ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

В. І. Ящук, А. І. Івануса,
Р. Л. Ткачук, В. С. Балацька

Система охорони державної таємниці

НАВЧАЛЬНИЙ ПОСІБНИК

Львів - 2025

УДК 351.862:005.8(477)

Рецензенти: **Олег ГАРАСИМЧУК**, кандидат технічних наук, доцент кафедри захисту інформації Національного університету “Львівська політехніка”

Євген МАРТИН, доктор технічних наук, професор, професор кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

Ящук В. І., Івануса А. І., Ткачук Р. Л., Балацька В. С. *Система охорони державної таємниці: навчальний посібник* / Львівський державний університет безпеки життєдіяльності. Львів : ЛДУБЖД, 2025. 237 с.

Навчальний посібник “Системи охорони державної таємниці” присвячений комплексному аналізу правових, організаційних та технічних аспектів захисту секретної інформації. У ньому розкрито питання законодавчого регулювання охорони державної таємниці, організації режимно-секретної роботи, контролю за допуском до секретної інформації, порядку роботи з документами, що мають відповідні грифи обмеженого доступу. Особливу увагу приділено заходам технічного захисту інформації, зокрема запобіганню витоку даних через технічні канали, а також методам оцінювання ризиків інформаційної безпеки. Вивчення цієї дисципліни є необхідним для формування у здобувачів освіти професійних компетентностей у сфері захисту інформації, що забезпечує державну безпеку. Опрацювання матеріалів посібника сприятиме розумінню принципів роботи режимно-секретних органів, ефективному застосуванню нормативно-правових актів та розвитку практичних навичок з охорони державної таємниці. Посібник орієнтований на студентів, аспірантів і фахівців, що навчаються або працюють у сфері інформаційної безпеки, державного управління, оборони, національної безпеки та правоохоронної діяльності.

Рекомендовано рішенням Вченої ради Львівського державного університету безпеки життєдіяльності
(Протокол № 4 від 26.11.2025 р.)

© Ящук В. І., 2025
© Івануса А. І., 2025
© Ткачук Р. Л., 2025
© Балацька В. С., 2025
© ЛДУ БЖД, 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 7
ПЕРЕДМОВА 9
ТЕМА. 1 ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ: ПОНЯТТЯ ТА ВИДИ 11
1. Поділ та загальна характеристика інформації за режимом доступу 11
2. Державна таємниця – особливий вид таємної інформації 16
3. Поняття, правова природа та ознаки комерційної таємниці 20
4. Перелік інформації, що охороняється в режимі комерційної таємниці 24
СЕМІНАРСЬКЕ ЗАНЯТТЯ ТЕМА 1 29
ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ: ПОНЯТТЯ ТА ВИДИ 29
ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ 30
ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ 32
ТЕМА. 2 ПРАВОВИЙ ЗАХИСТ ДЕРЖАВНОЇ ТАЄМНИЦІ 41
1. Становлення системи державної таємниці в Україні 41
2. Організаційно-правові заходи охорони та захисту державної таємниці 46
3. Організаційно-правова структура системи охорони державної таємниці 48
СЕМІНАРСЬКЕ ЗАНЯТТЯ ТЕМА 2 51
ПРАВОВИЙ ЗАХИСТ ДЕРЖАВНОЇ ТАЄМНИЦІ 51
ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ 52
ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ 54
ТЕМА 3 ПРОЦЕДУРА ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ 58
1. Доекспертна стадія віднесення інформації до державної таємниці 58
2. Стадія експертного розгляду інформації для прийняття рішення про віднесення її до державної таємниці 63
3. Стадія формалізації рішення 65
4. Основні засади віднесення відомостей, що містять ознаки державної таємниці, до різних ступенів секретності 66
СЕМІНАРСЬКЕ ЗАНЯТТЯ ТЕМА 3 68
ПРОЦЕДУРА ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ 68
ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ 69
ТА ПЕРЕВІРКИ ЗНАНЬ 69
ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ 71

ТЕМА 4 ДОСТУП ДО ІНФОРМАЦІЇ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЇЇ ВИКОРИСТАННЯ 75
3. Організація допуску до відомостей, що становлять державну таємницю 83
4. Порядок отримання спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею 87
5. Обов'язкові умови, пов'язані із забезпеченням безпеки використання, збереження та захисту державної таємниці 91
6. Технічний захист інформації, що містить державну таємницю 94
СЕМІНАРСЬКЕ ЗАНЯТТЯ ТЕМА 4 98
ДОСТУП ДО ІНФОРМАЦІЇ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЇХ ВИКОРИСТАННЯ 98
ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ 100
ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ 102
ТЕМА 5 ОРГАНІЗАЦІЯ ВНУТРІШНЬООБ'ЄКТНОГО ТА ПРОПУСКНОГО РЕЖИМУ НА ПІДПРИЄМСТВАХ, ЩО ПРАЦЮЮТЬ З ВІДОМОСТЯМИ, ВИЗНАЧЕНИМИ ДЕРЖАВНОЮ ТАЄМНИЦЕЮ 106
1. Структура та повноваження режимно-секретних органів 106
2. Внутрішньооб'єктовий режим та його задачі 109
3. Підрозділи підприємства, які вирішують завдання з організації внутрішньооб'єктового режиму 114
4. Організаційні засоби захисту інформації 117
СЕМІНАРСЬКЕ ЗАНЯТТЯ ТЕМА 5 122
ОРГАНІЗАЦІЯ ВНУТРІШНЬООБ'ЄКТОВОГО ТА ПРОПУСКНОГО РЕЖИМУ НА ПІДПРИЄМСТВАХ, ЩО ПРАЦЮЮТЬ З ВІДОМОСТЯМИ, ВИЗНАЧЕНИМИ ДЕРЖАВНОЮ ТАЄМНИЦЕЮ 122
ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ 124
ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ 126
ТЕМА 6 ВЕДЕННЯ ДОКУМЕНТІВ З ГРИФОМ "ТАЄМНО" 130
1. Ведення документів з грифом секретності 130
2. Складання номенклатури секретних справ. Формування, облік, зберігання та видача секретних справ 136
СЕМІНАРСЬКЕ ЗАНЯТТЯ ТЕМА 6 139
ВЕДЕННЯ ДОКУМЕНТІВ З ГРИФОМ ТАЄМНО 139

ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ СТУДЕНТІВ 141
ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ 142
ТЕМА 7 ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ. СПОСОБИ НЕСАНКЦІОНОВАНОГО ЗНЯТТЯ ІНФОРМАЦІЇ З ТЕХНІЧНИХ КАНАЛІВ ЇЇ ВИТОКУ 146
1. Поняття технічного каналу витоку інформації та їхня класифікація 146
2. Загальний підхід до технічного захисту інформації 149
3. Фізичні основи утворення технічних каналів витоку інформації 152
4. Організаційно-технічні заходи щодо ТЗІ на об’єкті 153
5. Основи несанкціонованого зняття інформації способом та засобами високочастотного нав’язування 155
6. Класифікація каналів витоку інформації 157
СЕМІНАРСЬКЕ ЗАНЯТТЯ ТЕМА 7 161
ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ. СПОСОБИ НЕСАНКЦІОНОВАНОГО ЗНЯТТЯ ІНФОРМАЦІЇ З ТЕХНІЧНИХ КАНАЛІВ ЇЇ ВИТОКУ 161
ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ 163
ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ 165
ТЕМА 8 МЕТОДИ ТА ЗАСОБИ БЛОКУВАННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ 169
1. Основні загальні положення технічного захисту інформації 169
2. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації 171
3. Захист акустичної інформації від зняття радіозакладними пристроями. Методи пошуку радіозакладних пристроїв 176
4. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами 180
5. Захист інформації від несанкціонованого запису звукозаписувальними пристроями 182
Основні напрями захисту 182
Виявлення звукозаписувальних пристроїв 182
Придушення можливості аудіозапису 183
Організаційні заходи 183
6. Захист електронної інформації 184

7. Захист письмової інформації від оптичного зняття 187
Технічні засоби захисту 188
СЕМІНАРСЬКЕ ЗАНЯТТЯ ТЕМА 8 191
МЕТОДИ ТА ЗАСОБИ БЛОКУВАННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ 191
ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ 193
ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ 195
ТЕМА 9 ВИДИ І ПРОЦЕДУРИ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА РОЗГОЛОШЕННЯ ДЕРЖАВНОЇ ТАЄМНИЦІ 199
1. Загальні підстави застосування юридичної відповідальності за розголошення державної таємниці 199
2. Кримінальна відповідальність за розголошення державної таємниці. Втрата документів, що містять державну таємницю 200
3. Адміністративна відповідальність за порушення режиму державної таємниці 205
4. Відповідальність за розголошення державної таємниці у нормах законодавства зарубіжних країн 207
СЕМІНАРСЬКЕ ЗАНЯТТЯ ТЕМА 9 219
ВИДИ І ПРОЦЕДУРИ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА РОЗГОЛОШЕННЯ ДЕРЖАВНОЇ ТАЄМНИЦІ 219
ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ 221
ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ 222
СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ 226

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АРК – Автономна Республіка Крим

АС – Автоматизована система

ВР – Верховна Рада

ВЧ – високочастотний

ГК України – Господарський кодекс України

ДБ – державна безпека

ДОДТЛ – Департамент охорони державної таємниці та ліцензування

ДСК – для службового користування

ДССЗЗІУ – Державна служба спеціального зв'язку та захисту інформації України

ДТ – державна таємниця

ДФС – державна фельд'єгерська служба

ЗВДТ – Звід відомостей Державної таємниці

ЗМІ – засоби масової інформації

ІзОД – інформація з обмеженим доступом

ІСБ – інформаційна система безпеки

КК – Кримінальний кодекс

КМУ – Кабінет Міністрів України

КПК – Кримінальний процесуальний кодекс

КСЗІ – Комплексні системи захисту інформації

ЛДУ БЖД – Львівський державний університет безпеки життєдіяльності

МОЗ – Міністерство охорони здоров'я

МОУ – Міністерство оборони України

МФЗ – міжміський фельд'єгерський зв'язок

НБ – національна безпека

НДДКР – науково-дослідні та дослідно-конструкторські роботи

НДІ – науково-дослідний інститут

ОВВ – органи виконавчої влади

ОІД – об’єкт інформаційної діяльності

ОМС – органи місцевого самоврядування

ОРД – оперативно-розшукова діяльність

ОРЗ – оперативно-розшукові заходи

ОТЗ – оперативно-технічні заходи

ПЕОМ – персональна електронно-обчислювальна машина

ПЕМВ – побічні електромагнітні випромінювання

ПЕМВН – побічні електромагнітні випромінювання та наведення

ПУО – підприємства, установи, організації

РАЦС – реєстрація актів цивільного стану

РНБОУ – Рада національної безпеки і оборони України

РП – розгорнутий перелік

РС – режим секретності

РСВ – режимно-секретний відділ

РСО – режимно-секретні органи

СБУ – Служба безпеки України

ТЗІ – технічний захист інформації

ТЗР – технічний засіб розвідки

ТКВІ – технічний канал витоку інформації

ЦК України – Цивільний кодекс України

ЦПК – Цивільно-процесуальний кодекс

ПЕРЕДМОВА

Сучасний світ неможливо уявити без інформації, а її безпека є запорукою національної стабільності, суверенітету та розвитку суспільства. У XXI столітті інформація стала стратегічним ресурсом, не менш цінним, ніж енергетичні чи фінансові. Той, хто володіє інформацією, має владу, вплив і здатність приймати ефективні рішення. Тому захист інформації, особливо державної таємниці, посідає ключове місце в системі національної безпеки України.

