкти) закладів вищої освіти із специфічними умовами навчання, що належать до сфери управління МВС України, та їх відокремлених структурних підрозділів (далі – ЗВО МВС України).

Запровадження пропускового режиму в ЗВО МВС України здійснюється з метою запобігання:

- неправомірному проникненню на території та об'єкти ЗВО МВС України сторонніх осіб;
- відвідуванню без належної на те потреби територій та об'єктів ЗВО МВС України працівниками ЗВО МВС України, відрядженими особами, а також іншими відвідувачами;
- несанкціонованому доступу сторонніх осіб до матеріальних носіїв секретної інформації та приміщень, де проводяться секретні роботи;
- несанкціонованому внесенню (ввезенню) на території та об'єкти ЗВО МВС України або винесенню (вивезенню) з територій та об'єктів ЗВО МВС України матеріальних носіїв секретної інформації, а також речей, матеріальних цінностей, обладнання, технічних засобів, аудіо-, відео-, фотоапаратури та інших технічних засобів з аналогічними функціями без відповідного дозволу ректора (першого проректора, проректора) ЗВО МВС України.

Наказом МВС України від 31.07.2019 № 636 встановлено, що координація та контроль за діяльністю структурного підрозділу, на який покладено функції із забезпечення пропускового режиму на території та об'єкти ЗВО МВС України, здійснюються проректором (згідно з розподілом обов'язків). До того ж забезпечення пропускового режиму на території та об'єкти ЗВО МВС України, а також режимних заходів з питань пропускового режиму здійснює підрозділ організації служби ЗВО МВС України. А безпосереднє забезпечення пропускового режиму на території та об'єкти ЗВО МВС України здійснюється шляхом фізичної охорони, функціонування бюро перепусток, КПП, постів із пропусковими функціями на входах (виходах) до (із) територій та об'єктів ЗВО МВС України, установа технічних засобів контролю доступу, відеоспостереження. Зазначені заходи забезпечення пропускового режиму можуть застосовуватися як окремо, так і в комплексі. Зокрема, фізична охорона, технічні засоби контролю доступу, відеоспостереження на територіях та об'єктах ЗВО МВС України забезпечують:

- запобігання проникненню сторонніх осіб на території та об'єкти ЗВО МВС України;
- регулювання доступу осіб до територій та об'єктів ЗВО МВС України;
- контроль за переміщенням осіб територіями та об'єктами ЗВО МВС України.

Отже, пропуск працівників та здобувачів освіти ЗВО МВС України здійснюється за службовими посвідченнями та/або перепустками, у тому числі магнітними (за наявності). Працівникам та здобувачам освіти ЗВО МВС України, особам, які проживають у гуртожитках ЗВО МВС України, перепустки видаються з дозволу ректора ЗВО МВС України чи особи, яка виконує його обов'язки, за відповідними заявками керівників структурних підрозділів ЗВО МВС України. У разі втрати працівником, здобувачем освіти ЗВО МВС України перепустки вони зобов'язані негайно повідомити про це свого безпосереднього керівника. У разі звільнення працівника із ЗВО МВС України чи його переведення до іншого місця роботи перепустка здається до структурного підрозділу ЗВО МВС України, який її видав, про що уповноважена особа цього підрозділу робить відмітку в обхідному листі. Слід окремо зазначити, що особам,

яким видано перепустки, заборонено передавати їх іншим особам.

Під час здійснення пропуску осіб на території та об'єкти ЗВО МВС України (крім осіб, які використовують для проходу магнітні перепустки), водіїв та пасажирів транспортних засобів особа, яка забезпечує пропускний режим, зобов'язана перевірити службові посвідчення або інші документи, що посвідчують особу (у тому числі відображення інформації, що міститься у відповідних документах в електронній формі з використанням мобільного додатка Єдиного державного вебпорталу електронних послуг «Портал Дія», яке пред'являється особою на електронному носії, критерії якого підтримують використання мобільного додатка Порталу Дія, без додаткового пред'явлення оригіналів таких документів), на:

- 1) відповідність документа встановленій формі;
- 2) належність документа його пред'явникові;
- 3) наявність відбитка печатки відповідного закладу і підпису особи, яка видала документ;
- 4) чинність документа (строк дії);
- 5) відсутність виправлень або підроблень у документі.

У разі виявлення неправильно оформленого документа або виникнення підозри щодо його підроблення особа не допускається на території та об'єкти ЗВО МВС України. Про такий факт особа, яка забезпечує пропускний режим, доповідає керівнику структурного підрозділу, на який покладено функції із забезпечення пропускового режиму на території та об'єкти ЗВО МВС України, який доповідає про це ректору (першому проректору, проректору) ЗВО МВС України.

Можна зробити висновок, що якісне дотримання Правил пропускового режиму, спрямоване на забезпечення режиму секретності як один з організаційно-правових заходів щодо охорони державної таємниці.

## **§ 6. ПОРЯДОК РОБОТИ З ДОКУМЕНТАМИ ТА ІНШИМИ МАТЕРІАЛЬНИМИ НОСІЯМИ ІНФОРМАЦІЇ, ЩО МІСТЯТЬ СЛУЖБОВУ ІНФОРМАЦІЮ**

Відповідно до положень ст. 5 Закону України «Про доступ до публічної інформації» від 13 січня 2011 року № 2939-VI доступ до інформації забезпечується шляхом:

- 1) систематичного та оперативного оприлюднення інформації:
  - в офіційних друкованих виданнях;
  - на офіційних вебсайтах в мережі Інтернет;
  - на єдиному державному вебпорталі відкритих даних;
  - на інформаційних стендах;
  - будь-яким іншим способом;
- 2) надання інформації за запитами на інформацію.

Стаття 6 цього законодавчого акта визначає інформацію з обмеженим доступом, до якої відноситься конфіденційна інформація, таємна інформація, службова інформація.

**Конфіденційна інформація** – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Розпорядники інформації, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди – лише в інтересах національної безпеки, економічного добробуту та прав людини.

**Таємна інформація** – це інформація, доступ до якої обмежується відповідно до частини другої статті 6 Закону України «Про доступ до публічної інформації», розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

Порядок доступу до таємної інформації регулюється законами України «Про доступ до публічної інформації», «Про державну таємницю», «Про розвідку» та іншими спеціальними законами.

Відповідно до вимог частини другої ст. 6 Закону України «Про доступ до публічної інформації» до службової може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «для службового користування». Доступ до таких документів надається згідно з частиною другою ст. 6 Закону України «Про доступ до публічної інформації».

Обмеження доступу до інформації здійснюється у разі дотримання сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Зазначаємо, що інформація з обмеженим доступом має надаватися розпорядником інформації, якщо він правомірно оприлюднив її раніше та якщо немає законних підстав для обмеження у доступі до такої інформації, які існували раніше.

Аналізуючи інформацію з обмеженим доступом, слід визначити, яка інформація не може бути обмеженою в доступі. До такої інформації належать

відомості про складання, розгляд і затвердження бюджетів, кошторисів розпорядників бюджетних коштів та плани використання бюджетних коштів одержувачів бюджетних коштів, а також їх виконання за розписами, бюджетними програмами та видатками (крім таємних видатків відповідно до статті 31 Бюджетного кодексу України), взяття розпорядниками та одержувачами бюджетних коштів бюджетних зобов'язань або здійснення розпорядження бюджетними коштами у будь-який інший спосіб, планування, формування, здійснення та виконання закупівлі товарів, робіт і послуг за бюджетні кошти, у тому числі оборонних закупівель (крім випадків, якщо окрема інформація про закупівлі товарів, робіт і послуг становить державну таємницю відповідно до Закону України «Про державну таємницю»), володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно. Згідно з положеннями ст. 5 Закону України «Про доступ до публічної інформації» не підлягає обмеженню також доступ до інформації про стан і результати перевірок та службових розслідувань фактів порушень, допущених у сферах діяльності, зазначених у цій частині.

Також не належать до інформації з обмеженим доступом відомості, зазначені в декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, поданій відповідно до Закону України «Про запобігання корупції», крім випадків, визначених цим законом.

Органи державної влади, органи місцевого самоврядування, інші суб'єкти владних повноважень, у тому числі на виконання делегованих повноважень, складають відповідні переліки відомостей, що становлять службову інформацію. Доступ до даних переліків не може бути обмеженим.

Постановою Кабінету Міністрів України від 19 жовтня 2016 року № 736 затверджена Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію (далі – Типова інструкція). У ній визначено єдині вимоги до ведення обліку, зберігання, використання і знищення документів

та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану під час провадження оперативно-розшукової, контррозвідувальної діяльності, діяльності у сфері оборони держави, та іншу службову інформацію, в органах державної влади, інших державних органах, органах влади Автономної Республіки Крим.

Типовою інструкцією регулюється створення та діяльність в установі комісії з питань роботи із службовою інформацією. Комісія повинна діяти в установі постійно. Варто звернути увагу, що з урахуванням особливостей діяльності установи за рішенням її керівника можуть утворюватися кілька таких комісій за напрямками діяльності установи.

До основних завдань комісії з питань роботи із службовою інформацією належить:

- складення на підставі пропозицій структурних підрозділів установи та з урахуванням вимог законодавства переліку відомостей, що становлять службову інформацію, і подання його на затвердження керівникові установи;
- перегляд документів з грифом «Для службового користування» з метою його підтвердження або скасування;
- розгляд документів з грифом «Для службового користування» на предмет встановлення в них відомостей, що містять відкриту інформацію, яка може бути використана під час опрацювання запитів на публічну інформацію;
- розслідування на підставі рішення керівника установи фактів втрати документів з грифом «Для службового користування» та розголошення службової інформації;
- розгляд питання щодо присвоєння грифа «Для службового користування» документам, що містять службову інформацію, яка не передбачена переліком відомостей, за поданням осіб, які підписують такий документ;
- вивчення та проведення оцінки матеріалів, з якими планується ознайомити іноземців або які будуть їм передані.

До складу комісії з питань роботи із службовою інформацією включаються працівники структурних підрозділів установи, в яких створюється службова інформація, а також працівники режимно-секретного, мобілізаційного

підрозділів, підрозділів криптографічного та/або технічного захисту інформації (у разі їх створення), структурного підрозділу з діловодства або документаційного забезпечення, підрозділу з питань запитів на інформацію або працівники, відповідальні за виконання відповідних функцій в установі. Також до складу комісій, утворених за напрямами діяльності установи, включаються кваліфіковані працівники з відповідних напрямів діяльності.

Доцільно зауважити, що перелік відомостей складається установою відповідно до вимог частини другої ст. 6 та ст. 9 Закону України «Про доступ до публічної інформації», затверджується керівником установи та оприлюднюється на її офіційному вебсайті, а за відсутності такого вебсайту – в інший прийнятний спосіб. Працівники, яким доручено опрацьовувати документ, що містить службову інформацію, визначаються керівником установи, його заступниками, керівниками структурних підрозділів у резолюції до такого документа.

Організація в установі роботи з документами, що містять службову інформацію, покладається на структурний підрозділ з діловодства або документаційного забезпечення, а за його відсутності – на окрему посадову особу (служба діловодства).

Документам, що містять службову інформацію, присвоюється гриф «Для службового користування». Документам, що містять службову інформацію з:

- мобілізаційних питань, додатково проставляється відмітка «Літер «М»;
- питань криптографічного захисту службової інформації, додатково проставляється відмітка «Літер «К»;
- питань спеціальної інформації, додатково проставляється відмітка «СІ».

Питання щодо необхідності присвоєння документу грифа «Для службового користування» вирішується виконавцем або посадовою особою, яка підписує документ, відповідно до переліку відомостей та з дотриманням вимог частини другої ст. 6 та ст. 9 Закону України «Про доступ до публічної інформації». До прийняття рішення про присвоєння документу грифа «Для службового користування» уповноважені особи повинні:

- перевірити, чи належить інформація, яку містить документ, до категорій, визначених у частині першій ст. 9 Закону України «Про доступ до публічної інформації»;
- встановити, чи належить відповідна інформація до такої, доступ до якої згідно із законом не може бути обмежено, в тому числі шляхом віднесення її до службової інформації;
- перевірити дотримання сукупності вимог, передбачених частиною другою ст. 6 Закону України «Про доступ до публічної інформації».

В окремих випадках питання щодо необхідності присвоєння документу грифа «Для службового користування» може бути розглянуто комісією з питань роботи із службовою інформацією за поданням посадової особи, яка підписуватиме документ.

Типовою інструкцією забороняється використовувати для передачі службової інформації відкриті канали зв'язку. Однак у разі виникнення необхідності в передачі (надсиланні) документів, що містять службову інформацію, юридичним особам, громадським об'єднанням без статусу юридичної особи та фізичним особам, на яких не поширюються вимоги Типової інструкції, останні беруть на себе письмове зобов'язання стосовно нерозголошення отриманої службової інформації. Саме тому керівники юридичних осіб, громадських об'єднань без статусу юридичної особи та фізичні особи за розголошення службової інформації несуть відповідальність відповідно до законодавства України.

Безпосередня відповідальність за організацію та забезпечення дотримання в установах порядку ведення обліку, зберігання та використання документів, що містять службову інформацію, покладається на їх керівників. Особи, винні в порушенні порядку ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, їх втраті або розголошенні службової інформації, що в них міститься, притягуються до дисциплінарної або іншої відповідальності, передбаченої законом.

Типовою інструкцією визначено елементи роботи з документами грифом «Для службового користування»:

- приймання та реєстрація;
- облік документів та облік електронних носіїв інформації;

- друківання і розмноження документів;
- надсилання документів;
- формування виконаних документів у справи;
- користування документами;
- перегляд документів з грифом «Для службового користування»;
- підготовка справ до передачі на архівне зберігання та знищення;
- забезпечення збереженості документів та проведення перевірки їх наявності;
- охорона службової інформації під час міжнародного співробітництва.

Приймання та реєстрація документів з грифом «Для службового користування» здійснюється централізовано службою діловодства. У разі надходження у неробочий час конвертів (паковань) з документами з грифом «Для службового користування» вони приймаються черговим працівником установи, який, не розкриваючи, передає їх наступного робочого дня до служби діловодства під розписку в журналі обліку конвертів (паковань) за відповідною формою. В установи, в яких не передбачене цілодобове чергування, забороняється доставляти у неробочий час документи з грифом «Для службового користування».

Вхідна кореспонденція з грифом «Для службового користування» розкривається працівником служби діловодства, відповідальним за діловодство стосовно документів, що містять службову інформацію. При цьому перевіряється відповідність кількості аркушів, примірників, додатків до документів та їх реєстраційних індексів зазначеним на конверті (пакованні) та в супровідному листі. У випадку надсилання не за адресою документів з грифом «Для службового користування» вони повинні бути повернуті відправникові без їх розгляду.

Під час реєстрації вхідного документа з грифом «Для службового користування» на першому його аркуші від руки або за допомогою штампа (автоматичного нумератора) службою діловодства проставляється відмітка про надходження із зазначенням скороченого найменування установи – одержувача документа, реєстраційного індексу, дати (у разі термінового виконання – години і хвилини) одержання документа. Слід зазначити, що відповідно до вимог Типової інструкції облік електронних носіїв інформації, книг та інших видань, які є додатками до вхідного супровідного листа, ведеться окремо від вхідних

документів. На супровідному листі, який долучається до відповідної справи, службою діловодства проставляються номер облікової форми, порядковий номер і дата взяття додатка на облік. Водночас реєстрація вхідних, вихідних та внутрішніх документів з грифом «Для службового користування» здійснюється окремо від документів, які не містять службову інформацію, з дотриманням вимоги щодо одноразовості реєстрації. А етапи проходження документів з грифом «Для службового користування» в установі повинні обов'язково відображатися в реєстраційних формах (журналах, картках, електронній базі даних).

Згідно з положеннями Типової інструкції тираж видання з грифом «Для службового користування», підготовлений в установі, обліковується за одним порядковим номером у журналі за відповідною формою. Відмітка про додатково надруковані примірники видання робиться у журналі, де вони реєструвалися вперше, із продовженням їх нумерації від останнього номера примірника такого видання.

Облік електронних носіїв інформації (жорстких і гнучких магнітних дисків, касет та бобін з магнітною стрічкою, дисків для лазерних систем зчитування, невід'ємної частини модулів флешпам'яті тощо), на які планується записувати службову інформацію, ведеться службою діловодства у журналі за відповідною формою. На захисній оболонці електронного носія інформації (пластмасовій капсулі гнучкого магнітного диска, касеті або бобіні з магнітною стрічкою, на верхньому боці диска для лазерних систем зчитування, невід'ємній частині корпусу модулів флешпам'яті тощо) зазначаються найменування установи, обліковий номер і дата взяття на облік електронного носія, гриф «Для службового користування». Обліковий номер жорсткого магнітного диска вказується на етикетці, що наклеюється на його корпусі або на опломбованому корпусі блока чи пристрою, в якому він розміщується. Наклеювання на електронний носій інформації етикеток з обліковими номерами, зазначеними у пунктах 35 і 36 Типової інструкції, здійснюється у спосіб, який виключає можливість розбирання пристрою без пошкодження етикетки, її непомітного видалення (зміни) або перенесення на інший носій інформації.

Слід наголосити на тому, що у випадку не внесення до журналу обліку електронних носіїв інформації, на які планується записувати службову

інформацію, забороняється записувати службову інформацію на такий електронний носій інформації. А гриф «Для службового користування» зберігається за електронним носієм інформації до моменту його знищення.

Друкування і розмноження в установі документів з грифом «Для службового користування» за допомогою електронно-обчислювальної та копіювально-розмножувальної техніки провадиться з урахуванням вимог законодавства у сфері захисту інформації. Тому друкування і розмноження документів з мобілізаційних питань та з питань спеціальної інформації здійснюється працівниками установи, які мають допуск до роботи з такими документами. Окрім того, під час друкування необхідно проставити у правому верхньому куті першої сторінки документа, що містить службову інформацію, гриф «Для службового користування» та номер примірника.