Захист державної таємниці – це комплексна діяльність, що поєднує правові, організаційні, інженерні та людські чинники. Від підготовленості фахівців у цій сфері залежить ефективність системи безпеки держави, адже кожне рішення може мати далекосяжні наслідки – від збереження стратегічних переваг до запобігання загрозам обороноздатності країни.

Саме з цього розуміння виникла ідея створення навчального посібника “Система охорони державної таємниці”, покликаного стати теоретичною й практичною основою підготовки фахівців з кібербезпеки та інформаційної безпеки. Автори прагнули систематизувати законодавчі, організаційні й технічні аспекти охорони державної таємниці та подати матеріал у логічній, доступній і практично орієнтованій формі.

Посібник побудовано так, щоб студент міг крок за кроком опанувати дисципліну: від базових понять, правових норм та нормативно-правових актів – до конкретних алгоритмів і методів захисту інформації. Кожен розділ містить теоретичний матеріал, приклади з реальної практики, а також завдання для самостійної та практичної роботи. Завершують кожен тематичний блок тестові запитання, що дозволяють перевірити рівень засвоєння матеріалу та підготуватися до подальших етапів навчання.

Особливу увагу приділено поєднанню теорії з практикою. Наведені приклади впровадження заходів безпеки на об’єктах інформаційної діяльності, у державних та приватних установах дають змогу побачити, як нормативні вимоги реалізуються через розробку режиму секретності, роботу експертів, технічні та організаційні заходи контролю.

Цінність видання полягає у формуванні професійної відповідальності та усвідомлення значущості обраної справи. Охорона державної таємниці – це не

лише виконання інструкцій, а служіння державним інтересам, що потребує компетентності, дисципліни й моральної стійкості. Автори прагнули, щоб навчання стало основою формування культури інформаційної безпеки кожного майбутнього фахівця.

В умовах інформаційних воєн, гібридних загроз та спроб зовнішнього втручання у внутрішні процеси України, підготовка спеціалістів із захисту державної таємниці набуває особливої актуальності. Сучасний фахівець повинен не лише знати законодавчу базу, а й уміти адаптувати знання до реальних ситуацій, аналізувати ризики, передбачати можливі витоки інформації та оперативно реагувати на загрози.

Посібник “Система охорони державної таємниці” поєднує класичні принципи й сучасні підходи до безпеки. У ньому висвітлено організацію режиму секретності, технічний і криптографічний захист, контроль доступу, а також особливості обробки, зберігання та передачі конфіденційних даних. Матеріали спрямовані на формування практичного мислення та здатності приймати обґрунтовані рішення в умовах невизначеності.

Кожна сторінка цього посібника спонукає замислитися над важливістю інформаційної безпеки, над тим, як навіть одна помилка чи неуважність можуть вплинути на державні інтереси. Працюючи з матеріалом, студент не лише здобуває знання, але й вчиться бачити світ крізь призму відповідальності – відповідальності за інформацію, за процеси, за людей і за безпеку держави.

Цей посібник створено, щоб стати вашим надійним провідником у складному, але надзвичайно цікавому світі охорони державної таємниці. Він допоможе не лише опанувати знання, але й відчути значущість своєї майбутньої професії, усвідомити роль фахівця з безпеки у збереженні миру, незалежності та стабільності держави.

Ми щиро сподіваємося, що цей навчальний посібник стане для вас не просто джерелом інформації, а й натхненням до постійного вдосконалення, дослідження, аналітичного мислення та практичного застосування отриманих знань. Нехай він допоможе вам стати справжніми професіоналами – людьми, які вміють мислити стратегічно, діяти рішуче й зберігати найцінніше – державну таємницю і безпеку України.

ТЕМА. 1
ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ: ПОНЯТТЯ ТА ВИДИ

ПЛАН

1. Поділ та загальна характеристика інформації за режимом доступу.

2. Державна таємниця особливий вид таємної інформації.

3. Поняття, правова природа та ознаки комерційної таємниці.

4. Об'єкти комерційної таємниці та суб'єкти права на комерційну таємницю.

1. Поділ та загальна характеристика інформації за режимом доступу

Інформація є найважливішим потенціалом держави та суспільства. *Під інформацією розуміють:*

– повідомлення, яке містить відомості, що можуть бути в тому числі і конфіденційними;

– відомості про раніше невідомі події;

– змістовний опис об'єкта;

– результат відображення реальної дійсності у свідомості людини; продукт наукового пізнання, неодмінну субстанцію свідомості; категорію, що міститься в усіх елементах і системах матеріального світу;

– властивість матерії.

Поняття "інформація" розкривається через поняття "відомості". Відомості – це копія реального факту. Інформація являє собою інформацію одного об'єкта щодо іншого об'єкта поза відносинами до суб'єкта.

Юридично значимі ознаки інформації:

– збереження інформації за суб'єктом, який її передає, що є однією з головних ознак інформації в ряді теорій; нематеріальний характер;

– інформація не існує сама пособі, а пов'язана з конкретним фізичним носієм;

– суб’єктивний характер – інформація з’являється в результаті діяльності суб’єкта, який має свідомість і є результатом його інтелектуальної діяльності.

Поняття “інформація” подано у Законі України “Про інформацію” за яким, останню розуміють як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Ст. 177 ЦК України “Види об’єктів цивільних прав” визначає, що об’єктами цивільних прав є речі, у тому числі гроші та цінні папери, інше майно, майнові права, результати робіт, послуги, результати інтелектуальної, творчої діяльності, інформація, а також інші матеріальні та нематеріальні блага.

Ст. 200 ЦК України визначено “Інформацією є документовані або публічно оголошені відомості про події та явища, що мали або мають місце у суспільстві, державі та навколишньому середовищі”.

Властивості та характеристики інформації:

– фізична невідчужуваність – інформація не здатна відчужуватись від її творця, носія;

– універсальність інформації – зміст інформації може бути будь-яким і про все;

– якість інформації характеризує ступінь її відповідності потребам, цілям і цінностям користувачів;

– системність інформації – полягає в тому, що будь-яка інформація, що створена людиною має певну внутрішню організаційну структуру встановлену в суспільстві правилами і законами;

– трансформованість інформації, тобто незалежність змісту інформації від форми фіксації і способу пред’явлення;

– невичерпність інформації – інформація може мати необмежену кількість користувачів, залишаючись незмінною;

– субстанційна несамостійність означає те, що без якихось матеріальних носіїв немає інформації. Ця властивість обумовлена зв’язком інформації з процесом її відображення;

– масовість інформації має два аспекти – якісний аспект, який розкриває масовість інформації як інформації суспільної, загальної для всіх та кількісний –

як інформації, яка розповсюджується серед широкої мережі споживачів, користувачів інформації;

– актуальність інформації – ступінь відповідності інформації розвитку суспільства.

Виділяють такі властивості інформації, які визначають стан її безпеки:

– конфіденційність – суб'єктивно визначена властивість інформації, яка вказує на необхідність введення обмежень на коло суб'єктів, які мають доступ до неї;

– цілісність – властивість інформації, яка полягає в її існуванні в незмінному вигляді певний проміжок часу;

– доступність – властивість інформації бути наданою своєчасно і безперешкодно всім суб'єктам, які мають для цього певні повноваження. Класифікація інформації за ступенем доступу є у Законі України "Про інформацію", стаття 20 Доступ до інформації за порядком доступу… інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Класифікаційні ознаки поділу інформації:

– залежно від режиму доступу – *відкрита інформація та інформація з обмеженим доступом;*

– за суб'єктною належністю – *інформація, що належить суб'єктам публічного права та інформація, що належить суб'єктам приватного права.*

В статті 21 Закону України "Про інформацію" визначено, що інформацією з обмеженим доступом є *конфіденційна, таємна та службова інформація.* Інформація з обмеженим доступом – це інформація, доступ до якої має лише обмежене коло осіб і оприлюднення якої заборонене розпорядником інформації відповідно до закону.

Види інформації з обмеженим доступом

Конфіденційна: Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежений фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку, відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Відносини, пов’язані з правовим режимом конфіденційної інформації, регулюються законом.

Службова: Службовою інформацією є інформація, що міститься в документах суб’єктів владних повноважень, які становлять внутрішньовідомчу 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, а також інформація, зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Таємна: Таємною інформацією є інформація, доступ до якої обмежується виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, 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, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу передбачену законом таємницю.

До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

– про стан довкілля, якість харчових продуктів і предметів побуту;

– про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

– 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;

– про факти порушення прав і свобод людини і громадянина;

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

– інші відомості, доступ до яких не може бути обмеженbq відповідно до законів та міжнародних договорів України, згоду на обов'язковість яких надано Верховною Радою України.

До різновидів конфіденційної інформації, за розголошення якої передбачена кримінальна відповідальність, належить:

– лікарська таємниця;

– таємниця листування;

– таємниця голосування;

– таємниця усиновлення (удочеріння);

– нотаріальна таємниця;

– комерційна та банківська таємниця;

– адвокатська таємниця;

– конфіденційна інформація про особу;

– комп'ютерна інформація з обмеженим доступом.

Відповідно до ст. 6 ЗУ "Про доступ до публічної інформації" і ст. 21 ЗУ "Про інформацію" не можуть бути віднесені до інформації з обмеженим доступом такі дані:

– про розпорядження бюджетними коштами;

– про володіння, користування чи розпорядження державним або комунальним майном, у тому числі копії відповідних документів;

– про умови отримання державних та/або комунальних коштів або майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно;

– декларації про доходи осіб та членів їхніх сімей, які претендують на зайняття чи займають виборну посаду в органах влади, обіймають посаду державного службовця, службовця органу місцевого самоврядування першої або другої категорії;

– про стан довкілля, якість харчових продуктів і предметів побуту;

– про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

– про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціаль–нодемографічні показники, стан правопорядку, освіти і культури населення.

2. Державна таємниця – особливий вид таємної інформації

Державна таємниця – 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 законом, державною таємницею і підлягають охороні державою.

Ознаки, які характеризують поняття "державна таємниця". Перша ознака полягає у тому, що державна таємниця є видом таємної інформації правове регулювання якої здійснюється відповідним законом. За другою ознакою державна таємниця характеризуються тим, що її становлять лише відомості у сфері оборони, економіки, зовнішніх відносин, науки і техніки, державної безпеки і охорони правопорядку. Третя ознака полягає в тому, що розголошення державної таємниці може завдати шкоди національній безпеці України. Четверта ознака полягає у тому, що на законодавчому рівні створено механізм віднесення інформації до державної таємниці та її засекречування. Ознакою державної таємниці є те, що її охорона здійснюється державою.