У друкованих виданнях гриф «Для службового користування» і номер примірника зазначаються на обкладинці та на титульному аркуші видання. Якщо видання складається з кількох частин, такий гриф зазначається на кожній його частині, що містить службову інформацію. Типовою інструкцією закріплено необхідність зазначити на зворотному боці останнього аркуша примірника документа, що залишається у справі установи, у нижньому лівому куті:

- кількість надрукованих примірників;
- перелік номерів примірників з найменуваннями адресатів (не більше чотирьох);
- номер пункту переліку відомостей установи або реквізити акта комісії з питань роботи із службовою інформацією, згідно з якими інформацію віднесено до службової;
- назва та обліковий номер електронного носія інформації або номер автоматизованого робочого місця, з якого друкувався документ.

Після реєстрації створеного документа з грифом «Для службового користування» його чернетки і роздруковані варіанти знищуються виконавцем шляхом подрібнення або іншим способом (спалювання, розплавлення, розчинення тощо), який виключає можливість їх прочитання та відновлення. Розмноження документів з грифом «Для службового користування»

здійснюється службою діловодства або іншим структурним підрозділом, визначеним розпорядчим документом установи, з дозволу керівника установи (його заступника) за умови оформлення замовлення за відповідною формою або згідно з резолюцією керівника установи. Також керівник установи може у встановленому порядку делегувати повноваження щодо надання дозволу на розмноження таких документів керівникам структурних підрозділів, у яких документи опрацьовуються або зберігаються. До того ж на кожному примірнику розмноженого документа від руки проставляється номер примірника.

Надсилання документів з грифом «Для службового користування» іншим установам у межах України здійснюється рекомендованим поштовим відправленням або кур'єрською службою установи (кур'єрами), підрозділами урядового фельд'єгерського зв'язку, підрозділами органів спеціального зв'язку, підрозділами відомчого фельд'єгерського зв'язку у складі Збройних сил України. Передача або надсилання службових документів з грифом «Для службового користування» телекомунікаційними, інформаційно-телекомунікаційними мережами здійснюється лише з використанням засобів криптографічного захисту інформації, що в установленому порядку допущені до експлуатації, з дотриманням вимог технічного захисту інформації. Умовою пересилання електронних носіїв інформації та документів з грифом «Для службового користування», що підлягають поверненню, є обов'язкове їх надсилання до установи із супровідним листом.

Документи з грифом «Для службового користування», які надсилаються, повинні бути вкладені в конверти або упаковані у спосіб, який виключає можливість доступу та прочитання тексту чи реквізитів без порушення цілісності пакування.

На конвертах (пакуваннях) зазначаються адреса та найменування установи-одержувача і відправника, реєстраційні індекси вкладених документів із проставленням відмітки «ДСК». Забороняється зазначати прізвища і посади керівників установи-одержувача, а також прізвища виконавців документів і назви структурних підрозділів. Електронні носії інформації упаковуються в окремий конверт (пакування), на якому вказуються дата та реєстраційний індекс супровідного листа. У разі надсилання документів, які повинні бути розкриті певною посадовою особою установи особисто, їх упаковують в окремий конверт,

у правому верхньому куті якого нижче грифа «Для службового користування» проставляється відмітка «Особисто», а в його нижній правій частині зазначаються посада, прізвище, ім'я, по батькові (ініціали) одержувача. Такий конверт вкладається в інший конверт, що оформляється відповідно до вимог, визначених пунктом 57 Типової інструкції. У лівому верхньому куті конверта проставляється відмітка «Подвійний конверт». Також варто звернути увагу, що відповідно до вимог Типової інструкції забороняється надсилати за межі України видання з грифом «Для службового користування» з метою книгообміну або експонування на відкритих виставках, презентаціях.

Виконані документи з грифом «Для службового користування» групуються у справи згідно із затвердженою в установі зведеною номенклатурою справ. Вимогами Типової інструкції дозволяється долучати до справи із грифом «Для службового користування» документи з відкритою інформацією, якщо такі документи стосуються питань такої справи. Документи, що стосуються організації режимно-секретної роботи в установі, формуються у справи у відповідному структурному підрозділі працівником, відповідальним за виконання такого виду робіт. До номенклатури справ включаються всі довідкові та реєстраційні картотеки, журнали реєстрації та обліку документів з грифом «Для службового користування». У разі коли в установі створюється понад 50 документів на рік з грифом «Для службового користування», їх доцільно формувати в окремі справи за видами (накази, інструкції, плани тощо).

Вхідні, вихідні, внутрішні документи з грифом «Для службового користування» передаються працівникам відповідно до резолюцій керівника установи або його заступників, керівників підрозділів установи.

Справи з грифом «Для службового користування», що зберігаються у службі діловодства чи інших структурних підрозділах, видаються у тимчасове користування працівникам установи на підставі замовлення за відповідною формою, резолюції керівника установи або затвердженого керівником установи (керівником структурного підрозділу установи) списку працівників, які мають право працювати з відповідною справою. Допуск працівників установи до роботи з документами, що містять службову інформацію з мобілізаційних питань

або з питань спеціальної інформації, здійснюється на підставі списку, складеного підрозділом чи посадовою особою, відповідальною за мобілізаційну роботу або роботу із спеціальною інформацією, і затвердженого керівником установи. Також справи та видання з грифом «Для службового користування» видаються у тимчасове користування і приймаються під розписку в журналі за відповідною формою. Під час повернення справи від працівника посадовою особою проводиться перевірка наявності кожного аркуша всіх документів справи відповідно до її внутрішнього опису. Доцільно зауважити, що Типовою інструкцією встановлено строки користування документами, справами, які мають гриф «Для службового користування». Так, справи з грифом «Для службового користування» видаються для тимчасового користування на строк, що не перевищує одного місяця.

У разі потреби працівник іншої установи може робити витяги з виданих йому документів з грифом «Для службового користування» у робочому зошиті, що має зазначений гриф, який після завершення роботи з документами надсилається установі, що робила запит на ознайомлення. Порядок оформлення робочого зошита визначається інструкцією установи. До того ж працівник іншої установи може ознайомитися зі змістом документа з грифом «Для службового користування», отриманим від іншої установи, лише за письмовою згодою установи – розробника такого документа.

Типова інструкція встановила заборону на використання службової інформації, що міститься в документах з грифом «Для службового користування», для відкритих виступів або опублікування у засобах масової інформації та демонструвати такі документи на стендах, у вітринах на відкритих виставках або в інших громадських місцях.

Перегляд документів з грифом «Для службового користування» проводиться з метою підтвердження наявності або відсутності в них відомостей, що становлять службову інформацію, не рідше ніж один раз на п'ять років. Скасування грифа «Для службового користування» здійснюється за відсутності законних підстав для обмеження у доступі до службової інформації, які існували раніше.

Безпосередньо перегляд документів з грифом «Для службового користування» з метою можливого скасування грифа обов'язково здійснюється під час підготовки:

- справ для їх передачі до архівного підрозділу (архіву) установи;
- документів Національного архівного фонду для їх передачі на постійне зберігання до державних архівних установ, архівних відділів міських рад.

Рішення про скасування грифа «Для службового користування» чи його підтвердження приймається комісією з питань роботи із службовою інформацією установи – розробника документа або відповідною комісією установи- правонаступника чи установи вищого рівня, якщо установа – розробник документа припинила свою діяльність. За рішенням комісії з питань роботи із службовою інформацією строк обмеження доступу до справ (документів) може бути продовжений. Таке рішення комісії з питань роботи із службовою інформацією оформляється протоколом, що підписується головою і секретарем комісії та набирає чинності з моменту затвердження протоколу керівником установи. У протоколі зазначаються види документів, їх реєстраційні дані, заголовки та номери за номенклатурою або описом справ, з яких знімається гриф «Для службового користування» або строк обмеження доступу до яких продовжено. Витяг з даного протоколу або його засвідчена копія передається разом із справами до архівного підрозділу (архіву) установи, а у разі передачі документів Національного архівного фонду на постійне зберігання – до державних архівних установ, архівних відділів міських рад.

Важливо наголосити, що про скасування грифа «Для службового користування» письмово повідомляються всі установи, яким надсилався такий документ. За потреби можуть надсилатися витяги з протоколу засідання комісії з питань роботи із службовою інформацією.

Типова інструкція визначає необхідність проведення експертизи цінності документів з грифом «Для службового користування» та їх підготовку до архівного зберігання. Зокрема, у кінці кожної закінченої справи з грифом «Для службового користування» на окремому аркуші робиться засвідчувальний напис, у якому зазначаються цифрами і словами кількість аркушів у справі, кількість аркушів внутрішнього опису, а також:

- наявність літерних і пропущених номерів аркушів;
- номери аркушів з наклеєними фотографіями, кресленнями, вирізками тощо;

- номери великоформатних аркушів;
- номери конвертів з укладеннями;
- кількість аркушів укладень.

Після засвідчувального напису працівник, який сформував справу, ставить підпис із зазначенням посади, прізвища і дати, який засвідчується печаткою служби діловодства або печаткою «Для пакетів». Усі наступні зміни у складі справи (пошкодження аркушів, заміна документів копіями, долучення нових документів) зазначаються у засвідчувальному написі з посиланням на відповідний розпорядчий документ. Справи з грифом «Для службового користування» після проведення експертизи цінності документів, що містяться в ній, підшиваються через чотири проколи спеціальними суровими нитками або дратвою. Справи постійного та тривалого (понад десять років) строків зберігання та особові справи оправляються у тверду обкладинку.

Також справи постійного та тривалого зберігання з грифом «Для службового користування» та особові справи включаються у відповідні описи справ разом з документами, що містять відкриту інформацію. При цьому в описі до номера справи та у графі «Індекс справи (тому, частини) з документами з грифом «Для службового користування» додається відмітка «ДСК». Під час передачі справ з грифом «Для службового користування» на постійне зберігання до державної архівної установи, архівного відділу міської ради установа-фондоутворювач разом з актом приймання-передавання справ, оформленим в установленому порядку, подає державній архівній установі, архівному відділу міської ради лист, у якому визначається порядок користування такими справами. Вилучені для знищення за результатами експертизи цінності справи з грифом «Для службового користування», строк зберігання яких закінчився, включаються до акта про вилучення для знищення документів, не внесених до Національного архівного фонду, що складається відповідно до вимог, установлених щодо всіх справ установи. Безпосереднє знищення видань з грифом «Для службового користування», що зберігаються у бібліотеках, здійснюється згідно з актом, який складається відповідно до встановлених вимог.

Крім викладеного вище, звертаємо увагу на те, що справи з грифом «Для службового користування» з дати їх створення (надходження) зберігаються за

місцем формування справ згідно із затвердженою зведеною номенклатурою справ до моменту їх передачі в архівний підрозділ (архів) установи. Документи і справи з грифом «Для службового користування» зберігаються у шафах, сейфах, що розташовані у службових приміщеннях або сховищах архіву.

Шафи, сейфи, службові приміщення, сховища архіву повинні надійно замикатися і опечатуватися металевими печатками. Водночас порядок виготовлення, ведення обліку, використання металевих печаток та порядок ведення обліку шаф, сейфів і ключів від них визначаються керівником установи. Отже, маємо змогу зробити висновок, що зберігання документів і справ із грифом «Для службового користування» здійснюється працівниками, які безпосередньо отримали їх під розписку, у спосіб, що унеможлиблює доступ до них сторонніх осіб.

Передача документів із грифом «Для службового користування» структурним підрозділам здійснюється через службу діловодства з проставленням відповідної відмітки в облікових формах. Відомчою інструкцією установи необхідно визначити порядок передачі одержаних у службі діловодства документів з грифом «Для службового користування» всередині одного структурного підрозділу для виконання (ознайомлення) від одного працівника структурного підрозділу іншому працівникові того самого підрозділу та ведення необхідних облікових форм. До того ж забороняється переміщення документів з грифом «Для службового користування» з однієї справи до іншої без повідомлення служби діловодства. Про всі переміщення документів уповноважена посадова особа повинна робити відповідні відмітки в облікових формах, у тому числі внутрішніх описах. Вилучення справ або окремих документів із справ з грифом «Для службового користування» забороняється. В окремих випадках на підставі рішення слідчого судді, суду архівний підрозділ (архів) установи або служба діловодства за письмовою вказівкою керівника установи здійснює вилучення оригіналів необхідних документів або справ. При цьому у структурному підрозділі (архіві) повинні залишитися протокол про вилучення документів з їх засвідченими копіями.

Отже, документи з грифом «Для службового користування» не дозволяється виносити за межі установи, крім випадків передачі документів на виконання у структурні підрозділи, що розташовуються поза межами основного

приміщення установи, та у разі виникнення необхідності в їх узгодженні, підписанні в установах, розташованих у межах одного населеного пункту. Таке винесення документа з грифом «Для службового користування» за межі установи здійснюється на підставі резолюції керівника установи (його заступника) або керівника структурного підрозділу, в якому такий документ (його проєкт) підготовлено. Такий документ з грифом «Для службового користування» повинен бути вкладений у конверт або упакований у такий спосіб, щоб виключити можливість його прочитання.

Відповідно до вимог Типової інструкції стан організації роботи з документами, що містять службову інформацію (наявність та фізичний стан документів, справ, видань, електронних носіїв інформації з грифом «Для службового користування»), не рідше ніж один раз на рік перевіряється комісією з питань проведення перевірки наявності документів з грифом «Для службового користування» після завершення діловодного року та формування справ. При цьому актом установи необхідно визначити строк проведення перевірки та склад комісії з питань її проведення.

Водночас теоретичного аналізу потребує питання охорони службової інформації під час міжнародного співробітництва. Згідно з Типовою інструкцією керівник установи або його заступник, відповідальний за організацію прийому та роботу з іноземцями приймає рішення про можливість прийому установою іноземних делегацій, груп та окремих іноземних громадян та осіб без громадянства. Безпосередню організацію прийому іноземців і проведення роботи з ними забезпечує структурний підрозділ з питань зовнішніх відносин, а в установах, де такий підрозділ відсутній, – посадова особа, визначена керівником установи в розпорядчому документі. Підрозділом зовнішніх відносин разом з іншими структурними підрозділами установи, що беруть участь у прийомі іноземців, за участю структурного підрозділу технічного захисту інформації (особи, відповідальної за виконання такої роботи) розробляється програма прийому іноземців, яка повинна містити:

- відомості про іноземців, найменування їх посад, а також інформацію про підприємство, установу, організацію, яку вони представляють, період перебування в установі;

- мету прийому іноземців, перелік питань, які плануються для обговорення. Інформація про діяльність установи, яка може бути доведена до іноземців або їм передана, зазначається у додатку до програми;
- список посадових осіб установи, відповідальних за прийом іноземців і виконання інших завдань, пов'язаних з перебуванням іноземців в установі (із зазначенням змісту таких завдань);
- перелік структурних підрозділів установи (із зазначенням приміщень, цехів, дільниць, лабораторій), які відвідуватимуться іноземцями;
- перелік місць та порядок застосування іноземцями кіно-, фото-, аудіо- і відеоапаратури, інших технічних засобів;
- маршрути і порядок пересування іноземців територією установи;
- інші необхідні заходи.

Керівник установи або його заступник, відповідальний за організацію прийому та роботу з іноземцями затверджує програму прийому іноземців. Також керівник установи або за його дорученням керівник підрозділу зовнішніх відносин у разі коли під час прийому іноземців передбачається передача іноземцям в установленому законодавством порядку службової інформації, яка була зібрана під час провадження оперативно-розшукової, контррозвідувальної діяльності, діяльності у сфері оборони держави, зобов'язаний своєчасно проінформувати у письмовій формі орган СБУ про склад іноземної делегації (групи) із зазначенням прізвищ, імен і посад її членів, період перебування та мету відвідання установи. Разом з указаною інформацією надсилається копія програми прийому іноземців. Крім того, з метою запобігання витоку службової інформації відомості, документи та інші матеріальні носії інформації, яким надано гриф «Для службового користування» та з якими планується ознайомити іноземців або які будуть їм надані, оцінюються комісією з питань роботи із службовою інформацією до затвердження програми прийому іноземців. Своє рішення комісія з питань роботи із службовою інформацією оформляє актом про результати проведення експертної оцінки, що затверджується керівником установи.

Отже, акт про результати проведення експертної оцінки повинен містити:

- дані щодо підстав проведення експертної оцінки;
- назву, реєстраційні дані, гриф обмеження доступу до документа, номер носія інформації, яка є предметом експертної оцінки;
- назву та вид носія інформації, його реєстраційні дані, сторінки, пункти, абзаци та інші дані щодо інформації, яка містить відомості, що становлять службову інформацію;
- сферу життєдіяльності держави, якій може бути завдано шкоди внаслідок оприлюднення такої інформації, та обґрунтування такого висновку;
- пункти переліку відомостей, що становлять службову інформацію, яким відповідають наявні в матеріальних носіях інформації відомості;
- найменування органу державної влади, іншого державного органу, органу місцевого самоврядування, органу влади Автономної Республіки Крим, іншого суб'єкта, що виконує владні управлінські функції відповідно до законодавства і є розпорядником зазначеної службової інформації.

А безпосередні носії інформації з грифом «Для службового користування» можуть бути надані для ознайомлення іноземцям після вилучення з них відомостей, що становлять службову інформацію.

Варто зазначити, що в установах, що систематично здійснюють прийом іноземців, виділяються та обладнуються окремі приміщення для роботи з іноземцями. Підготовка інших приміщень установи для прийому іноземців передбачає припинення в них робіт, пов'язаних з обробкою службової інформації, вилучення документів з грифом «Для службового користування», приховування або маскування виробів (стендів), наочної документації, що містять службову інформацію. Приміщення, в яких проводиться робота з іноземцями, до початку їх відвідування іноземцями та після його завершення перевіряються працівниками структурного підрозділу технічного захисту інформації, які повинні скласти відповідну довідку про результати такої перевірки.