До державної таємниці у порядку, встановленому Законом, відноситься інформація:

1) у сфері оборони:

– про зміст стратегічних і оперативних планів та інших документів бойового управління, підготовку та проведення військових операцій, стратегічне та мобілізаційне розгортання військ, а також про інші найважливіші показники, які характеризують організацію, чисельність, дислокацію, бойову і мобілізаційну

готовність, бойову та іншу військову підготовку, озброєння та матеріально-технічне забезпечення Збройних Сил України та інших військових формувань;

– про дислокацію, характеристики пунктів управління, зміст заходів загальнодержавного та регіонального, у разі необхідності – міського і районного рівня, щодо приведення у готовність єдиної державної системи цивільного захисту населення і територій до виконання завдань в особливий період та про організацію системи зв'язку (оповіщення) в особливий період, можливості населених пунктів, регіонів і окремих об'єктів щодо евакуації, розосередження населення і забезпечення його життєдіяльності; забезпечення виробничої діяльності об'єктів національної економіки у воєнний час;

– про геодезичні, гравіметричні, картографічні та гідрометеорологічні дані і характеристики, які мають значення для оборони країни;

– про застосування систем озброєння, підготовку та проведення військових операцій;

– про винаходи, дослідження і розробку нових зразків озброєння в інтересах забезпечення національної безпеки і оборони та про результати таких досліджень і розробок;

– про заходи та показники розвитку Збройних Сил України та їх спроможностей;

– про склад, завдання та матеріально-технічне забезпечення розвідувального органу Міністерства оборони України та зібрану і створену ним інформацію в результаті його діяльності;

2) у сфері економіки, науки і техніки:

– про зміст мобілізаційних планів державних органів та органів місцевого самоврядування, мобілізаційні потужності, заходи мобілізаційної підготовки і мобілізації та обсяги їх фінансування, запаси та обсяги постачання стратегічних видів сировини і матеріалів, а також зведені відомості про номенклатуру та рівні накопичення, загальні обсяги поставок, відпуску, закладення, оновлення, розміщення і фактичні запаси державного матеріального резерву;

– про використання транспорту, зв'язку, потужностей інших галузей та об'єктів інфраструктури держави в інтересах її безпеки;

– про плани, обсяги та інші найважливіші характеристики добування, виробництва та реалізації окремих стратегічних видів сировини і продукції;

– про державні запаси дорогоцінних металів монетарної групи, коштовного каміння, валюти та інших цінностей, операції, пов'язані з виготовленням грошових знаків і цінних паперів, їх зберіганням, охороною і захистом від підробок, обігом, обміном або вилученням з обігу, а також про інші особливі заходи фінансової діяльності держави;

– про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, предметом яких є створення новітніх складних зразків озброєння, військової або спеціальної техніки та інші роботи, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України;

– про найменування, загальну кількість, вартість озброєння, військової техніки, боєприпасів, запасних частин та матеріалів до них, що закуповуються для потреб військових формувань (правоохоронних органів);

– про кількість, строки поставок військовим формуванням чи правоохоронним органам, спеціальним формуванням Міністерства внутрішніх справ України для забезпечення їх боєздатності основних видів пального (мастильних матеріалів), речового майна та продовольства;

– про факт та предмет закупівлі товарів, робіт і послуг оборонного призначення для забезпечення Збройних Сил України та інших військових формувань та правоохоронних органів (крім випадків, якщо окрема інформація про закупівлю таких товарів, робіт і послуг оборонного призначення, що закуповуються відповідно до Закону України "Про оборонні закупівлі", становить державну таємницю. У такому разі окрема інформація розміщується у додатку до тендерної документації).

Інформація не може бути повторно віднесена до державної таємниці після розсекречення та оприлюднення.

3) у сфері зовнішніх відносин:

– про директиви, плани, вказівки делегаціям і посадовим особам з питань зовнішньополітичної і зовнішньоекономічної діяльності України, спрямовані на забезпечення її національних інтересів і безпеки;

– про військове, науково-технічне та інше співробітництво України з іноземними державами, якщо розголошення відомостей про це завдаватиме шкоди національній безпеці України;

– про експорт та імпорт озброєння, військової і спеціальної техніки, окремих стратегічних видів сировини і продукції;

– про зміст секретної інформації, отриманої від іноземної держави чи міжнародної організації;

4) у сфері державної безпеки та охорони правопорядку:

– про особовий склад органів, що здійснюють оперативно-розшукову, розвідувальну чи контррозвідувальну діяльність;

– про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової, розвідувальної і контррозвідувальної діяльності;

– про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність;

– про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють оперативно-розшукову, розвідувальну і контррозвідувальну діяльність;

– про організацію та порядок здійснення охорони адміністративних будинків та інших державних об’єктів, посадових та інших осіб, охорона яких здійснюється відповідно до Закону України “Про державну охорону органів державної влади України та посадових осіб”;

– про систему урядового та спеціального зв’язку;

– про організацію, зміст, стан і плани розвитку криптографічного захисту секретної інформації, зміст і результати наукових досліджень у сфері криптографії;

– про системи та засоби криптографічного захисту секретної інформації, їх розроблення, виробництво, технологію виготовлення та використання;

– про державні шифри, їх розроблення, виробництво, технологію виготовлення та використання;

– про організацію режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, державні програми, плани та інші заходи у сфері охорони державної таємниці;

– про результати перевірок, здійснюваних згідно з законом прокурором у порядку відповідного нагляду за додержанням законів, та про зміст матеріалів оперативно-розшукової діяльності, досудового розслідування та судочинства з питань, зазначених у цій статті сфер;

– про інші засоби, форми і методи охорони державної таємниці.