Слід зважати на заборону залишати іноземців у службових приміщеннях та на території установи без супроводу під час прийому і проведення роботи з ними. У виняткових випадках за рішенням керівника установи супровід

іноземців може не здійснюватися за умови використання на маршрутах їх слідування технічних засобів охорони та спостереження.

За результатами прийому іноземців підрозділ зовнішніх відносин складає у довільній формі звіт про виконання програми роботи з іноземцями, в якому зазначаються:

- відомості про іноземців, зміст проведених з ними бесід;
- інформація, яка використовувалася чи була передана іноземцям, перелік відповідних матеріальних носіїв інформації (документів, науково-технічної документації, зразків виробів тощо);
- інформація, отримана від іноземців;
- пропозиції та рекомендації за результатами візиту іноземців.

Про виконання програми роботи з іноземцями керівником установи затверджується відповідний звіт. У разі передачі іноземцям документів або матеріальних носіїв, що містять службову інформацію, зібрану під час провадження оперативно-розшукової, контррозвідувальної діяльності, діяльності у сфері оборони держави, копія затвердженого звіту протягом п'яти робочих днів надсилається органіві СБУ, а також за рішенням керівника установи іншим заінтересованим установам.

Підсумовуючи щодо роботи з інформацією з обмеженим доступом, слід зазначити, що Типовою інструкцією визначено випадки необхідності дотримання вимог Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого Постановою Кабінету Міністрів України від 18 грудня 2013 року № 939. Положення цього Порядку використовуються у разі виникнення необхідності в одночасному забезпеченні охорони службової інформації та режиму секретності під час міжнародного співробітництва.

## **§ 7. ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ. ЗАСЕКРЕЧУВАННЯ ТА РОЗСЕКРЕЧЕННЯ МАТЕРІАЛЬНИХ НОСІЇВ СЕКРЕТНОЇ ІНФОРМАЦІЇ**

### **7.1. ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ**

Віднесення інформації до державної таємниці – це процедура, яка визначена положеннями Закону України «Про державну таємницю» щодо прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їхньої секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України в разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, з опублікуванням цього Зводу та змін до нього.

До державної таємниці в порядку, встановленому статтею 8 Закону України «Про державну таємницю» відноситься інформація:

- у сфері оборони;
- у сфері економіки, науки і техніки;
- у сфері зовнішніх відносин;
- у сфері державної безпеки та охорони правопорядку.

Слід указати інформацію, яка не належить до державної таємниці. Це відомості:

- 1) про стан довкілля, якість харчових продуктів і предметів побуту, вплив товару (роботи, послуги) на життя та здоров'я людини;
- 2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;
- 3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування і соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти та культури населення;

- 4) про факти порушень прав і свобод людини та громадянина;
- 5) про незаконні дії державних органів, органів місцевого самоврядування та їх посадових і службових осіб;
- б) інша інформація, доступ до якої відповідно до законів та міжнародних договорів, згода на обов'язковість яких надано Верховною Радою України, не може бути обмежено.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності «особливої важливості», «цілком таємно» та «таємно» лише за умови, що вони належать до категорій, зазначених у частині першій статті 8 Закону України «Про державну таємницю» і їхнє розголошення завдаватиме шкоди інтересам національної безпеки України та з дотриманням вимог статті 6 Закону України «Про доступ до публічної інформації».

Варто зауважити, що існує заборона на віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

## **7.2. ДЕРЖАВНИЙ ЕКСПЕРТ З ПИТАНЬ ТАЄМНИЦЬ: ЙОГО ПРАВА ТА ОБОВ'ЯЗКИ**

Віднесення інформації до державної таємниці здійснюється мотивованим рішенням державного експерта з питань таємниць за його власною ініціативою, за зверненням керівників відповідних державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян.

Державний експерт з питань таємниць відносить інформацію до державної таємниці з питань, прийняття рішень з яких належить до його компетенції згідно з посадою. У разі, якщо прийняття рішення про віднесення інформації до державної таємниці належить до компетенції кількох державних експертів з питань таємниць, воно за ініціативою державних експертів або за пропозицією Служби безпеки України приймається колегіально та ухвалюється простою більшістю голосів.

Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця

інформація, чи зміни до нього у порядку, встановленому Законом України «Про державну таємницю».

Відповідно до положень статті 9 Закону України «Про державну таємницю» державний експерт з питань таємниць здійснює віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування.

Державний експерт з питань таємниць відповідно до покладених на нього завдань:

1) визначає:

- підстави, за якими інформацію має бути віднесено до державної таємниці;
- підстави та доцільність віднесення до державної таємниці інформації про винаходи (корисні моделі), призначені для використання у сферах, зазначених у частині першій статті 8 Закону України «Про державну таємницю»;
- доцільність віднесення до державної таємниці інформації про винаходи (корисні моделі), що мають подвійне застосування, на підставі порівняльного аналізу ефективності цільового використання та за згодою автора (власника патенту);
- ступінь секретності інформації, віднесеної до державної таємниці;
- державний орган (органи), якому надається право приймати рішення щодо кола суб'єктів, які матимуть доступ до секретної інформації;

2) готує висновок щодо завданої національній безпеці України шкоди у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації;

3) установлює та продовжує строк дії рішення про віднесення інформації до державної таємниці із зазначенням дати її розсекречення;

4) дає Службі безпеки України рішення про зміну ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці у разі, якщо підстави, на яких цю інформацію було віднесено до державної таємниці, перестали існувати;

5) затверджує за погодженням із Службою безпеки України розгорнуті переліки відомостей, що становлять державну таємницю, зміни до них,

контролює відповідність змісту цих переліків Зводу відомостей, що становлять державну таємницю;

6) розглядає пропозиції державних органів, органів місцевого самоврядування, підприємств, установ, організацій, об'єднань громадян та окремих громадян щодо віднесення інформації до державної таємниці та її розсекречування;

7) затверджує висновки щодо обізнаності з державною таємницею громадян, які мають чи мали допуск до державної таємниці;

8) контролює обґрунтованість і правильність надання документам, виробам та іншим матеріальним носіям інформації, які містять відомості, включені до Зводу відомостей чи розгорнутих переліків відомостей, що становлять державну таємницю, відповідного грифа секретності, своєчасність зміни такого грифа та розсекречування цих носіїв із наданням їм реквізиту «розсекречено»;

9) бере участь у розробленні критеріїв визначення шкоди, яку може бути завдано національній безпеці України у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації.

Також державний експерт з питань таємниць під час виконання покладених на нього функцій зобов'язаний:

1) погоджувати за посередництвом Служби безпеки України свої висновки про скасування рішень щодо віднесення інформації до міждержавних таємниць з відповідними посадовими особами держав-учасниць міжнародних договорів України про взаємне забезпечення збереження міждержавних таємниць та повідомляти їх про прийняті рішення щодо віднесення інформації до державної таємниці, на яку поширено чинність цих договорів;

2) подавати Службі безпеки України не пізніше, ніж через десять днів з моменту підписання рішення про віднесення відомостей до державної таємниці або про скасування цих рішень, а розгорнуті переліки відомостей, що становлять державну таємницю, – у той же строк з моменту їхнього затвердження;

3) розглядати протягом одного місяця пропозиції Служби безпеки України про віднесення інформації до державної таємниці, скасування чи продовження терміну дії раніше прийнятого рішення про віднесення інформації до державної таємниці;

4) надавати відповідний гриф секретності рішенням про віднесення інформації до державної таємниці та про скасування цих рішень залежно від важливості їхнього змісту;

5) брати участь у засіданнях державних експертів з питань таємниць;

б) ініціювати питання щодо притягнення до відповідальності посадових осіб, які порушують законодавство України про державну таємницю.

Окрім того, державний експерт з питань таємниць має право:

1) безперешкодно проводити перевірку виконання державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями, що перебувають у сфері його діяльності, рішень про віднесення інформації до державної таємниці, скасування цих рішень, додержання порядку засекречення інформації та у разі виявлення порушень давати обов'язкові для виконання приписи про їх усунення;

2) створювати експертні комісії із фахівців і науковців, які мають допуск до державної таємниці, для підготовки проєктів рішень про віднесення інформації до державної таємниці, зниження ступеня її секретності та скасування зазначених рішень, висновків щодо обізнаності з державною таємницею громадян, які мають чи мали допуск до державної таємниці, а також для підготовки відповідних висновків у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації;

3) скасовувати безпідставні рішення про надання носію інформації грифа секретності, зміну або скасування цього грифа;

4) клопотати про притягнення до відповідальності посадових осіб, які порушують законодавство України про державну таємницю;

5) отримувати в установленому порядку від державних органів, органів місцевого самоврядування, підприємств, установ та організацій відомості, необхідні для виконання своїх функцій.

Слід звернути увагу, що відповідно до положень Закону України «Про державну таємницю» державний експерт з питань таємниць несе персональну відповідальність за законність та обґрунтованість свого рішення про віднесення інформації до державної таємниці або про зниження ступеня секретності такої інформації чи скасування рішення про віднесення її до державної таємниці, а

також за умисне неприйняття рішення про віднесення до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України.

У рішенні державного експерта з питань таємниць про віднесення інформації до державної таємниці зазначаються:

1) інформація, яка має становити державну таємницю, та її відповідність категоріям і вимогам, передбаченим статтею 8 Закону України «Про державну таємницю» та статтею 6 Закону України «Про доступ до публічної інформації»;

2) підстави для віднесення інформації до державної таємниці;

3) критерії віднесення інформації до державної таємниці, зокрема:

- визначення рівня та опис загрози і шкоди національній безпеці (національним інтересам) у разі невіднесення інформації до державної таємниці;
- визначення дати або події розсекречування інформації;
- ступінь секретності зазначеної інформації;
- обсяг фінансування заходів, необхідних для охорони такої інформації;
- державний орган, орган місцевого самоврядування, підприємство, установа, організація чи громадянин, який вніс пропозицію про віднесення цієї інформації до державної таємниці, та державний орган (органи), якому надається право визначати коло суб'єктів, що матимуть доступ до цієї інформації;
- строк, протягом якого діє рішення про віднесення інформації до державної таємниці.

Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, та інших обставин. Він не може перевищувати для інформації зі ступенем секретності «особливої важливості» – 30 років, для інформації «цілком таємно» – 10 років, для інформації «таємно» – 5 років.

Після закінчення передбаченого частиною першою статті 13 Закону України «Про державну таємницю» строку дії рішення про віднесення інформації до державної таємниці державний експерт з питань таємниць

приймає рішення про скасування рішення про віднесення її до державної таємниці або приймає рішення про продовження строку дії зазначеного рішення в межах строків, встановлених частиною першою ст. 13 цього закону. Установлення строку дії рішення про віднесення інформації до державної таємниці, прийняття рішення про його продовження здійснюються з дотриманням вимог статті 6 Закону України «Про доступ до публічної інформації».

### **7.3. ЗАСЕКРЕЧУВАННЯ ТА РОЗСЕКРЕЧУВАННЯ МАТЕРІАЛЬНИХ НОСІЇВ СЕКРЕТНОЇ ІНФОРМАЦІЇ**

Згідно із Законом України «Про державну таємницю» засекречування матеріальних носіїв інформації – це введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

Відповідно до положень статті 15 Закону України «Про державну таємницю» засекречування матеріальних носіїв інформації здійснюється шляхом надання на підставі Зводу відомостей, що становлять державну таємницю (розгорнутих переліків відомостей, що становлять державну таємницю), відповідному документу, виробу або іншому матеріальному носію інформації грифа секретності посадовою особою, яка готує або створює документ, виріб або інший матеріальний носій інформації. Засекречування документів здійснюється лише в частині відомостей, що становлять державну таємницю. У разі подання запиту на документ, частина якого засекречена, доступ до такого документа забезпечується в частині, що не засекречена.

Гриф секретності – це реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності цієї інформації. Гриф секретності кожного матеріального носія секретної інформації повинен відповідати ступеню секретності інформації, яка в ньому міститься, згідно із Зводом відомостей, що становлять державну таємницю, – «особливої важливості», «цілком таємно» або «таємно». Реквізити кожного матеріального носія секретної інформації складаються із:

- грифа секретності;

- номера примірника;
- статті Зводу відомостей, що становлять державну таємницю, на підставі якої здійснюється засекречення;
- найменування посади та підпису особи, яка надала гриф секретності.

Якщо реквізити, вказані в частині другій статті 15 Закону України «Про державну таємницю», неможливо нанести безпосередньо на матеріальний носій секретної інформації, вони мають бути зазначені в супровідних документах.

Слід зауважити, що забороняється надавати грифи секретності, передбачені Законом України «Про державну таємницю», матеріальним носіям іншої таємної інформації, яка не становить державної таємниці, або конфіденційної інформації.

Перелік посад, перебування на яких дає посадовим особам право надавати матеріальним носіям секретної інформації грифи секретності, затверджується керівником державного органу, органу місцевого самоврядування, підприємства, установи, організації, що провадить діяльність, пов'язану з державною таємницею.

Після закінчення встановлених строків засекречування матеріальних носіїв інформації та у разі підвищення чи зниження ступеня секретності такої інформації, визначеного державним експертом з питань таємниць, або скасування рішення про віднесення її до державної таємниці керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, у яких здійснювалося засекречування матеріальних носіїв інформації, або керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, які є їх правонаступниками, чи керівники вищого рівня зобов'язані протягом шести місяців забезпечити зміну грифа секретності або розсекречування цих матеріальних носіїв секретної інформації та письмово повідомити про це керівників державних органів, органів місцевого самоврядування, підприємств, установ, організацій, яким були передані такі матеріальні носії секретної інформації.

Також строк засекречування матеріальних носіїв інформації має відповідати строку дії рішення про віднесення інформації до державної таємниці,

встановленого рішенням державного експерта з питань таємниць. Перебіг строку засекречування матеріальних носіїв інформації починається з часу надання їм грифа секретності.

Розсекречування матеріальних носіїв секретної інформації варто тлумачити як зняття в установленому законодавством порядку (Закон України «Про державну таємницю») обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

## **§ 8. СУТНІСТЬ ТА ПОРЯДОК ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ЗА РЕЖИМОМ СЕКРЕТНОСТІ**

### **8.1. КОНТРОЛЬ ЗА ДОТРИМАННЯМ РЕЖИМУ СЕКРЕТНОСТІ**

Охорона державної таємниці – це комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв. Матеріальні носії секретної інформації – це матеріальні об’єкти, у тому числі фізичні поля, у яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо. Саме тому контроль дозволяє вчасно виявити порушення вимог законодавчих та нормативних актів, що встановлюють порядок проведення секретних робіт та поводження з секретними документами, і вчасно вживати необхідних заходів щодо усунення причин та умов, які сприяють виникненню таких порушень.

Відповідно до чинних норм Закону України «Про державну таємницю» керівники державних органів, органів місцевого самоврядування, підприємств, установ та організацій зобов’язані здійснювати постійний контроль за забезпеченням охорони державної таємниці. Зокрема, державні органи, органи місцевого самоврядування, підприємства, установи і організації, що розміщують замовлення в підрядників, зобов’язані контролювати стан охорони державної таємниці, яка була передана підрядникам у зв’язку з виконанням замовлення.

У статті 37 Закону України «Про державну таємницю» зазначено, що державні органи, яким рішенням державного експерта з питань таємниць було надано право вирішувати питання про доступ державних органів, органів місцевого самоврядування, підприємств, установ, організацій до конкретної секретної інформації, зобов’язані контролювати стан охорони державної таємниці в усіх державних органах, органах місцевого самоврядування, на

підприємствах, в установах і організаціях, які виконують роботи, пов'язані з відповідною державною таємницею, або зберігають матеріальні носії зазначеної секретної інформації.

Правом контролювати стан охорони державної таємниці в усіх державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, а також у зв'язку з виконанням цих повноважень одержувати безоплатно від них інформацію з питань забезпечення охорони державної таємниці наділена Служба безпеки України. На підставі цього варто зауважити, що висновки СБУ, які містяться в актах офіційних перевірок за результатами контролю стану охорони державної таємниці, є обов'язковими для виконання посадовими особами підприємств, установ та організацій незалежно від їхніх форм власності.

Доцільно звернути увагу, що захист державної таємниці – це одна з основних функцій Служби безпеки України нарівні з контррозвідкою та боротьбою з тероризмом. Саме тому СБУ дбає про охорону секретної інформації, розголошення якої може зашкодити країні. На сьогодні захист державної таємниці є надзвичайно важливим як у зв'язку з безпрецедентною активністю російських спецслужб, так і через глобалізацію світового інформаційного простору.

Безпосередньо в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях контрольними функціями наділені РСО. Так, з метою здійснення контрольної функції РСО уповноважені здійснювати перевірки стану й організації роботи з питань захисту державної таємниці та забезпечення режиму секретності в підрозділах державного органу, органу місцевого самоврядування, підприємства, установи та організації, а також у підвідомчих їм установах та підприємствах, давати відповідні рекомендації. Також РСО здійснюють перевірки додержання режиму секретності на робочих місцях працівників, що мають допуск до державної таємниці, вмісту спецсховищ (приміщень, сейфів, металевих шаф, спецчемоданів, спецпапок тощо), наявності документів, виробів та інших матеріальних носіїв секретної інформації. Громадянин зобов'язаний повідомляти посадових осіб, які надали йому доступ до державної таємниці, та відповідні РСО про виникнення обставин, передбачених статтею 23 Закону України «Про державну таємницю»:

1) відсутності у громадянина обґрунтованої необхідності в роботі із секретною інформацією;

2) сприяння громадянином діяльності іноземної держави, іноземної організації або їхніх представників, а також окремих іноземців чи осіб без громадянства, що завдає шкоди інтересам національної безпеки України, або участі громадянина в діяльності політичних партій та громадських організацій, діяльність яких заборонена в порядку, установленому законом;

3) відмови громадянина взяти на себе письмове зобов'язання щодо збереження державної таємниці, яка буде йому довірена, а також за відсутності його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці;

4) наявності у громадянина судимості за тяжкі або особливо тяжкі злочини, не погашеної чи не знятої в установленому порядку;

5) наявності у громадянина психічних розладів, які можуть завдати шкоди охороні державної таємниці, відповідно до переліку, затвердженого Міністерством охорони здоров'я України і Службою безпеки України.

До того ж громадянин зобов'язаний повідомляти і про інші обставини, які перешкоджають збереженню довіреної йому державної таємниці, а також повідомляти в письмовій формі про свій виїзд з України.

На керівників покладено персональну відповідальність за забезпечення належного додержання режиму секретності підлеглими, за своєчасну розробку та практичне здійснення заходів захисту державної таємниці від витоку та розголошення. Керівники зобов'язані:

- постійно вивчати стан режиму секретності з метою своєчасного виявлення та перекриття можливих каналів витоку секретної інформації;
- планувати цілеспрямовані заходи щодо забезпечення зберігання державної таємниці та неухильного додержання режиму секретності;
- постійно здійснювати контроль за неухильним виконанням вимог, наказів та інструкцій, що регламентують порядок додержання режиму секретності;
- проводити роботу із запобігання необґрунтованому допуску до секретних робіт і документів;

- ретельно інструктувати працівників, які одержали через службову необхідність допуск до секретних робіт і документів;
- своєчасно інформувати керівні органи про проведення заходів щодо забезпечення режиму секретності, виявлення недоліків та їх усунення;
- забезпечувати належний режим секретності під час проведення нарад, на яких обговорюються питання, пов'язані з державною таємницею.

Крім цього, обов'язком керівників є проведення нарад із режиму секретності та контролю за додержанням режиму секретності у відповідному підрозділі, здійснення планових та позапланових (раптових) перевірок. Це спеціальні обов'язки, покладені на них, і тому вони несуть персональну відповідальність за збереження державної та службової таємниці в підлеглих їм органах.

## **8.2. КОНТРОЛЬ ЗА ТЕХНІЧНИМ ЗАХИСТОМ ІНФОРМАЦІЇ, ЯКУ ВІДНЕСЕНО ДО ДЕРЖАВНОЇ ТАЄМНИЦІ В ОРГАНАХ І ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ**

Порядок організації та здійснення контролю Національною поліцією України за станом технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, у підрозділах центрального органу управління НП України, територіальних (у тому числі міжрегіональних) органах в Автономній Республіці Крим, областях, містах Києві та Севастополі, районах, містах, районах у містах, а також установах забезпечення НП України регламентується Положенням про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України, яке затверджено наказом МВС України від 29.02.2016 № 139.

Контроль за станом технічного захисту інформації (далі – ТЗІ) в органах і підрозділах НП України здійснюється Управлінням режиму та технічного захисту інформації Національної поліції України (далі – УРТЗІ НП України).

Контроль за станом ТЗІ полягає в перевірці виконання вимог нормативно-правових актів і нормативно-технічних документів з ТЗІ та відбувається з метою

визначення стану ТЗІ в органах, щодо яких здійснюється ТЗІ, виявлення порушень з ТЗІ та запобігання ним. Ця діяльність здійснюється УРТЗІ НП України шляхом організації та проведення контрольно-інспекторської роботи з питань ТЗІ стосовно органів, щодо яких здійснюється ТЗІ.

Контроль заходів з ТЗІ в органах, щодо яких здійснюється ТЗІ, виконується відповідними підрозділами, обов'язком яких, за письмовим наказом керівника територіального (у тому числі міжрегіонального) органу поліції, є забезпечення ТЗІ в цих органах. Відповідальними особами за організацію та контроль заходів з ТЗІ в органах, щодо яких здійснюється ТЗІ, є їхні керівники.

Отже, відповідно до вимог Положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України контрольно-інспекторська робота з питань ТЗІ включає планування та проведення перевірок стану ТЗІ в органах, щодо яких здійснюється ТЗІ, аналіз їхніх результатів та надання рекомендацій щодо вдосконалення заходів з ТЗІ. За результатами контрольно-інспекторської роботи проводиться аналіз та узагальнення стану ТЗІ в органах, щодо яких здійснюється ТЗІ. У свою чергу, аналітичні матеріали щодо стану ТЗІ в органах, щодо яких здійснюється ТЗІ, доповідаються Голові НП України або його заступникові відповідно до розподілу функціональних обов'язків.

Перевірки стану ТЗІ діляться на комплексні, цільові (тематичні) та контрольні. Такі перевірки можуть бути плановими та позаплановими.

У процесі комплексної перевірки визначається відповідність комплексу ТЗІ (комплексної системи захисту інформації) вимогам нормативно-правових актів та нормативно-технічних документів системи ТЗІ. Під час проведення цільової (тематичної) перевірки перевіряються окремі складові комплексу ТЗІ (комплексної системи захисту інформації) на відповідність упроваджених заходів вимогам нормативно-правових актів та нормативно-технічних документів системи ТЗІ. Також під час проведення контрольної перевірки визначається повнота та достатність проведених заходів щодо усунення недоліків, які були виявлені в ході проведення попередньої комплексної або цільової перевірки. Слід вказати, що контрольні перевірки проводяться після отримання письмового повідомлення про усунення недоліків.

Отже, планові перевірки здійснюються згідно з планом основних організаційних і практичних заходів УРТЗІ НП України, який затверджується начальником УРТЗІ НП України. Позапланові перевірки проводяться в разі наявності відомостей щодо порушень виконання вимог нормативно-правових актів з питань ТЗІ або в разі виникнення потреби у визначенні повноти та достатності заходів з ТЗІ, ужитих органами, щодо яких здійснюється ТЗІ. Такі перевірки можуть проводитися з попередженням або без попередження керівників органів, щодо яких здійснюється ТЗІ.

Керівництво органів, щодо яких здійснюється ТЗІ, повідомляється про проведення перевірки не менше ніж за десять діб до її початку (за винятком проведення позапланової перевірки). Безпосередньо перевірки стану ТЗІ здійснюються посадовими особами УРТЗІ НП України, на яких покладено виконання завдань щодо здійснення контролю за станом ТЗІ. Підставою для допуску посадових осіб УРТЗІ НП України до перевірки та надання документів, необхідних для її проведення (у тому числі з обмеженим доступом), є наявність припису на проведення перевірки, форму якого визначено у додатку до цього Положення, за підписом Голови НП України або його заступника відповідно до розподілу функціональних обов'язків, та інших документів з дотриманням вимог законодавства про державну таємницю.

Окремо слід вказати, що перевірки Департаменту оперативної служби Національної поліції України, Департаменту оперативно-технічних заходів Національної поліції України та Департаменту кримінальної розвідки Національної поліції України здійснюються за приписом на проведення перевірки, підписаним Головою НП України або його заступником, який відповідно до розподілу функціональних обов'язків координує та контролює діяльність цих Департаментів.

Для проведення перевірки стану ТЗІ посадові особи УРТЗІ НП України пред'являють керівникові органу, щодо якого здійснюється ТЗІ, або особі, яка виконує його обов'язки, припис на проведення перевірки та службові посвідчення. Під час проведення перевірки стану ТЗІ контролю підлягають повнота та достатність упроваджених на об'єктах інформаційної діяльності заходів з ТЗІ, їх відповідність вимогам нормативно-правових актів, виконання рекомендацій щодо усунення порушень з ТЗІ. За результатами перевірок

посадовими особами УРТЗІ НПУ у довільній формі складається відповідна довідка про результати перевірки стану ТЗІ.

Безпосередньо в цій довідці мають бути відображені такі напрями роботи:

- організаційні заходи щодо забезпечення ТЗІ;
- заходи з технічного захисту мовної інформації;
- заходи з технічного захисту інформації, яка обробляється в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, засобах розмноження документів та інших технічних засобах, що використовуються для обробки інформації;
- заходи з технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, під час організації проектування будівництва, реконструкції та капітального ремонту об'єктів інформаційної діяльності;
- заходи з технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, під час прийому іноземних делегацій, іноземців та осіб без громадянства.

Варто зауважити, що довідки про результати перевірок стану ТЗІ готуються у двох примірниках. Перший примірник довідки про результати перевірки надсилається до органу, щодо якого здійснюється ТЗІ, другий – до УРТЗІ НП України.

На підставі аналізу здійснення контролю Національною поліцією України за станом технічного захисту державних інформаційних ресурсів та інформації, вимогу щодо захисту якої встановлено законом, у підрозділах НП України слід вказати категорії порушення ТЗІ. Так, відповідно до вимог зазначеного нормативно-правового акта порушення ТЗІ діляться на три категорії, які визначають можливість реалізації загроз безпеці інформації:

- перша категорія – невиконання вимог нормативно-правових актів та нормативно-технічних документів з ТЗІ, унаслідок чого створюється реальна загроза порушення конфіденційності (зокрема завдяки витоку (просочення) технічними каналами) та (або) цілісності й доступності інформації;
- друга категорія – невиконання вимог нормативно-правових актів та нормативно-технічних документів з ТЗІ, унаслідок чого створюються

передумови для порушення конфіденційності (зокрема за рахунок витоку (просочення) технічними каналами) та (або) цілісності й доступності інформації;

- третя категорія – невиконання інших вимог з ТЗІ.

Положенням про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України встановлено кваліфікаційні ознаки порушень ТЗІ:

1) ознаки порушень першої категорії:

- установлення факту циркуляції інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, на об'єктах інформаційної діяльності, в інформаційних або інформаційно-телекомунікаційних системах за умови підтвердження інструментально-розрахунковими методами наявності технічного каналу витоку інформації;
- установлення факту обробки інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних або інформаційно-телекомунікаційних системах, які мають вихід незахищеними каналами зв'язку за межі контрольованої зони, за умови відсутності атестата відповідності на комплексну систему захисту інформації;
- установлення факту обробки інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних або інформаційно-телекомунікаційних системах, які не мають виходу за межі контрольованої зони, за умови доступу до її інформаційних ресурсів користувачів, які мають різні повноваження (права доступу до інформації), та за умови відсутності атестата відповідності на комплексну систему захисту інформації;
- установлення факту обробки державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, які мають підключення до телекомунікаційних мереж (у тому числі телекомунікаційних мереж загального користування), за умови відсутності атестата відповідності на комплексну систему захисту інформації;
- установлення факту несанкціонованого доступу користувачів інформаційних, телекомунікаційних або інформаційно-телекомунікаційних систем до державних інформаційних ресурсів або

інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, шляхом порушення встановлених правил розмежування доступу або подолання заходів захисту;

2) ознаки порушень другої категорії:

- установлення факту циркуляції державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, на об'єктах інформаційної діяльності, в інформаційних або інформаційно-телекомунікаційних системах за умови відсутності підтвердження інструментально-розрахунковими методами відповідності комплексу ТЗІ нормам та вимогам з ТЗІ;
- установлення факту обробки державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, в інформаційних або інформаційно-телекомунікаційних системах, які мають вихід за межі контрольованої зони захищеними каналами, за умови відсутності атестата відповідності на комплексну систему захисту інформації;
- установлення факту обробки державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних або інформаційно-телекомунікаційних системах, які не мають виходу за межі контрольованої зони, за умови відсутності атестата відповідності на комплексну систему захисту інформації;
- сукупність невиконаних організаційних заходів з ТЗІ, що унеможливорює створення та функціонування комплексної системи захисту інформації;

3) невиконання вимог нормативно-правових актів щодо впровадження організаційних заходів з ТЗІ, а також інших норм та вимог у сфері захисту інформації, що не призводить до порушень першої або другої категорії, кваліфікується як порушення третьої категорії.

Посадові особи органів, щодо яких здійснюється ТЗІ, під час перевірки зобов'язані надавати всі необхідні для проведення перевірки документи та забезпечувати умови для її проведення. Під час проведення перевірок формулюється висновок перевірки, у якому надано оцінку стану ТЗІ, зазначено повноту та достатність заходів щодо впровадження комплексу ТЗІ (комплексної системи захисту інформації) та їх відповідність вимогам нормативно-правових

актів з ТЗІ. Основним критерієм відповідності стану ТЗІ вимогам нормативно-технічних документів та нормативно-правових актів є відсутність порушень ТЗІ.

Висновок за результатами контрольної перевірки, крім оцінки стану ТЗІ, відображає повноту виконання рекомендацій (виконано, не виконано, виконано не в повному обсязі) щодо відповідності стану ТЗІ вимогам нормативно-правових актів та нормативно-технічних документів з ТЗІ, наданих у довідці попередньої перевірки. Також визначається оцінка стану ТЗІ в окремих напрямках організації роботи та складових комплексу ТЗІ (комплексної системи захисту інформації), що перевірялися. До того ж з метою погодження стану ТЗІ з вимогами нормативно-правових актів та нормативно-технічних документів з ТЗІ посадові особи УРТЗІ НП України, які здійснювали перевірку, у довідці про результати перевірки надають конкретні рекомендації щодо усунення виявлених порушень, виконання яких є обов'язковим для посадових осіб органів, щодо яких здійснюється ТЗІ. Крім того, для з'ясування причин, які призвели до порушень першої категорії, а також притягнення осіб, які їх учинили, до відповідальності посадовими особами УРТЗІ НП України ініціюється проведення відповідних службових розслідувань (перевірок). Службові розслідування (перевірки) можуть також ініціюватися під час порушень другої категорії в разі встановлення факту обробки інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, на неатестованих об'єктах інформаційної діяльності.

Керівники органів, щодо яких здійснюється ТЗІ, зобов'язані з метою погодження стану ТЗІ з вимогами нормативно-правових актів та нормативно-технічних документів з ТЗІ, а також виконання рекомендацій, наданих за результатами перевірки, у місячний строк після отримання довідки про результати перевірки затвердити план усунення недоліків, один примірник якого надсилається до УРТЗІ НП України. За результатами проведення заходів, визначених планом усунення недоліків, до УРТЗІ НП України в строки, зазначені у довідці про результати перевірки, надсилається повідомлення про виконання рекомендацій щодо погодження стану ТЗІ з вимогами нормативно-правових актів та нормативно-технічних документів з ТЗІ.

## **§ 9. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ РЕЖИМУ СЕКРЕТНОСТІ**

### **9.1. ЗАГАЛЬНІ ПІДСТАВИ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ ЗА ПОРУШЕННЯ РЕЖИМУ СЕКРЕТНОСТІ**

Спеціальні нормативні акти передбачають диференційовану відповідальність за порушення вимог режиму секретності. Диференціюючи відповідальність, слід звертати увагу передусім на ступінь секретності розголошеної інформації, а також форму і вид вини посадової особи.

У кожному конкретному випадку підлягають відповідальності лише ті особи, кому була довірена або стала відома інформація по службі чи роботі. Установивши факт порушення режиму секретності, необхідно довести вину конкретної особи.

Слід визнати, що загроза цих порушень є об'єктивно великою, оскільки вони становлять суспільну небезпеку. Тому кримінальний закон передбачає відповідальність у разі наявності або умисної форми вини, або через необережність.

Насамперед необхідно визначити основні ознаки юридичної відповідальності:

- є засобом охорони встановленого державою правопорядку;
- є нормативно визначеною і полягає в застосуванні (реалізації) санкцій правових норм;
- є наслідком протиправного діяння;
- супроводжується державним і громадським осудом правопорушника і вчиненого ним діяння;
- пов'язана з примусом, з негативними для правопорушника наслідками (морального або матеріального характеру), яких він має зазнати;
- реалізується у відповідних процесуальних формах.

Стаття 39 Закону України «Про державну таємницю» регламентує загальні відповідальності за порушення законодавства про державну таємницю. Саме тому посадові особи та громадяни винні в:

- розголошенні державної таємниці;
- утраті документів та інших матеріальних носіїв секретної інформації;
- недодержанні встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;
- засекречуванні інформації, зазначеної у частинах третій і четвертій статті 8 Закону України «Про державну таємницю»;
- навмисному невіднесенні до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України, а також необґрунтованому заниженні ступеня секретності або необґрунтованому розсекречуванні секретної інформації;
- безпідставному засекречуванні інформації, у тому числі з порушенням вимог Закону України «Про доступ до публічної інформації»;
- наданні грифа секретності матеріальним носіям інформації, яка не становить державної таємниці, або ненаданні грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставному скасуванні чи зниженні грифа секретності матеріальних носіїв секретної інформації;
- порушенні встановленого законодавством порядку надання допуску та доступу до державної таємниці;
- порушенні встановленого законодавством режиму секретності та невиконанні обов'язків щодо збереження державної таємниці;
- невжитті заходів щодо забезпечення охорони державної таємниці та незабезпеченні контролю за охороною державної таємниці;
- провадженні діяльності, пов'язаної з державною таємницею, без одержання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщенні державних замовлень на виконання робіт, доведенні мобілізаційних завдань, пов'язаних з державною таємницею, в державних органах, органах

місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

- недодержанні вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства і проведення роботи з ними;
- невиконанні норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї інформації або просочення її технічними каналами – несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно із законом.

Наприклад, стаття 12 Дисциплінарного статуту Національної поліції України дисциплінарний проступок визнає як протиправну винну дію чи бездіяльність поліцейського, що полягає в порушенні ним службової дисципліни, невиконанні чи неналежному виконанні обов'язків поліцейського або виходить за їхні межі, порушенні обмежень та заборон, визначених законодавством для поліцейських, а також у вчиненні дій, що підривають авторитет поліції. За наявності даних про розголошення поліцейськими конфіденційної, таємної, службової або іншої інформації, яка містить таємницю, що охороняється законом, призначається службове розслідування. Порядок проведення службових розслідувань у Національній поліції України затверджений наказом МВС України від 07.11.2018 р. № 893 «Про реалізацію окремих положень Дисциплінарного статуту Національної поліції України».