3. Поняття, правова природа та ознаки комерційної таємниці

Першим документом, який має міжнародний статус і передбачив регулювання секретів виробництва, дослідники визнають Угоду ТРІПС (вона говорить про закриту інформацію).

Згідно із ст. 39 Угоди про торговельні аспекти прав інтелектуальної власності, під закритою інформацією розуміється інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній конфігурації і поєднанні її компонентів не є загальновідомою і легко доступною особам в тих колах, які зазвичай мають справу з подібною інформацією; з огляду на що вона є секретною вона має комерційну цінність і є об'єктом належних в даних обставинах кроків, спрямованих на збереження її секретності з боку особи, правомірно контролюючої цю інформацію.

Німецька та Австрійська доктрина використовує для визначення конфіденційних відомостей два терміни:

– "торговий секрет" ("Geschäftsgeheimnis");

– "виробничий секрет" ("Betriebsgeheimnis").

Італійська доктрина використовує термін "промислові і торгові секрети" ("segreto industriale e commerciale"), данське право оперує поняттям "відомості про виробничі і торговельні відносини" ("oplysninger om drifts-eller forretningsforhold"). Більшість науковців схиляються до використання поняття "господарська таємниця" ("Wirtschaftsgeheimnis"). Аналогом цих універсальних термінів в нашому законодавстві виступає поняття "комерційна таємниця".

Основне визначення комерційної таємниці міститься в ст. 505 Цивільного кодексу України: інформація 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.

У Цивільному кодексі передбачено ще три статті, присвячені правовому регулюванню комерційної таємниці:

ст. 506. Майнові права інтелектуальної власності на комерційну таємницю;

ст. 507. Охорона комерційної таємниці органами державної влади;

ст. 508. Строк чинності права інтелектуальної власності на комерційну таємницю.

Згідно з ч. 1 ст. 36 Господарського кодексу України, комерційною таємницею є відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею.

Господарським кодексом регламентовано:

ст. 36. Неправомірне збирання, розголошення та використання відомостей, що є комерційною таємницею;

ст. 155. Об'єкти прав інтелектуальної власності;

ст. 162. Правомочності суб'єктів господарювання щодо комерційної таємниці.

ст. 36. Господарського кодексу України є аналогічною Главі 4 Закону України "Про захист від недоброякісної конкуренції" Неправомірне збирання, розголошення та використання комерційної таємниці.

Юридично значимими ознаками, необхідними і достатніми для визнання інформації комерційною таємницею суб'єкта господарювання, є такі:

– Комерційною таємницею може визнаватися лише інформація.

– Інформація, яка становить комерційну таємницю, не потребує офіційного визнання її охороноспроможності, реєстрації чи дотримання інших формальних процедур для поширення на неї правової охорони.

Це інформація технічного, організаційного, комерційного, виробничого та іншого характеру, що пов’язана з підприємницькою діяльністю; не є державною таємницею, або інформацією, яка відповідно не може належати до комерційної таємниці; згідно з нормами вітчизняного законодавства є об’єктом права інтелектуальної власності суб’єкта підприємницької діяльності, використання якої не завдасть шкоди суспільству. Така інформація має бути не відомою та не легкодоступною для інших осіб. Внаслідок її невідомості вона має комерційну цінність. Розголошення комерційної таємниці, згідно зі ст. 36 ГК України, “може завдати шкоди інтересам суб’єкта господарювання”. Зміст та об’єм комерційної таємниці встановлюється володільцем інформації на власний розсуд. Ще однією особливою ознакою комерційної таємниці є необмеженість строку її захисту.

Практика підприємницької діяльності під грифом комерційноцінної інформації зберігає як знання і досвід виробничо-технічного характеру, що є результатами інтелектуальної діяльності, так і інформацію, що становить предмет ділового чи іншого інтересу господарюючого суб’єкта.

О. Сліпачук усі види інформації, які можуть вважатися комерційною таємницею, умовно розділяє на дві групи: технічна інформація і комерційна інформація. До першої групи належать незапатентовані науково-технічні розробки, бази даних та інші комп’ютерні програми, створені підприємством, усі види “ноу-хау”, технічні проекти, промислові зразки, незапатентовані товарні знаки тощо. До другої групи віднесено умови контрактів, дані про постачальників і покупців, інформація про переговори, маркетингові дослідження, дані про розрахунок відпускних цін, розміри знижок тощо.

Г. Виноградова та О. Шпак, роблять висновок, що поняття комерційної таємниці є ширшим, ніж поняття об’єкта інтелектуальної власності, який може входити до складу комерційної таємниці суб’єкта підприємницької діяльності, оскільки може включати в себе інформацію щодо певних фактів, подій, явищ та продукти інтелектуальної діяльності. Зважаючи на це, потрібно забезпечити

захист інформації, яка є результатом інтелектуальної діяльності, і інформації, що не містить таких ознак.

Комерційна таємниця не обов'язково є об'єктом інтелектуальної власності, однак інформація, що захищена законодавством про інтелектуальну власність, може бути визнана комерційною таємницею.

Переваги комерційної таємниці полягають у тому що:

1) вона не пов'язана з витратами на реєстрацію;

2) її дія необмежена в часі;

3) її охорона починає діяти негайно;

4) для встановлення охорони не потрібне її розкриття або реєстрація у державному органі.