**Службове розслідування** – це діяльність зі збирання, перевірки та оцінки матеріалів і відомостей про дисциплінарний проступок поліцейського, яка проводиться з метою своєчасного, повного та об'єктивного з'ясування всіх обставин учинення поліцейським дисциплінарного проступку, встановлення причин і умов його вчинення, вини, ступеня тяжкості дисциплінарного проступку, розміру заподіяної шкоди та для підготовки пропозицій щодо усунення причин вчинення дисциплінарних проступків. Службове розслідування призначається за письмовим наказом керівника, якому надані повноваження із застосування до поліцейського дисциплінарного стягнення.

## 9.2. АДМІНІСТРАТИВНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ РЕЖИМУ СЕКРЕТНОСТІ

Стаття 212-2 Кодексу України про адміністративні правопорушення передбачає підстави адміністративної відповідальності за порушення законодавства про державну таємницю, а саме:

1) недодержання встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

2) засекречування інформації:

- про стан довкілля, якість харчових продуктів і предметів побуту;
- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися та загрожують безпеці громадян;
- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти та культури населення;
- про факти порушень прав і свобод людини та громадянина;
- про незаконні дії органів державної влади, органів місцевого самоврядування та їхніх посадових осіб;
- іншої інформації, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена;

3) безпідставне засекречування інформації;

4) надання грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненадання грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставне скасування чи зниження грифа секретності матеріальних носіїв секретної інформації;

5) порушення встановленого законодавством порядку надання допуску та доступу до державної таємниці;

6) нежиття заходів щодо забезпечення охорони державної таємниці та незабезпечення контролю за охороною державної таємниці;

7) провадження діяльності, пов'язаної з державною таємницею, без отримання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщення державних замовлень на виконання робіт,

доведення мобілізаційних завдань, пов'язаних з державною таємницею, в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

8) недодержання вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців й осіб без громадянства та проведення роботи з ними;

9) невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності.

Кваліфікуючою ознакою такого адміністративного правопорушення є повторне протягом року вчинення порушення з переліку передбачених частиною першою цієї статті, за яке особу вже було піддано адміністративному стягненню.

Стаття 212-5 Кодексу України про адміністративні правопорушення передбачає підстави адміністративної відповідальності за порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію.

Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану під час оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до розголошення такої інформації, – тягне за собою накладення штрафу на громадян від двадцяти до сорока неоподатковуваних мінімумів доходів громадян і на посадових осіб – від шістдесяти до ста шістдесяти неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення, передбаченого частиною першою цієї статті, за яке особу вже було піддано адміністративному стягненню, – тягне за собою накладення штрафу на громадян від сорока до ста сорока неоподатковуваних мінімумів доходів громадян і на посадових осіб – від ста шістдесяти до двохсот шістдесяти неоподатковуваних мінімумів доходів громадян (пропоную повністю вказати текст статті).

Відповідно до статті 255 Кодексу України про адміністративні правопорушення на працівників Служби безпеки України покладено зобов'язання складати протоколи про вчинення адміністративних правопорушень у сфері державної таємниці.

### **9.3. КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ РЕЖИМУ СЕКРЕТНОСТІ**

Розділом XIV Кримінального кодексу України (далі – КК України) передбачено кримінальну відповідальність за злочини у сфері охорони державної таємниці. Родовим об'єктом цих злочинів є сукупність суспільних відносин, що забезпечують обороноздатність України, її незалежність, територіальну цілісність і недоторканність. Важливість цього об'єкта зумовлено тим, що відповідно до конституційних положень (ст. 17) захист інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу.

Кримінальна відповідальність за порушення режиму секретності передбачена статтями 328, 329, 330 КК України.

#### **Стаття 328. Розголошення державної таємниці**

1. Розголошення відомостей, що становлять державну таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства – карається позбавленням волі на строк від двох до п'яти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

2. Те саме діяння, якщо воно спричинило тяжкі наслідки, – карається позбавленням волі на строк від п'яти до восьми років.

**Безпосереднім об'єктом** цього злочину є суспільні відносини з охорони державної таємниці в різних сферах діяльності держави, що можна охарактеризувати як відносини інформаційної безпеки. У разі посягання на цей об'єкт може заподіюватися шкода військовому, економічному, науковому потенціалу держави. Зберігання державної таємниці – одна з гарантій незалежності України, її недоторканності та національної безпеки.

**Предметом** цього кримінального правопорушення є відомості, що становлять державну таємницю.

**Об'єктивний бік** злочину, передбаченого в ч. 1 ст. 328 КК України, визначено як розголошення відомостей, що становлять державну таємницю, тобто протиправне доведення їх до відома сторонніх осіб (хоча б однієї особи). Сторонні особи – це особи, яким ці відомості не повинні бути відомими. Розголошення може виражатися як у дії, так і бездіяльності. Дія може виявлятися, наприклад, у розголошенні секретних даних у розмові, письмовому повідомленні, шляхом публікації у пресі, у виступі по радіо чи телебаченню, у передачі для друкування особі, яка не має права на ознайомлення з цими відомостями, у показі креслень, документів та ін. Бездіяльність може полягати в недотриманні правил збереження, обігу, перевезення матеріалів, документів, коли створюється можливість ознайомлення з відомостями сторонніх осіб. Спосіб розголошення для кваліфікації значення не має. Злочин вважається закінченим з моменту розголошення відомостей, тобто коли вони стали відомі хоча б одній сторонній особі.

**Суб'єктивний бік** цього злочину – це будь-яка форма вини: як умисел (прямий чи непрямий), так і необережність (самовпевненість чи недбалість).

Обов'язковою ознакою вини є усвідомлення суб'єктом того, що відомості, які розголошуються, становлять державну таємницю, і що вони доводяться до відома сторонніх осіб. Так, розголошення відомостей буде вчинене з прямим умислом, якщо суб'єкт бажав похвалитися про наявність у нього інформації про державну таємницю. Недбалість наявна, наприклад, у разі, коли особа, приймаючи відвідувачів, не ховає зі столу документ, котрий містить державну таємницю, що дає можливість прочитати його стороннім особам.

**Мотиви й мета** розголошення можуть бути різними і на кваліфікацію вчиненого за ст. 328 КК України не впливають. Винятком є мета ослаблення держави та мета передачі відомостей, що становлять державну таємницю, іноземній державі, іноземній організації або їх представникам, які є обов'язковими ознаками державної зради або шпигунства як злочинів проти основ національної безпеки України.

**Суб'єкт злочину** спеціальний – це особа, якій відомості, що містять державну таємницю, були довірені або стали відомі у зв'язку з виконанням службових обов'язків. Це може бути як службова особа, так і інша особа, пов'язана по службі з такими відомостями (секретар, шифрувальник тощо).

Військовослужбовець за розголошення відомостей військового характеру, що становлять державну таємницю, відповідає за ст. 422 КК України.

Частина 2 ст. 328 КК України передбачає кваліфікаційну ознаку розголошення державної таємниці – спричинення тяжких наслідків. Закон не розкриває зміст поняття тяжких наслідків, його треба визначати на основі або підставі конкретних матеріалів справи (оцінке поняття). Це випадки, коли дані, наприклад, стали відомі іноземній розвідці чи її представникам або коли розголошені відомості за своїм змістом є особливо важливими (наприклад, особливо важливі дані про новітні розробки у сфері оборони).

### **Стаття 329. Втрата документів, що містять державну таємницю**

1. Втрата документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, а також предметів, відомості про які становлять державну таємницю, особою, якій вони були довірені, якщо втрата стала результатом порушення встановленого законом порядку поводження із зазначеними документами та іншими матеріальними носіями секретної інформації або предметами, – карається позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

2. Те саме діяння, якщо воно спричинило тяжкі наслідки, – карається позбавленням волі на строк від двох до п'яти років.

**Об'єкт** цього злочину збігається з об'єктом розголошення державної таємниці (див. коментар до ст. 328 КК України).

**Предметом** означеного злочину є:

1) документи, тобто письмові, з певними реквізитами акти, що містять відомості, які становлять державну таємницю (схеми, карти, накази, звіти, наукові висновки тощо);

2) інші матеріальні носії секретної інформації (дискети, кінофільми та ін.);

3) предмети, відомості про які є державною таємницею (наприклад, нові види зброї, прилади, медичні препарати тощо).

За характером предмета слід відрізняти ст. 329 КК України від ст. 328 КК України, у якій предметом є відомості, які містять державну таємницю.

**З об'єктивного боку** цей злочин характеризується сукупністю трьох обов'язкових ознак:

1) порушення встановленого законом порядку поводження з документами, матеріальними носіями інформації або предметами;

2) втрата документа або предмета;

3) причинного зв'язку між порушенням правил і втратою.

Порушення встановленого порядку поводження з документами або предметами може виражатися як у дії, так і в бездіяльності, що порушують конкретні правила, спеціально встановлені для охорони документів, носіїв інформації, предметів, унаслідок чого вони втрачаються, тобто виходять із володіння особи, якій вони були довірені (десь забуті, викрадені, випадково викинуті тощо). Порушення правил, наприклад, може виражатися в роботі з документом у неналежному місці; залишення відкритим сейфа, де зберігаються документи, предмети та ін. Між порушенням правил і втратою повинен бути встановлений необхідний причинний зв'язок.

**Обов'язковою умовою втрати** є вихід документів, предметів з володіння особи, якій вони були довірені, поза її волею. Якщо ж предмет переданий, залишений за волею особи, і відомості стали надбанням сторонніх осіб, то це є розголошенням відомостей, що становлять державну таємницю, і кваліфікується за ст. 328 КК України. Тривалість часу, на який були втрачені документи, предмети (назавжди або через деякий час повернуті, знайдені), не має значення.

Закінченим цей злочин є з моменту втрати, за якої створена реальна можливість ознайомлення з названими документами, предметами сторонніх осіб (тобто фактичне ознайомлення сторонніх осіб зі змістом документів, предметів не є обов'язковим). Якщо втрата такої реальної можливості не містила, то склад злочину, що аналізується, відсутній. Наприклад, якщо внаслідок порушення

правил поведження предмет був знищений, то особа не може відповідати за ст. 329 КК України. У разі наявності ознак службового злочину відповідальність може наставати за ст. 367 КК України.

**Із суб'єктивного боку** втрата документів, що містять державну таємницю, характеризується складною (змішаною) формою вини: до порушення правил можливий як умисел, так і необережність, а до самої втрати – тільки необережність.

**Суб'єктом** злочину є особа, якій документи, матеріальні носії секретної інформації, предмети, були довірені. Це може бути обумовлено або службовими функціями, або виконуваною роботою, або окремим дорученням.

Військовослужбовець за втрату документів, що містять відомості військового характеру, відповідає за ст. 422 КК України.

Частина 2 ст. 329 КК України передбачає як кваліфікаційну ознаку спричинення тяжких наслідків, характеристика яких аналогічна тій, що надана під час аналізу такої самої ознаки розголошення державної таємниці.

### **Стаття 330. Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни**

1. Передача або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства, – караються обмеженням волі на строк до трьох років або позбавленням волі на строк від двох до п'яти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

2. Ті самі дії, учинені з корисливих мотивів, або такі, що спричинили тяжкі наслідки для інтересів держави, або вчинені повторно, або за попередньою змовою групою осіб, – караються позбавленням волі на строк від чотирьох до

восьми років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

**Безпосередній об'єкт** цього злочину збігається з об'єктом злочину, передбаченого в ст. 328 КК України.

**Предметом** зазначеного злочину є відомості економічного, науково-технічного й іншого характеру, що становлять конфіденційну інформацію, яка є власністю держави, тобто відомості, що стосуються діяльності окремих підприємств, установ, наукових, господарських організацій, дипломатичних відносин, політики, розголошення яких може завдати шкоди діяльності цих організацій і вплинути на обороноздатність держави. Конфіденційна інформація характеризується обов'язковою сукупністю трьох ознак:

1) вона не містить у собі державної таємниці (що відрізняє ст. 330 КК України від ст. 328; ст. 329 КК України);

2) вона є власністю держави;

3) вона є обмеженою для користування: заборона на її передачу іноземним підприємствам, установам, організаціям або їх представникам міститься в наказах, інструкціях, розпорядженнях міністерств і відомств.

**Об'єктивний бік** злочину виражається у двох формах:

1) передача іноземним підприємствам, установам, організаціям відомостей, що становлять конфіденційну інформацію, будь-яким способом (повідомлення по телефону, у листі, на дискеті тощо);

2) збирання зазначених відомостей з метою їхньої передачі. Способи збирання можуть бути різними (викрадення, фотографування, підслуховування тощо) і на кваліфікацію не впливають.

Злочин вважається закінченим або з моменту передачі, або з моменту початку збирання відомостей з метою їхньої передачі. Не має значення, за чиєю ініціативою збираються відомості: або за ініціативою іноземної організації, або особа сама за власною ініціативою збирає їх.

**Суб'єктивний бік** виражається в прямому умислі, за якого особа, насамперед, усвідомлює конфіденційний характер інформації й те, що ця інформація є власністю держави. Це усвідомлення зумовлено тим, що особи, які працюють з такою інформацією, підлягають обов'язковому ознайомленню під розписку про конфіденційність інформації та встановлені правила щодо

користування нею, наприклад, заборонаю виносити за межі службового приміщення документи з такою інформацією, розмножувати їх технічними засобами, які не обладнані спеціальними пристроями охорони тощо.

Обов'язковим є й усвідомлення винним того, що відомості передаються або збираються для передачі саме іноземним підприємствам, установам, організаціям або їх представникам (це можуть бути будь-які іноземні організації: як державні, так і недержавні – наукові, комерційні, посередницькі тощо).

**Із суб'єктивного боку** передача або збирання конфіденційної інформації не повинні містити ознак державної зради або шпигунства, тобто умисел не повинен бути спрямованим на завдання шкоди основам національної безпеки України.

**Суб'єкт злочину спеціальний** – особа, якій конфіденційна інформація була довірена або стала відома у зв'язку з виконанням службових обов'язків.

Частина 2 ст. 330 КК України передбачає відповідальність за ті самі дії, учинені з корисливих мотивів, або такі, що спричинили тяжкі наслідки для інтересів держави, або вчинені повторно, або за попередньою змовою групою осіб. Корисливий мотив означає спрямованість передачі або збирання інформації на одержання матеріальної вигоди (грошей, майна, вигод майнового характеру) або звільнення від обов'язків матеріального характеру (наприклад, у рахунок погашення боргу).

Отже, втрата чи розголошення державної таємниці через службову недбалість або в інтересах іноземних спецслужб передбачає кримінальну відповідальність. Так, за інформацією Служби безпеки України тільки протягом 2019 року СБУ локалізувала понад 2 тисячі передумов для витоку секретної інформації.

## **§ 10. КОНТРОЛЬ УСПІШНОСТІ**

### **10.1. ДІАГНОСТИКА УСПІШНОСТІ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Контроль успішності навчальної діяльності здобувачів вищої освіти з навчальної дисципліни поєднує теоретичний матеріал курсу «Режим секретності», контрольні заходи й аналітичну роботу.

Академічні успіхи здобувачів вищої освіти визначаються за допомогою контрольних заходів, передбачених навчальним планом, обов'язковим переведенням підсумкових оцінок у національну шкалу та шкалу ECTS.

Контрольні заходи охоплюють поточний, модульний (рубіжний) та підсумковий контроль. Поточний контроль проводиться для перевірки засвоєння знань, умінь і навичок з кожної теми навчальної дисципліни. Форми поточного контролю спрямовуються на якість виконання самостійної роботи, підготовку до семінарських / практичних занять та перевірку рівня знань під час аудиторних занять.

Науково-педагогічні працівники повинні довести критерії оцінювання з модулю «Режим секретності» (роботу на лекційних, семінарських (практичних) заняттях, виконання самостійних навчальних та індивідуальних творчих завдань, модульного контролю) до відома здобувачів вищої освіти на початку вивчення навчальної дисципліни.

У ході поточного контролю здійснюється систематичне вимірювання приросту знань та їхня корекція. Поточний контроль проводиться під час лекційних, семінарських занять з метою перевірки знань курсантів з окремих тем та рівня їхньої підготовленості до виконання конкретної роботи. У процесі поточного контролю успішності та якості підготовки визначається ступінь засвоєння навчального матеріалу, своєчасно виявляються недоліки в підготовці та вживаються необхідні заходи, пов'язані з удосконаленням методики викладання, оптимізації роботи курсантів під час навчальних занять, надається

індивідуальна допомога. Оцінки, отримані курсантами, проставляються викладачами в журналах обліку відвідування та успішності кожної навчальної групи / взводу. Одним з видів поточного контролю є тестовий зріз перевірки знань з дисципліни.

## **10.2. ТЕСТОВІ ЗАВДАННЯ З КУРСУ «РЕЖИМ СЕКРЕТНОСТІ»**

**1. Відповідно до Закону України «Про державну таємницю» оберіть правильне визначення поняття «режим секретності»:**

- а) встановлений згідно з вимогами Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці;
- б) встановлений згідно з вимогами нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці;
- в) встановлений згідно з вимогами Закону єдиний порядок забезпечення охорони державної таємниці.

**2. Звід відомостей, що становлять державну таємницю – це:**

- а) акт, у якому зведено переліки відомостей, що становлять державну таємницю у сфері оборони, охорони правопорядку та здійснення оперативно-розшукової діяльності;
- б) акт, у якому зведено переліки відомостей, що становлять державну таємницю у сфері охорони правопорядку;
- в) акт, у якому зведено переліки відомостей, що згідно з рішенням державних експертів з питань таємниць, що становлять державну таємницю у сферах, визначених Законом України «Про державну таємницю».

**3. Звід відомостей, що становлять державну таємницю, формує та публікує на підставі рішень державних експертів з питань таємниць:**

- а) Верховна Рада України;
- б) Служба безпеки України;
- в) Міністерство юстиції України.

**4. До державної таємниці належить інформація:**

- а) у сфері оборони, у сфері економіки, науки і техніки, у сфері зовнішніх відносин, у сфері державної безпеки та охорони правопорядку;
- б) у сфері охорони правопорядку, здійснення оперативно-розшукової діяльності, діяльності державних органів та органів місцевого самоврядування;
- в) у сфері оборони, науки і техніки.

**5. Чи належить до державної таємниці інформація стосовно стану довкілля, харчових продуктів і предметів побуту:**

- а) ні;
- б) так;
- в) так, залежно від санітарних норм.

**6. Чи належить до державної таємниці інформація про факти порушення прав і свобод людини та громадянина:**

- а) ні;
- б) так;
- в) так, за рішенням прокурора.

**7. Інформація зі ступенем секретності «особливої важливості» має строк дії:**

- а) до 30 років;
- б) до 10 років;
- в) до 5 років.

**8. Інформація зі ступенем секретності «цілком таємно» має строк дії:**

- а) до 30 років;
- б) до 10 років;
- в) до 5 років.

**9. Інформація зі ступенем секретності «таємно» має строк дії:**

- а) до 30 років;

- б) до 10 років;
- в) до 5 років.

**10. Термін дії допуску до державної таємниці для форми 1 становить:**

- а) 5 років;
- б) 10 років;
- в) 15 років.

**11. Термін дії допуску до державної таємниці для форми 2 становить:**

- а) 5 років;
- б) 7 років;
- в) 15 років.

**12. Термін дії допуску до державної таємниці для форми 3 становить:**

- а) 7 років;
- б) 10 років;
- в) 15 років.

**13. Форма допуску 1 для роботи із секретною інформацією має ступені секретності:**

- а) «особливої важливості», «цілком таємно», «таємно»;
- б) «цілком таємно», «таємно»;
- в) «таємно».

**14. Форма допуску 2 для роботи із секретною інформацією має ступені секретності:**

- а) «особливої важливості», «цілком таємно», «таємно»;
- б) «цілком таємно», «таємно»;
- в) «таємно».

**15. Форма допуску 3 для роботи із секретною інформацією має ступені секретності:**

- а) «особливої важливості», «цілком таємно», «таємно»;
- б) «цілком таємно», «таємно»;
- в) «таємно».

**16. У який строк СБУ здійснює перевірку у зв'язку з допуском громадян до державної таємниці:**

- а) один рік;
- б) один місяць;
- в) за необхідності.

**17. Відповідно до яких законів України СБУ здійснює перевірку громадян у зв'язку з допуском громадян до державної таємниці:**

- а) Закону України «Про державну таємницю», Закону України «Про оперативно-розшукову діяльність»;
- б) Закону України «Про державну таємницю», Закону України «Про оперативно-розшукову діяльність», Закону України «Про інформацію»;
- в) Закону України «Про державну таємницю», Закону України «Про Національну поліцію», Закону України «Про інформацію».

**18. Допуск до державної таємниці надається відповідно до Закону України «Про державну таємницю»:**

- а) дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання;
- б) дієздатним громадянам України віком від 20 років, які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності;
- в) дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої діяльності або навчання.

**19. Допуск до державної таємниці не надається у разі:**

- а) наявності у громадянина судимості за тяжкі злочини;
- б) наявності у громадянина судимості за тяжкі злочини, не погашеної чи не знятої у встановленому порядку;
- в) наявності у громадянина судимості за нетяжкі злочини.

**20. Допуск до державної таємниці не надається у разі:**

- а) відмови громадянина взяти на себе зобов'язання щодо збереження державної таємниці, яка йому довірена;
- б) за відсутності його згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці;
- в) відмови громадянина взяти на себе письмове зобов'язання щодо збереження державної таємниці, яка йому довірена, а також за відсутності його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці.

**21. Чи надається доступ до державної таємниці іноземцям та особам без громадянства:**

- а) не надається взагалі;
- б) надається на загальних підставах;
- в) надається у виняткових випадках на підставі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

**22. Доступ до державної таємниці надається:**

- а) дієздатним громадянам України, яким надано допуск до державної таємниці;
- б) дієздатним громадянам України, які не мають допуску до державної таємниці;
- в) громадянину України, який займається науково-дослідницькою діяльністю.

**23. Чи має право Служба безпеки України контролювати стан охорони державної таємниці:**

- а) не має;

- б) так, має;
- в) так, має, але в окремих випадках.

**24. Яку відповідальність несуть особи за порушення законодавства про державну таємницю:**

- а) дисциплінарну, адміністративну, кримінальну;
- б) цивільно-правову та дисциплінарну;
- в) тільки кримінальну.

**25. Який підрозділ є головним режимно-секретним органом у системі Національної поліції України:**

- а) Управління режиму та технічного захисту інформації НП України;
- б) Департамент внутрішньої безпеки НП України;
- в) Департамент карного розшуку.

**26. Відповідно до Закону України «Про державну таємницю» оберіть правильне визначення поняття «гриф секретності»:**

- а) реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності цієї інформації;
- б) реквізит, що засвідчує допуск та доступ до секретної інформації;
- в) категорія, яка характеризує важливість інформації.

**27. Допуск до державної таємниці – це:**

- а) оформлення права громадянина на доступ до секретної інформації;
- б) надання дозволу на ознайомлення із секретною інформацією;
- в) надання дозволу на провадження діяльності, пов'язаної з державною таємницею.

**28. Який орган державної влади визначає державну політику щодо державної таємниці:**

- а) Кабінет Міністрів України;
- б) Верховна Рада України;
- в) Конституційний Суд України.

**29. Яким наказом СБУ затверджений ЗВДТ:**

- а) № 383 від 23.12.2020 р.;
- б) № 440 від 12.08.2005 р.;
- в) № 1030 від 23.10.2006 р.

**30. Які ступені секретності визначені Законом України «Про державну таємницю»:**

- а) «для службового користування», «таємно», «цілком таємно»;
- б) «таємно», «цілком таємно», «особливої важливості»;
- в) «не таємно», «таємно», «цілком таємно».

**31. Якою постановою Кабінету Міністрів України затверджено Типову інструкцію про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію:**

- а) № 736 від 19.10.2016 р.;
- б) № 1893 від 27.11.1998 р.;
- в) № 632 від 09.09.1994 р.

**32. На кого покладається відповідальність за організацію та забезпечення дотримання в установах порядку ведення обліку, зберігання та використання документів, що містять службову інформацію:**

- а) на режимно-секретний орган;
- б) на керівника установи;
- в) на заступника керівника установи.

**33. Гриф «Для службового користування» зберігається за електронним носієм інформації до:**

- а) вказівки керівника установи;
- б) пересилання до іншої установи;
- в) моменту його знищення.

**34. Яким наказом регламентується діловодство в МВС України:**

- а) № 747 від 23.08.2012 р.;

- б) № 211 від 02.04.2005 р.;
- в) № 70 від 19.02.2009 р.

**35. Технічний захист секретної інформації – це:**

- а) вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації;
- б) комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;
- в) вид організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, які блокують інформацію.

**36. Чи дозволяється надання грифу секретності, передбаченого Законом України «Про державну таємницю», матеріальним носіям іншої таємної інформації, яка не становить державної таємниці:**

- а) дозволяється за рішенням керівника установи;
- б) забороняється;
- в) дозволяється за погодженням із СБУ.

**37. За розголошення державної таємниці передбачено кримінальну відповідальність:**

- а) статтею 330 КК України;
- б) статтею 329 КК України;
- в) статтею 328 КК України.

**38. За передачу або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави, передбачено кримінальну відповідальність:**

- а) статтею 330 КК України;
- б) статтею 329 КК України;
- в) статтею 328 КК України.

**39. За втрату документів, що містять державну таємницю передбачено кримінальну відповідальність:**

- а) статтею 330 КК України;
- б) статтею 329 КК України;
- в) статтею 328 КК України.

**40. Яка стаття Кодексу України про адміністративні правопорушення регламентує підстави притягнення до адміністративної відповідальності за порушення законодавства про державну таємницю:**

- а) стаття 55 КУпАП;
- б) стаття 212-2 КУпАП;
- в) стаття 212 КУпАП.

**41. Державна таємниця – це:**

- а) вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані в порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;
- б) надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;
- в) категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях.

**42. За розголошення відомостей військового характеру, що становлять державну таємницю, або втрату документів чи матеріалів, що**

**містять такі відомості, передбачено кримінальну відповідальність:**

- а) статтею 329 КК України;
- б) статтею 422 КК України;
- в) статтею 368 КК України.

**43. Засекречування матеріальних носіїв інформації – це:**

- а) вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;
- б) зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;
- в) введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

**44. Розсекречування матеріальних носіїв інформації – це:**

- а) вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;
- б) зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;
- в) введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

**45. Державний експерт з питань таємниць – це:**

- а) посадова особа, уповноважена організовувати секретне діловодство в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях з незначним обсягом робіт, пов'язаних з державною таємницею, де штатним розписом не передбачено створення РСО;
- б) посадова особа, уповноважена здійснювати відповідно до вимог Закону України «Про державну таємницю» повноваження режимно-секретного органу в органах виконавчої, законодавчої та судової влади;
- в) посадова особа, уповноважена здійснювати відповідно до вимог Закону України «Про державну таємницю» віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування.

**46. Відповідно до вимог Закону України «Про державну таємницю» віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування здійснює:**

- а) державний експерт з питань таємниць;
- б) начальник (керівник) режимно-секретного органу;
- в) начальник управління режиму та технічного захисту інформації НП України.

**47. Єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передачі та транспортування матеріальних носіїв секретної інформації встановлюються:**

- а) Верховною Радою України;
- б) Кабінетом Міністрів України;
- в) Службою безпеки України.

**48. Призначення осіб на посади заступників керівників з питань режиму, начальників РСО та їх заступників, а також видання наказу про покладення на окремого працівника обов'язків щодо забезпечення режиму секретності здійснюється за погодженням з:**

- а) органами Служби безпеки України за погодженням з керівником органу, установи, підприємства;
- б) керівником кримінальної поліції Національної поліції України за погодженням з відповідним керівником територіального / міжрегіонального органу / підрозділу Національної поліції України;
- в) органами Служби безпеки України та РСО вищих державних органів, органів місцевого самоврядування, підприємств, установ і організацій.

**49. До складу режимно-секретного органу входять:**

- а) підрозділи режиму, секретного діловодства та інші підрозділи, що безпосередньо забезпечують охорону державної таємниці, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації;
- б) підрозділи діловодства, канцелярія та інші підрозділи, що безпосередньо забезпечують охорону таємної інформації, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації;
- в) різні підрозділи, що безпосередньо забезпечують охорону службової таємниці, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації.

**50. Охорона державної таємниці – це:**

- а) вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;
- б) комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на

запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;

- в) введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

**51. Матеріальні носії секретної інформації – це:**

- а) матеріальні об'єкти, які характеризують важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях;
- б) матеріальні об'єкти, які характеризують важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою;
- в) матеріальні об'єкти, в тому числі фізичні поля, у яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

**52. Хто визначає підстави, за якими інформацію має бути віднесено до державної таємниці:**

- а) уповноважена особа, яка має відповідний допуск до державної таємниці;
- б) державний експерт з питань таємниць;
- в) керівник режимно-секретного органу.

**53. Хто визначає ступінь секретності інформації, віднесеної до державної таємниці:**

- а) уповноважена особа, яка має відповідний допуск до державної таємниці;
- б) державний експерт з питань таємниць;
- в) керівник режимно-секретного органу.

**54. Віднесення інформації до державної таємниці здійснюється:**

- а) мотивованим рішенням державного експерта з питань таємниць за його власною ініціативою, за зверненням керівників відповідних державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян;
- б) мотивованим рішенням Служби безпеки України за результатами опрацювання звернень уповноважених осіб, яким надано допуск до державної таємниці;
- в) мотивованим рішенням керівника режимно-секретного органу за результатами висновку Служби безпеки України.

**55. На підставі та в межах якого нормативно-правового акта державні органи створюють галузеві або відомчі розгорнуті переліки відомостей, що становлять державну таємницю, а також можуть створювати міжгалузеві або міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю:**

- а) відповідного відомчого нормативно-правового акта, який затверджується наказом керівника органу, установи, підприємства;
- б) відповідної постанови Кабінету Міністрів України;
- в) Зводу відомостей, що становлять державну таємницю.

**56. Реквізити кожного матеріального носія секретної інформації складаються із:**

- а) грифа секретності, номера примірника, статті Зводу відомостей, що становлять державну таємницю, на підставі якої здійснюється засекречення та найменування посади та підпису особи, яка надала гриф секретності;
- б) грифа для службового користування, статті переліку інформації, яка віднесена до службової, посади та підпису уповноваженої особи, яка виконала документ або інший матеріальний носій інформації;
- в) грифа секретності, номера примірника, статті переліку інформації, яка віднесена до службової, посади та підпису уповноваженої

особи, яка виконала документ або інший матеріальний носій інформації.

**57. У разі неможливості нанесення безпосередньо на матеріальний носій секретної інформації реквізити матеріального носія секретної інформації мають бути зазначені в:**

- а) самому документі;
- б) записах виконавця документа;
- в) супровідних документах.

**58. З метою охорони державної таємниці впроваджуються:**

- а) загальні вимоги, які передбачають заборону друкарського оформлення та дозволяють лише рукописне оформлення матеріального носія секретної інформації;
- б) єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;
- в) єдині вимоги щодо узгодження використання суб'єктами режимно-секретної діяльності різних бланків та печаток для службового користування.

**59. З метою охорони державної таємниці впроваджуються:**

- а) відкритість, доступність інформації, свобода обміну інформацією та достовірність і повнота інформації;
- б) забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації та створення умов для формування в Україні інформаційного суспільства;
- в) режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею та спеціальний порядок допуску та доступу громадян до державної таємниці.

**60. У разі, коли за умовами своєї професійної діяльності громадянин постійно працює з відомостями, що становлять державну таємницю:**

- а) йому повинна надаватися відповідна компенсація за роботу в умовах режимних обмежень, види, розміри та порядок надання якої встановлюються Кабінетом Міністрів України;
- б) йому надається відповідна компенсація керівником органу, підрозділу установи за узгодженням з керівником режимно-секретного органу;
- в) йому повинна надаватися відповідна компенсація за роботу в умовах режимних обмежень лише співробітникам режимно-секретних органів.

### Контроль правильних відповідей

1 – а	11 – б	21 – в	31 – а	41 – а	51 – в
2 – в	12 – б	22 – а	32 – б	42 – б	52 – б
3 – б	13 – а	23 – б	33 – в	43 – в	53 – б
4 – а	14 – б	24 – а	34 – а	44 – б	54 – а
5 – а	15 – в	25 – а	35 – а	45 – в	55 – в
6 – а	16 – б	26 – а	36 – б	46 – а	56 – а
7 – а	17 – а	27 – а	37 – в	47 – б	57 – в
8 – б	18 – а	28 – б	38 – а	48 – в	58 – б
9 – в	19 – б	29 – а	39 – б	49 – а	59 – в
10 – а	20 – в	30 – б	40 – б	50 – б	60 – а

### 10.3. ЗАВДАННЯ ДЛЯ САМОКОНТРОЛЮ ЗНАНЬ

- Дайте визначення поняттю державної таємниці.
- Назвіть види таємниць, які пов'язані з професійною діяльністю.
- Що таке гриф секретності?
- Сформулюйте поняття та поясніть сутність режиму секретності.
- У чому полягає призначення режиму секретності?
- Яку інформацію відносять до державної таємниці?
- Яка інформація не належить до державної таємниці?
- Охарактеризуйте правові засади режиму секретності.

- Сформулюйте загальні положення Закону України «Про державну таємницю».
- Дайте характеристику державній політиці щодо державної таємниці.
- Визначте компетенцію органів державної влади у сфері охорони державної таємниці.
- Що є компетенцією органів місцевого самоврядування у сфері охорони державної таємниці.
- Який орган державної влади є спеціально уповноваженим у сфері забезпечення охорони державної таємниці?
- Хто зобов'язаний забезпечувати охорону державної таємниці в органах державної влади, діяльність яких пов'язана з державною таємницею?
- Хто повинен забезпечувати охорону державної таємниці в органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею?
- Які складники системи нормативно-правового забезпечення режиму секретності в Україні?
- У якому Законі України подано поняття інформації?
- Який Закон України регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці?
- Продовжить речення «Звід відомостей, що становлять державну таємницю, – це...».
- Назвіть види юридичної відповідальності за порушення режиму секретності.
- Укажіть підстави притягнення до адміністративної відповідальності за порушення режиму секретності.
- У чому полягає кримінальна відповідальність за порушення режиму секретності?
- У чому полягає дисциплінарна відповідальність за порушення режиму секретності?
- Визначте компетенцію РСО відповідно до Закону України «Про державну таємницю».
- Які обов'язки суб'єктів режимно-секретної діяльності.

- Які підрозділи входять до складу режимно-секретних органів?
- Які права мають режимно-секретні органи?
- Охарактеризуйте режимно-секретні підрозділи МВС України та Національної поліції України.
- Що таке матеріальні носії секретної інформації?
- Як здійснюється засекречування матеріальних носіїв інформації?
- Як здійснюється розсекречування матеріальних носіїв інформації?
- Дайте визначення поняттю «допуск до державної таємниці».
- Які є форми допуску до державної таємниці?
- Що передбачає надання допуску до державної таємниці?
- Коли допуск до державної таємниці не надається?
- Як здійснюється переоформлення громадянам допуску до державної таємниці?
- Укажіть підстави надання доступу до державної таємниці.
- У якій формі виконується рішення про надання доступу до секретної інформації?
- Чи може надаватися доступ до державної таємниці іноземцям та особам без громадянства?
- Назвіть обмеження для громадянина у зв'язку з допуском до державної таємниці.
- На який період громадянин може бути обмежений у праві виїзду на постійне місце проживання до іноземної держави?
- У яких випадках виїзд на постійне місце проживання до іноземної держави не обмежується?
- Що таке ступінь секретності? Яким може бути ступінь секретності?
- На якій підставі секретна інформація до скасування рішення про віднесення її до державної таємниці може бути передана іноземній державі?
- Що повинно надаватися громадянину в разі, коли за умовами своєї професійної діяльності він постійно працює з відомостями, що становлять державну таємницю?
- Який орган здійснює контроль за додержанням законодавства про державну таємницю з метою запобігання її поширенню в пресі та інших засобах масової інформації?