Недоліки комерційної таємниці полягають у тому, що:

1) якщо таємниця втілена в продукті, треті особи можуть самостійно розкрити секретну: інформацію і використовувати її на законних підставах шляхом зворотного інжинірингу;

2) якщо комерційна таємниця розкрита широкому загалові, охорона не надається;

3) охорона надається виключно від неналежного одержання, використання або розкриття конфіденційної інформації;

4) охорона комерційної таємниці є меншою, ніж охорона патентів;

5) комерційна таємниця не забезпечує охорони від тих, хто самостійно приходить до аналогічної ідеї, що тримається в секреті.

Закон не передбачає покарання за добросовісне розкриття, що має бути здійснене у такі законні способи, як:

1) самостійне створення; комерційна таємниця не забезпечує виняткові, тому потенційно будь-хто може розкрити вашу комерційну таємницю самостійно і використовувати або запатентувати її;

2) зворотний інжиніринг – це звична практика, яка використовується для визначення механізму функціонування або складових продукту і яка полягає в тому, що конкурент вивчає продукт з метою його відтворення або навіть виготовлення більш досконалого.

4. Перелік інформації, що охороняється в режимі комерційної таємниці

Перелік інформації, що охороняється в режимі комерційної таємниці найчастіше містить:

– список покупців і постачальників (чим більше інформації такий список містить, *наприклад*, хто з партнерів більш цінний, тим більш імовірне визнання її секретом виробництва);

– технічні проекти, креслення, схеми та карти; інформацію про стратегії і методи ведення бізнесу тощо;

– інформацію про ціни й витрати;

– відомості НДДКР;

– вихідний код комп'ютерних програм;

– технології виробництва;

– негативний досвід (*наприклад*, відомості про непрацездатні технологічні процеси);

– дослідні зразки, прототипи;

– рецепти і способи приготування; генетичний матеріал.

Згідно із частиною 2 статті 505 Цивільного кодексу України, 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.

До даних, що становлять комерційну таємницю, належать секретні відомості (інформація) науково-технологічного та комерційного характеру, пов'язані з:

– виробництвом і технологією (ідеї, винаходи, відкриття, створені підприємством бази даних, комп'ютерні програми, ноу-хау, технічні проекти, описи технологічних іспитів, промислові зв'язки);

– фінансовою діяльністю (нові методи організації праці та виробництва, укладені та заплановані контракти, інформація про конфіденційні переговори);

– господарською діяльністю (огляди ринку, маркетингові дослідження плани розвитку підприємства).

Види комерційної таємниці можна класифікувати:

– за природою:

- технологічні;
- виробничі;
- організаційні;
- маркетингові;
- інтелектуальні;
- рекламні;

– за належністю власнику:

- власність організації;
- власність групи організацій;
- власність однієї особи;
- власність групи осіб;

– за призначенням:

- економічні;
- ноу-хау;
- нові технології;
- технічні вироби;
- зразки.

Відповідно до Постанови Кабінету Міністрів України "Про перелік відомостей, що не становлять комерційної таємниці" *комерційну таємницю не становлять:*

– установчі документи, документи, що надають можливість займатися підприємницькою чи господарською діяльністю та її окремими видами;

– інформація за всіма встановленими формами державної звітності;

– дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;

– відомості про кількість і склад працюючих, їх заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;

– документи про сплату податків і обов'язкових платежів;

– інформація про забруднення довкілля, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;

– документи про платоспроможність;

– відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об’єднаннях та інших організаціях, які займаються підприємницькою діяльністю;

– відомості, що відповідно до чинного законодавства підлягають оголошенню.

В ч. 2 ст. 506 ЦК України зазначено, що майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визначила інформацію комерційною таємницею, якщо інше не встановлено договором. Зі змісту ст. 36 ГК України випливає, що дані норми спрямовані на охорону комерційної таємниці, володарем якої виступає суб’єкт господарювання.

Оскільки комерційну таємницю законодавець відносить до об’єктів інтелектуальної власності, то у відповідності ст. 421 ЦК України: “Суб’єктами права інтелектуальної власності є: творець (творці) об’єкта права інтелектуальної власності (автор, виконавець, винахідник тощо) та інші особи, яким належать особисті немайнові та (або) майнові права інтелектуальної власності відповідно до цього Кодексу, іншого закону чи договору”.

На основі положень Закону України “Про правовий статус іноземців та осіб без громадянства” можна стверджувати, що стосовно комерційної таємниці іноземці та особи без громадянства в Україні мають такі ж права й обов’язки, як і громадяни України, в тому числі у сфері підприємництва, зовнішньоекономічної та трудової діяльності.

Іноземці та особи без громадянства користуються таким же правовим захистом своїх прав на комерційну таємницю, як і громадяни України, а також на рівних підставах і в однаковому обсязі з останніми несуть відповідальність за порушення прав інших осіб на комерційну таємницю та невиконання відповідних своїх обов’язків.

Інформація, що визначена як *комерційна таємниця*, має особливий правовий статус, оскільки її розголошення або незаконне використання може завдати власникові істотних економічних збитків. Така інформація повинна мати *реальну або потенційну комерційну цінність*, тобто бути невідомою третім особам, мати значення для діяльності підприємства, установи чи організації та забезпечувати певні конкурентні переваги на ринку.

Відповідно, *суб'єктами права на комерційну таємницю* виступають насамперед *суб'єкти підприємницької діяльності* – юридичні особи та фізичні особи-підприємці, які у процесі своєї діяльності створюють, використовують або зберігають інформацію, що становить комерційну цінність. Саме вони мають право визначати перелік таких відомостей, встановлювати порядок їх захисту, а також вживати заходів для запобігання несанкціонованому доступу, копіюванню чи поширенню.