- Який порядок отримання літератури у спеціальній бібліотеці та роботи з нею?
- Дайте визначення поняттю «доступ громадян до державної таємниці».
- Як відбувається перевірка громадян у зв'язку з допуском їх до державної таємниці?
- Що передбачає скасування допуску до державної таємниці?
- Охарактеризуйте роботу з документами, які містять конфіденційну інформацію.
- Визначте обов'язки громадян щодо збереження державної таємниці.
- Що передбачає технічний та криптографічний захист секретної інформації?
- У чому полягає контроль за забезпеченням охорони державної таємниці?
- Назвіть основні заходи щодо забезпечення охорони державної таємниці.
- Визначте повноваження СБУ в питаннях, пов'язаних з державною таємницею.
- Визначте права та обов'язки державного експерта з питань таємниць.
- Що передбачає контроль за дотриманням режиму секретності?
- У чому полягає контроль за технічним захистом інформації, яка відноситься до державної таємниці в органах і підрозділах Національної поліції України?

## ВИСНОВКИ

Практична діяльність працівників Національної поліції України тісно пов'язана з використанням інформації, яка становить державну або службову таємницю, складанням, зберіганням і використанням документів, що містять таку інформацію.

У зв'язку з допуском до державної таємниці на працівників покладаються певні обов'язки – загальні та спеціальні. Загальні обов'язки поділяють на дві групи: перша передбачає вимоги, для додержання яких працівники мають виконувати активні позитивні дії із забезпечення режиму секретності та конспірації; друга містить обов'язки у формі правових заборон, спрямованих на необхідність утримання від певних дій, видів поведінки, що можуть спричинити розголошення секретних відомостей, втрату секретних документів або завдати іншої шкоди охороні державної таємниці.

Розглядаючи питання, пов'язані з поняттям, сутністю, призначенням, правовим регулюванням режиму секретності, допуском та доступом громадян до секретних робіт і документів, беручи за основу законодавчу та нормативну базу, визначено поняття «державна таємниця», «режим секретності», «режим секретності в НП України» тощо.

Установлено, що основним законодавчим актом у зазначеній сфері суспільних відносин є Закон України «Про державну таємницю». Особливе значення серед нормативних актів має Звід відомостей, що становлять державну таємницю, затверджений наказом СБУ від 23.12.2020 р. № 383. Також питання, пов'язані з дотриманням державної таємниці, регламентовано указами Президента України, постановами Кабінету Міністрів України. Крім того, МВС України та НП України ухвалено низку наказів, що регулюють питання дотримання режиму секретності та збереження державної таємниці в повсякденній діяльності поліцейських.

Визначено правовий статус працівників, допущених до секретних робіт і документів, їхні основні обов'язки й обмеження. У процесі службової діяльності

співробітники органів внутрішніх справ, особливо їх оперативні підрозділи, працюють з інформацією, яка не підлягає широкому розповсюдженню. Ця інформація стосується окремих форм, методів, прийомів і результатів діяльності органів внутрішніх справ щодо розв'язання завдань боротьби зі злочинністю, зміцнення правопорядку, віднесених законодавством до категорії державної таємниці.

З'ясовано, що суб'єктами режимно-секретної діяльності є органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші органи державної влади, Верховна Рада АР Крим, Рада міністрів АР Крим, органи місцевого самоврядування, підприємства, установи й організації всіх форм власності, об'єднання громадян, що провадять діяльність, пов'язану з державною таємницею. Законом України «Про державну таємницю» закріплено повноваження суб'єктів режимно-секретної діяльності. Створення, реорганізація чи ліквідація РСО здійснюються за погодженням із Службою безпеки України. У своїй роботі РСО постійно взаємодіють із СБУ.

Також охарактеризовано підстави та порядок оформлення громадянину доступу й допуску до секретних робіт і документів. Розглянуто основні обов'язки й обмеження для працівників, допущених до роботи, пов'язаної з державними таємницями.

Зроблено висновок, що розголошення, втрата такої інформації, а також відомостей про заходи, які плануються і здійснюються органами внутрішніх справ щодо забезпечення громадської безпеки й боротьби зі злочинністю, порушують їх нормальну діяльність, що значно знижує її ефективність.

Важливе значення в діяльності, пов'язаній із забезпеченням режиму секретності, має контроль за його дотриманням. Контроль за дотриманням режиму секретності здійснюється керівниками та режимно-секретними органами. Крім відомчого контролю, контрольними функціями наділені органи СБУ. З'ясовано, що на керівників покладено персональну відповідальність за забезпечення належного додержання режиму секретності в підпорядкованих їм підрозділах, своєчасну розробку та практичне здійснення заходів захисту державної таємниці від витоку та розголошення.

На основі аналізу правових засад режиму секретності було досліджено положення Кримінального кодексу України та Кодексу України про адміністративні правопорушення, що регламентують підстави та порядок притягнення до кримінальної та адміністративної відповідальності за порушення режиму секретності та розголошення державної таємниці. Спеціальними нормативними актами передбачено диференційовану відповідальність за порушення вимог режиму секретності. Законом України «Про державну таємницю» визначено підстави юридичної відповідальності за недотримання державної таємниці. Особи, винні в порушенні вимог режиму секретності, несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно із законом.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Про державну таємницю : Закон України від 21 січня 1994 р. № 3855-ХІІ. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>.
2. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-ХІІ. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2657-12>.
3. Звід відомостей, що становить державну таємницю : наказ СБУ від 23 грудня 2020 р. № 383 URL: <https://zakon.rada.gov.ua/laws/show/z0052-21#Text>.
4. Волошина М. О. Режим секретності : конспект лекцій. М. О. Волошина. Дніпро : ДДУВС, 2019. 134 с.
5. Собченко Л. І. Засади правового регулювання режиму секретності в оперативно-розшуковій діяльності підрозділів кримінальної поліції. *Форум права*. 2018. № 2. С. 151–157. URL: [http://nbuv.gov.ua/j-pdf/FP\\_index.htm\\_2018\\_2\\_20.pdf](http://nbuv.gov.ua/j-pdf/FP_index.htm_2018_2_20.pdf).
6. Усов Д. С. Захист державної таємниці за кримінальним законодавством інших країн на пострадянському просторі. *Публічне право*. 2013. № 3 (11). С. 103–109. URL: [file:///C:/Users/%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD/Downloads/pp\\_2013\\_3\\_16.pdf](file:///C:/Users/%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD/Downloads/pp_2013_3_16.pdf).
7. Охорона державної таємниці. URL: <https://ssu.gov.ua/okhrona-derzhavnoi-taiemnytsi>.
8. Охорона державної таємниці : навч. посібник / В. С. Зачепило, З. А. Шандра, І. Р. Опірський, І. Я. Тишик, Л. В. Мороз. Львів : Видавництво Львівської політехніки, 2015. 168 с.
9. Семенюк О. Г. Кримінологічний аналіз загроз у сфері охорони державної таємниці. *Інформація і право*. 2016. № 2 (17). С. 106–113. URL: [http://ippi.org.ua/sites/default/files/14\\_0.pdf](http://ippi.org.ua/sites/default/files/14_0.pdf).
10. Антонов К. В. Проблеми правової охорони інституту державної таємниці у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 2. С. 355–358. URL: [http://www.lsej.org.ua/2\\_2020/94.pdf](http://www.lsej.org.ua/2_2020/94.pdf).
11. Конституція України від 28 червня 1996 року. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>.

12. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.

13. Про доступ до публічної інформації : Закон України від 13 січня 2011 р. № 2939-VI. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>.

14. Про Дисциплінарний статут Національної поліції України : Закон України від 15 березня 2018 р. № 2337-VIII. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2337-19>.

15. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 р. № 80/94-ВР. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text>.

16. Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 р. № 2135-XII. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2135-12/conv#n49>.

17. Порядок організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях : Постанова Кабінету Міністрів України від 18.12.2013 р. № 939 (для службового користування).

18. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію : Постанова Кабінету Міністрів України від 19.10.2016 р. № 736. URL: <https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text>.

19. Деякі питання документування управлінської діяльності : Постанова Кабінету Міністрів України від 17 січ. 2018 р. № 55. URL: <https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#Text>.

20. Про затвердження Інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, у системі Міністерства внутрішніх справ України : наказ МВС України від 03.02.2017 р. № 88.

21. Кримінальний кодекс України (статті 328, 329, 330, 422) від 5 квітня 2001 р. № 2341-III (редакція від 13.08.2020). URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>.

22. Кримінальний процесуальний кодекс України (глава 40) від 13 квітня 2012 р. № 4651-VI (редакція від 13.08.2020). URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>.

23. Кодекс України про адміністративні правопорушення (статті 255, 212-2, 212-5, 212-6) від 07 груд. 1984 р. (редакція від 13.08.2020). URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>.

24. Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць : Указ Президента України від 19 трав. 2020 р. № 190/2020. URL: <https://zakon.rada.gov.ua/laws/show/190/2020#Text>.

25. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27 верес. 1999 р. № 1229/99. URL: <https://zakon.rada.gov.ua/laws/show/1229/99#Text>.

26. Положення про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці : затверджено Постановою Кабінету Міністрів України від 15.06.1994 р. № 414 (редакція від 15.01.2019). URL: <https://zakon.rada.gov.ua/laws/show/414-94-%D0%BF#Text>.

27. Порядок отримання спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею. URL: <https://ssu.gov.ua/poriadok-otrymannia-spetsialnoho-dozvolu>.

28. Про затвердження Інструкції про порядок погодження органами Служби безпеки України призначення особи на посаду заступника керівника підприємства, установи, організації з питань режиму, начальника РСО : наказ СБУ від 08.05.2015 р. № 306. URL: <https://ssu.gov.ua/npb-nakaz-306>.

29. Про затвердження форм звітів про стан забезпечення охорони державної таємниці та інструкції про порядок їх оформлення і подання : наказ СБУ від 17.01.2020 р. № 6. URL: <https://ssu.gov.ua/npb-nakazy>.

30. Інструкція про порядок оформлення та подання звіту про стан забезпечення охорони державної таємниці та узагальненого звіту про стан забезпечення охорони державної таємниці за підзвітні суб'єкти режимно-секретної діяльності : наказ СБУ від 17.01.2020 р. № 6. URL: <https://ssu.gov.ua/npb-nakazy>.

31. Про Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства : Указ Президента України від 17 липня 2006 р. № 621/2006. URL: <https://zakon.rada.gov.ua/laws/show/621/2006#Text>.

32. Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації : Указ Президента України від 14 грудня 2004 р. № 1483/2004 (редакція від 29.10.2014). URL: <https://zakon.rada.gov.ua/laws/show/1483/2004#Text>.

33. Про затвердження Положення про контроль за станом технічного захисту інформації в апараті МВС, територіальних органах з надання сервісних послуг МВС, закладах, установах і на підприємствах, що належать до сфери управління МВС : наказ МВС України від 23 грудня 2019 р. № 1082. URL: <https://zakon.rada.gov.ua/laws/show/z0038-20#Text>.

34. Правила пропускового режиму на території апарату Міністерства внутрішніх справ України : затверджені наказом МВС України від 22 квітня 2016. № 318 (редакція від 26.03.2021). URL: <https://zakon.rada.gov.ua/laws/show/z0716-16#Text>.

35. Правила з організації пропускового режиму на території та до будівель закладів вищої освіти із специфічними умовами навчання, що належать до сфери управління МВС : затверджені наказом МВС України від 31 липня 2019. № 636 (редакція від 09.03.2021). URL: <https://zakon.rada.gov.ua/laws/show/z0943-19#n13>.

36. Про внесення змін до Інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, у системі Міністерства внутрішніх справ України : наказ МВС України від 11 березня 2019 р. № 170. URL: [https://mvs.gov.ua/ua/pages/5906\\_NAKAZ\\_\\_170\\_Pro\\_vnesennya\\_zmin\\_do\\_Instrukcii\\_pro\\_poryadok\\_vedennya\\_obliku\\_zberigannya\\_vikoristannya\\_i\\_znishchennya\\_dokumentiv\\_ta\\_inshih\\_materialnih\\_nosiiv\\_informacii\\_shcho\\_mistyat\\_sluzhbovu\\_informaciyu\\_u\\_sistemi\\_Ministerstva\\_vnutrishnih\\_sprav\\_Ukraini.htm](https://mvs.gov.ua/ua/pages/5906_NAKAZ__170_Pro_vnesennya_zmin_do_Instrukcii_pro_poryadok_vedennya_obliku_zberigannya_vikoristannya_i_znishchennya_dokumentiv_ta_inshih_materialnih_nosiiv_informacii_shcho_mistyat_sluzhbovu_informaciyu_u_sistemi_Ministerstva_vnutrishnih_sprav_Ukraini.htm).

37. Про затвердження Положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України : наказ МВС України від 29 лютого 2016 р. № 139 URL: <https://zakon.rada.gov.ua/laws/show/z0431-16#Text>.

38. Положення про Управління режиму та технічного захисту інформації Національної поліції України : затверджено наказом Національної поліції України від 27 листопада 2015 р. № 122. URL: [https://www.npu.gov.ua/assets/userfiles/files/pdf/Polozhennya\\_pro\\_Upravlinnya\\_rezhimy\\_ta\\_teh\\_zahusty\\_informacii.pdf](https://www.npu.gov.ua/assets/userfiles/files/pdf/Polozhennya_pro_Upravlinnya_rezhimy_ta_teh_zahusty_informacii.pdf).

39. Про затвердження Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України : наказ МВС України від 26 грудня 2016 р. № 1351. URL: <https://www.nai.au.kiev.ua/rezhimno-sekr-ta-dokum-zabez/nakazi-mvs/nakaz-mvs-ukrayini-vid-26-gradnya-2016-roku-n-1351.pdf>.

40. Цивільний кодекс України від 16 січ. 2003 р. № 435-IV (редакція від 16.08.2020). URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>.

## ДОДАТКИ

Додаток 1

### СЛОВНИК ТЕРМІНІВ

Додаток 1.1

#### **ТЕРМІНИ ЗГІДНО З ВИМОГАМИ ЗАКОНУ УКРАЇНИ «ПРО ДЕРЖАВНУ ТАЄМНИЦЮ»**

1. **Державна таємниця (також – секретна інформація)** – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

2. **Віднесення інформації до державної таємниці** – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього.

3. **Гриф секретності** – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності цієї інформації.

4. **Державний експерт з питань таємниць** – посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування.

5. **Допуск до державної таємниці** – оформлення права громадянина на доступ до секретної інформації.

6. **Доступ до державної таємниці** – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов’язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов’язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

7. **Засекречування матеріальних носіїв інформації** – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

8. **Звід відомостей, що становлять державну таємницю**, – акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених цим Законом сферах.

9. **Категорія режиму секретності** – категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях.

10. **Криптографічний захист секретної інформації** – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

11. **Матеріальні носії секретної інформації** – матеріальні об’єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

12. **Охорона державної таємниці** – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв.

13. **Режим секретності** – встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці.

14. **Розсекречування матеріальних носіїв секретної інформації** – зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

15. **Спеціальна експертиза щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею**, – експертиза, що проводиться з метою визначення в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, передбачених цим Законом, для провадження діяльності, пов'язаної з державною таємницею.

16. **Ступінь секретності («особливої важливості», «цілком таємно», «таємно»)** – категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою.

17. **Технічний захист секретної інформації** – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Додаток 1.2

## **ТЕРМІНИ ЗГІДНО З ВИМОГАМИ ЗВОДУ ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ ДЕРЖАВНУ ТАЄМНИЦЮ (НАКАЗ СБУ ВІД 23.12.2020 № 383)**

1. **Безпека урядового або спеціального зв'язку (системи зв'язку)** – стан зв'язку (системи зв'язку), за якого забезпечується запобігання можливому витоку інформації, що передається в системі зв'язку (порушення режимів роботи системи зв'язку).

2. **Вимоги (рекомендації) щодо забезпечення захисту секретної інформації (протидії технічним розвідкам)** – встановлені характеристики, властивості, параметри, які висуваються до об'єктів інформаційної діяльності (об'єктів протидії), інформаційно-телекомунікаційних систем, засобів обробки секретної інформації, засобів і комплексів (систем) технічного захисту інформації та їх окремих складових з метою забезпечення захищеності секретної інформації.

3. **Витік секретної інформації** – неконтрольоване поширення секретної інформації, яке призводить до її несанкціонованого одержання.

4. **Відомості за окремими показниками** – відомості для засекречування у разі наявності одного з перерахованих у статті показників.

5. **Відомості за окремими складовими показниками** – відомості для засекречування у разі наявності інформації про окремі складові показники, що є невід’ємними складовими ознаками використаного терміна, що вживається у статті.

6. **Відомості за сукупністю всіх показників** – відомості для засекречування у разі наявності всіх перерахованих у статті показників.

7. **Відомості за сукупністю всіх складових показників** – відомості для засекречування у разі наявності інформації про всі складові показники, що є невід’ємними складовими ознаками використаного терміна, що вживається у статті.

8. **Ефективність технічного захисту секретної інформації (протидії технічній розвідці)** – ступінь відповідності вжитих заходів щодо технічного захисту секретної інформації (протидії технічній розвідці) установленим нормам і вимогам.

9. **Загроза для секретної інформації** – передумови витоку, можливості блокування чи порушення цілісності секретної інформації.

10. **Засоби криптографічного захисту інформації** – засоби шифрування інформації; засоби виготовлення ключових даних або ключових документів та управління ключовими даними, що використовуються в засобах криптографічного захисту інформації; засоби захисту від нав’язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізують алгоритми криптографічного перетворення інформації; засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані алгоритми криптографічного перетворення інформації.

11. **Комплекс технічного захисту інформації** – сукупність організаційних та інженерних заходів, призначених для захисту секретної інформації від витоку технічними каналами та спеціального впливу.

12. **Модель загроз для секретної інформації** – формалізований опис методів та засобів здійснення загроз для секретної інформації.

13. **Норми ефективності захисту інформації (протидії технічній розвідці)** – граничнодопустимі значення чисельних показників, виконання яких

забезпечує потрібну ефективність технічного захисту секретної інформації (протидії технічній розвідці).

**14. Об'єкт оперативно-розшукового, контррозвідального чи розвідального заходу** – фізична або юридична особа, стосовно якої здійснюється оперативно-розшукова, контррозвідальна чи розвідальна діяльність за наявності підстав, передбачених чинним законодавством України.

**15. Організація оповіщення** – комплекс заходів, які здійснюються з метою доведення до державних органів, підприємств, установ, організацій сигналів оповіщення у разі введення в державі воєнного стану та проведення мобілізації, організацій чергування та забезпечення цих органів технічними засобами зв'язку.

**16. Основні спеціальні вимоги** – вимоги до захисту інформації від витоку технічними каналами, виконання яких обов'язкове під час побудови та експлуатації систем чи комплексів урядового або спеціального зв'язку.

**17. Особливий режим діяльності** – сукупність організаційних та технічних заходів і правил, спрямованих на забезпечення режиму доступу та перебування на конкретному об'єкті.

**18. Пересилання матеріальних носіїв секретної інформації** – сукупність операцій з приймання, оброблення, перевезення та доставки (вручення) кореспонденції та інших матеріальних носіїв інформації.

**19. Система спеціального зв'язку** – сукупність обладнання, засобів, комплексів та систем обробки, передачі, технічного та криптографічного захисту інформації, що організаційно, технічно та функціонально поєднані в єдине ціле, призначена для забезпечення користувачів спеціальним зв'язком.

**20. Спеціальна перевірка** – комплекс передбачених законодавством України та відомчими нормативно-правовими актами заходів, що проводяться або проводилися у зв'язку з призначенням особи на посаду в державні органи, що здійснюють оперативно-розшукову, контррозвідальну та/або розвідальну діяльність.

**21. Спеціальні види зв'язку (спеціальний зв'язок)** – види зв'язку, під час використання яких з метою приховування змісту інформації здійснюється її криптографічне перетворювання.

**22. Спеціальні вимоги** – сукупність організаційних та інженерно-технічних вимог до умов експлуатації певного типу або зразка засобу обчислювальної техніки, виконання яких є необхідним для забезпечення захисту

інформації від витоку каналами побічних електромагнітних випромінювань та наведень, які встановлюються нормативними документами у сфері технічного захисту інформації.

**23. Спеціальні технічні засоби** – технічні засоби, устаткування, апаратура, прилади, пристрої, програмне забезпечення, препарати та інші вироби, призначені (спеціально розроблені, виготовлені, запрограмовані або пристосовані) для негласного отримання інформації.

**24. Суб'єкт режимно-секретної діяльності** – органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші органи державної влади, Верховна Рада АР Крим, Рада міністрів АР Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян, що провадять діяльність, пов'язану з державною таємницею.

**25. Технічна розвідка** – несанкціоноване здобування секретної інформації за допомогою технічних засобів та її аналіз.

**26. Технічний захист секретної інформації** – діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (або) витоку секретної інформації технічними каналами.

**27. Технічні засоби охорони** – обладнання систем охоронно-тривожної сигналізації, контролювання доступу, охоронного відеоспостереження, а також контрольно-пропускне і доглядове обладнання.

Додаток 1.3

## **ТЕРМІНИ ЗГІДНО З ВИМОГАМИ ЗАКОНУ УКРАЇНИ «ПРО ІНФОРМАЦІЮ»**

1. **Документ** – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання в часі та просторі.

2. **Захист інформації** – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

3. **Інформація** – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

4. **Суб'єкт владних повноважень** – орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

5. **Інформація про фізичну особу (персональні дані)** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

6. **Науково-технічна інформація** – будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

7. **Правова інформація** – будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

8. **Статистична інформація** – документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

9. **Соціологічна інформація** – будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо.

10. **Інформацією з обмеженим доступом** є конфіденційна, таємна та службова інформація.

11. **Конфіденційною** є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

12. **Масова інформація** – інформація, що поширюється з метою її доведення до необмеженого кола осіб.

13. **Засоби масової інформації** – засоби, призначені для публічного поширення друкованої або аудіовізуальної інформації.

14. **Інформаційна продукція** – матеріалізований результат інформаційної діяльності, призначений для задоволення потреб суб'єктів інформаційних відносин.

15. **Інформаційна послуга** – діяльність з надання інформаційної продукції споживачам з метою задоволення їхніх потреб.

**ТЕРМІНИ ЗГІДНО З ВИМОГАМИ ЗАКОНУ УКРАЇНИ «ПРО РОЗВІДКУ»**

1. **Розвідка** – організаційно-функціональне поєднання визначених цим Законом розвідувальних органів та діяльності, яку вони здійснюють самостійно або у взаємодії між собою та з іншими суб'єктами розвідувального співтовариства з метою забезпечення національної безпеки і оборони України.

2. **Розвідувальна діяльність** – система розвідувальних заходів, що проводяться розвідувальними органами України для виконання покладених на ці органи завдань та здійснення визначених цим Законом функцій.

3. **Розвідувальний захід** – комплекс дій та рішень розвідувального органу та/або у випадках, визначених Законом України «Про розвідку», іншого суб'єкта розвідувального співтовариства із застосуванням методів, сил і засобів розвідки.

4. **Розвідувальна інформація** – усні, зафіксовані на матеріальних носіях (у тому числі у зразках виробів і речовин) чи відображені в електронному вигляді відомості або дані, які не є загальнодоступними або які неможливо отримати офіційним шляхом, про наміри, плани і дії іноземних держав, організацій та осіб чи про їхні потенційні можливості щодо реалізації таких намірів і планів, а також про процеси, події, обставини, технології, знання в інтересах національної безпеки і оборони України.

5. **Розвідувальна таємниця** – вид таємної інформації, що охоплює відомості та дані, отримані або створені розвідувальними органами України під час виконання покладених на ці органи завдань та здійснення функцій, визначених Законом України «Про розвідку», розголошення яких може завдати шкоди функціонуванню розвідки і доступ до яких обмежено відповідно до цього Закону в інтересах національної безпеки України.

6. **Розвідувальні органи України** – державні органи, уповноважені Законом України «Про розвідку» здійснювати розвідувальну діяльність з метою захисту національних інтересів України від зовнішніх загроз.

7. **Сили і засоби розвідки** – співробітники розвідувальних органів та особи, залучені до конфіденційного співробітництва з цими органами, органи військового управління розвідки та військові частини розвідки, підрозділи,

підприємства, установи, організації, заклади, засоби та структури прикриття, будівлі, приміщення, транспортні засоби, інформаційні системи та бази даних, технічні засоби розвідки, озброєння, боєприпаси, військова та спеціальна техніка, спеціальні технічні засоби, інше майно, кошти в національній та іноземній валютах, які використовуються для здійснення розвідувальної діяльності або для організації чи забезпечення її здійснення, а також сили і засоби інших суб'єктів розвідувального співтовариства у випадках, визначених Законом України «Про розвідку».

8. **Спеціальні (активні) заходи** – розвідувальні заходи, спрямовані на сприяння реалізації національних інтересів України, протидію намірам, планам і діям, що створюють зовнішні загрози національній безпеці України.

Додаток 1.5

## **ТЕРМІНИ ЗГІДНО З ВИМОГАМИ ЗАКОНУ УКРАЇНИ «ПРО НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ»**

1. **Воєнна безпека** – захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від воєнних загроз.

2. **Державна безпека** – захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру.

3. **Загрози національній безпеці України** – явища, тенденції і чинники, що унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України.

4. **Національна безпека України** – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз.

5. **Сили безпеки** – правоохоронні та розвідувальні органи, державні органи спеціального призначення з правоохоронними функціями, сили цивільного захисту та інші органи, на які Конституцією та законами України покладено функції із забезпечення національної безпеки України.

6. **Сили оборони** – Збройні Сили України, а також інші утворені відповідно до законів України військові формування, правоохоронні та розвідувальні органи, органи спеціального призначення з правоохоронними функціями, на які Конституцією та законами України покладено функції із забезпечення оборони держави.

Додаток 1.6

## **ТЕРМІНИ ЗГІДНО З ВИМОГАМИ ЗАКОНУ УКРАЇНИ «ПРО НАЦІОНАЛЬНУ СИСТЕМУ КОНФІДЕНЦІЙНОГО ЗВ'ЯЗКУ»**

1. **Спеціальна телекомунікаційна система (мережа)** – телекомунікаційна система (мережа), призначена для обміну інформацією з обмеженим доступом.

2. **Спеціальна телекомунікаційна система (мережа) подвійного призначення** – спеціальна телекомунікаційна система (мережа), призначена для забезпечення телекомунікацій (електрозв'язку) в інтересах органів державної влади та органів місцевого самоврядування, з використанням частини її ресурсу для надання послуг іншим споживачам.

3. **Національна система конфіденційного зв'язку** - сукупність спеціальних телекомунікаційних систем (мереж) подвійного призначення, які за допомогою криптографічних та/або технічних засобів забезпечують обмін інформацією з обмеженим доступом, крім інформації, що становить державну таємницю в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану.

4. **Суб'єкти Національної системи конфіденційного зв'язку** – органи державної влади та органи місцевого самоврядування, юридичні та фізичні особи, що беруть участь у створенні, функціонуванні, розвитку та використанні цієї системи.

**ТЕРМІНИ ЗГІДНО З ВИМОГАМИ НАКАЗУ МВС УКРАЇНИ ВІД  
29.02.2016 № 139 «ПРО ЗАТВЕРДЖЕННЯ ПОЛОЖЕННЯ ПРО  
КОНТРОЛЬ ЗА СТАНОМ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В  
ОРГАНАХ І ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ»**

1. **Контрольно-інспекторська робота з питань ТЗІ** – діяльність, спрямована на визначення та вдосконалення стану ТЗІ в органах, щодо яких здійснюється ТЗІ.

2. **Об'єкт інформаційної діяльності** – інженерно-технічна споруда (приміщення), транспортний засіб, де провадиться діяльність, пов'язана з державними інформаційними ресурсами та інформацією, вимога щодо захисту якої встановлена законом.

3. **Передумови витоку (просочення) інформації технічними каналами** – наявність технічного каналу поширення інформації за відсутності підтвердженої відповідності впроваджених заходів вимогам та нормам з ТЗІ.

4. **Порушення у сфері ТЗІ** – невиконання вимог нормативно-правових актів та нормативно-технічних документів системи ТЗІ за категоріями, які визначають можливість реалізації загроз безпеці інформації.

5. **Реальна загроза витоку (просочення) інформації технічними каналами** – наявність технічного каналу поширення інформації за умови підтвердження відповідними інструментально-розрахунковими методами невідповідності впроваджених заходів вимогам та нормам з ТЗІ.

6. **Технічний канал витоку інформації** – сукупність джерела інформації, середовища її поширення та технічних засобів розвідки.

## ВИДИ ТАЄМНИЦЬ, ПОВ'ЯЗАНИХ З ПРОФЕСІЙНОЮ ДІЯЛЬНІСТЮ

1. **Адвокатська таємниця** – будь-яка інформація, що стала відома адвокату, помічнику адвоката, стажисту адвоката, особі, яка перебуває у трудових відносинах з адвокатом, про клієнта, а також питання, з яких клієнт (особа, якій відмовлено в укладенні договору про надання правової допомоги з передбачених Законом України «Про адвокатуру та адвокатську діяльність») звертався до адвоката, адвокатського бюро, адвокатського об'єднання, зміст порад, консультацій, роз'яснень адвоката, складені ним документи, інформація, що зберігається на електронних носіях, та інші документи і відомості, одержані адвокатом під час здійснення адвокатської діяльності (ст. 22 Закону України «Про адвокатуру та адвокатську діяльність»).

2. **Банківська таємниця** – інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам під час надання послуг банку (ст. 60 Закону України «Про банки і банківську діяльність»).

3. **Військова таємниця** – відомості військового характеру, предмети, документи або матеріали, що містять відомості військового характеру, які становлять державну таємницю (ст. 422 Кримінального кодексу України).

4. **Журналістська таємниця** – журналіст має право на збереження таємниці авторства та джерел інформації, за винятком випадків, коли ці таємниці обнародуються на вимогу суду (п. 11, ст. 26 Закону України «Про друковані засоби масової інформації (пресу) в Україні»).

5. **Комерційна таємниця** – інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці (ст. 505 Цивільного кодексу України).

6. **Лікарська таємниця** – медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків. Під час використання інформації, що становить лікарську таємницю, в навчальному процесі, науково-дослідній роботі, у тому числі у випадках її публікації у спеціальній літературі, повинна бути забезпечена анонімність пацієнта (ст. 40 Закону України «Основи законодавства України про охорону здоров'я»).

7. **Нотаріальна таємниця** – сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, в тому числі про особу, її майно, особисті майнові та немайнові права і обов'язки тощо (ст. 8 Закону України «Про нотаріат»).

8. **Публічна інформація з обмеженим доступом** – інформацією з обмеженим доступом є:

- **конфіденційна інформація** – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов (ст. 7 Закону України «Про доступ до публічної інформації»);
- **таємна інформація** – інформація, доступ до якої обмежується відповідно до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю (ст. 8 Закону України «Про доступ до публічної інформації»);
- **службова інформація** – відповідно до вимог частини другої статті 6 Закону України «Про доступ до публічної інформації» до службової може належати така інформація:
- що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами

державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

- зібрана у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

**9. Розвідувальна таємниця** – вид таємної інформації, що охоплює відомості та дані, отримані або створені розвідувальними органами України під час виконання покладених на ці органи завдань та здійснення функцій, визначених Законом України «Про розвідку», розголошення яких може завдати шкоди функціонуванню розвідки і доступ до яких обмежено відповідно до Закону України «Про розвідку» в інтересах національної безпеки України. (ст. 1 Закону України «Про розвідку»).

**10. Таємниця досудового розслідування** – відомості досудового розслідування можна розголошувати лише з письмового дозволу слідчого або прокурора і в тому обсязі, у якому вони визнають можливим. Слідчий, прокурор попереджає осіб, яким стали відомі відомості досудового розслідування, у зв'язку з участю в ньому, про їх обов'язок не розголошувати такі відомості без його дозволу (ст. 222 Кримінального процесуального кодексу України).

**11. Таємниця наради суддів** – під час ухвалення вироку ніхто не має права перебувати в нарадчій кімнаті (нарадча кімната – приміщення, спеціально призначене для ухвалення судових рішень, прим. автора), крім складу суду, який здійснює судовий розгляд. Суд вправі перервати нараду лише для відпочинку з настанням нічного часу. Під час перерви судді не можуть спілкуватися з особами, які брали участь у кримінальному провадженні. Судді не мають права розголошувати хід обговорення та ухвалення вироку в нарадчій кімнаті (ст. 367 Кримінального процесуального кодексу України).

**12. Таємниця нарадчої кімнати** – під час ухвалення судового рішення ніхто не має права перебувати в нарадчій кімнаті, крім складу суду, який розглядає справу. Під час перебування в нарадчій кімнаті суддя не має права розглядати інші судові справи. Судді не мають права розголошувати хід обговорення та ухвалення рішення у нарадчій кімнаті (ст. 245 Цивільного процесуального кодексу України, ст. 228 Кодексу адміністративного судочинства України).

**13. Таємниця сповіді** – кожному громадянину в Україні гарантується право на свободу совісті, ніхто не має права вимагати від священнослужителів

відомостей, одержаних ними при сповіді віруючих (ст. 3 Закону України «Про свободу совісті та релігійні організації»).

14. **Таємниця усиновлення** – особа має право на таємницю перебування на обліку тих, хто бажає усиновити дитину, пошуку дитини для усиновлення, подання заяви про усиновлення та її розгляду, рішення суду про усиновлення. Дитина, яка усиновлена, має право на таємницю, у тому числі і від неї самої, факту її усиновлення (ст. 226 Сімейного кодексу України).

15. **Зміст завдань сертифікаційної роботи зовнішнього незалежного оцінювання належить до інформації з обмеженим доступом** з моменту створення набору завдань сертифікаційної роботи зовнішнього незалежного оцінювання та до моменту його санкціонованого використання особами, що проходять зовнішнє незалежне оцінювання. У разі потреби спеціально уповноважена державою установа (організація) може відносити зміст завдань сертифікаційної роботи до інформації з обмеженим доступом на більш тривалий період часу (п. 8 ст. 45 Закону України «Про вищу освіту»).

*Навчальне видання*

**СЕРГІЙ ПЕТРОВИЧ ПЕКАРСЬКИЙ**

## **РЕЖИМ СЕКРЕТНОСТІ**

**НАВЧАЛЬНИЙ ПОСІБНИК**

*Підготовлено до друку ВД «Дакор»  
Друкується в авторській редакції*

Підписано до друку 24.06.2021. Гарнітура BookmanС. Формат 60x84 1/16  
Папір офсетний. Друк офсетний. Ум.-друк. Арк.8,95. Обкл. вид. арк. 8,32. Наклад 300 прим.

---

**ТОВ «ВД «Дакор»**

Свід. ДК № 4349 від 05.07.2012

(044) 461-85-06; vd\_dakor@ukr.net

04073, м. Київ, просп. Степана Бандери, 8