Право на комерційну таємницю виникає у суб'єкта після здійснення певних *юридичних фактів*, що підтверджують його статус та дії, спрямовані на захист відповідної інформації. Ці факти поділяються на *об'єктивні та суб'єктивні умови.*

– *Об'єктивні умови* відображені у чинному законодавстві – у Цивільному кодексі України, Господарському кодексі, Законі України «Про інформацію», а також у підзаконних актах, які регламентують порядок охорони інформації з обмеженим доступом. Вони визначають загальні вимоги до створення, класифікації, обігу й захисту комерційної таємниці.

– *Суб'єктивні умови* полягають у самостійному застосуванні законним власником комплексу заходів із захисту комерційно цінної інформації. До них належать організаційно-правові, технічні та режимні дії: обмеження кола осіб, допущених до інформації; укладання договорів про нерозголошення (NDA); маркування документів грифом «Комерційна таємниця»; впровадження систем контролю доступу до електронних і паперових носіїв; ведення журналів обліку та зберігання матеріалів тощо.

Суб'єктами права на комерційну таємницю можуть бути не лише комерційні структури, а й організації, що здійснюють некомерційну діяльність і працюють з інформацією, що має фактичну або потенційну цінність, наприклад, науково-дослідні установи, навчальні заклади чи інноваційні організації.

Таким чином *комерційна таємниця* є елементом конкурентної стратегії та інструментом захисту інтелектуального потенціалу й інновацій. Її ефективна охорона потребує поєднання правових, організаційних і технічних заходів, а також відповідальності власників інформації.

Серед учасників відносин, що складаються з приводу комерційної таємниці, виділяють органи державної влади, місцевого самоврядування, фізичні особи без статусу суб'єкта підприємницької діяльності, суб'єкти публічного права.

Ця категорія суб'єктів виступає у якості користувачів інформації, що становить комерційну таємницю. Право на доступ до комерційної таємниці мають органи державної влади, місцевого самоврядування в рамках закріпленої за ними компетенції для реалізації поставлених перед ними завдань.

Поняття "право на комерційну таємницю" можна застосовувати в двох значеннях:

1) у суб'єктивному розумінні цим терміном позначається комплекс повноважень, які належать конкретній особі по відношенню до конкретної комерційної таємниці;

2) в об'єктивному розумінні цей термін позначає правовий інститут, який охоплює систему норм права, що регулюють суспільні відносини щодо комерційних таємниць.

Основою регламентації прав суб'єктів на комерційну таємницю є Цивільний кодекс України. Ст. 418 зазначеного Кодексу називає таке право на результат інтелектуальної діяльності "правом інтелектуальної власності", яке становлять особисті немайнові та (або) майнові права інтелектуальної власності.

Згідно з ч. 1 ст. 506 Цивільного кодексу України, *майновими правами на комерційну таємницю є:*

– право на використання комерційної таємниці;

– виключне право дозволяти використання комерційної таємниці;

– виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці;

– інші майнові права інтелектуальної власності, встановлені законом.

Право на комерційну таємницю надає суб'єктам такі основні можливості:

1) воно забезпечує суб'єкта права на таку інформацію можливістю її засекречування від широкої публіки;

2) воно надає відповідному суб'єкту можливість вимагати, щоб інші особи утримувалися від використання незаконних способів одержання інформації, яка становить його комерційну таємницю;

3) суб'єкт права на комерційну таємницю має можливість її розкрити;

4) відповідний суб'єкт може звертатися за захистом своїх порушених прав до суду.

СЕМІНАРСЬКЕ ЗАНЯТТЯ
ТЕМА 1
ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ: ПОНЯТТЯ ТА ВИДИ

План семінарського заняття

1. Поділ та загальна характеристика інформації за режимом доступу.

2. Державна таємниця – особливий вид таємної інформації.

3. Поняття, правова природа та ознаки комерційної таємниці.

4. Об'єкти комерційної таємниці та суб'єкти права на комерційну таємницю.

Ключові поняття та терміни: захист інформації, конфіденційна інформація, державна таємниця, рівні секретності, гриф секретності, комерційна таємниця, службова інформація.

Завдання для самостійної роботи над темою

Завдання 1. Опрацювати теоретичний матеріал теми 1 дистанційного курсу "Система охорони державної таємниці" у Віртуальному університеті ЛДУ БЖД.

Завдання 2. Користуючись рекомендованою літературою та ресурсами мережі Інтернет, самостійно опрацювати та коротко законспектувати такі питання:

1. Яка інформація належить до різновидів конфіденційної інформації, за розголошення якої передбачена кримінальна відповідальність?

2. Охарактеризуйте правовий статус іноземців та осіб без громадянства стосовно комерційної таємниці у сфері підприємництва, зовнішньоекономічної та трудової діяльності.

Завдання 3. Використовуючи теоретичний матеріал лекції розв'яжіть ситуаційні завдання та обгрунтуйте аргументи для дискусійних тем.

Ситуація 1: Компанія випадково розкрила конфіденційну інформацію

про новий продукт до офіційного релізу. Які можуть бути наслідки та як слід було б захистити ці дані?

Ситуація 2: Вам стали відомі внутрішні фінансові дані компанії, в якій ви працюєте. Що ви повинні зробити, щоб ці дані залишалися конфіденційними?

Ситуація 3: У навчальному закладі обговорюються персональні дані студентів. Яких законодавчих та етичних принципів слід дотримуватися, щоб забезпечити їх захист?

Ситуація 4: Ваш колега попросив доступ до документів компанії з грифом "Для службового користування". Які ваші дії, якщо ця людина не має права доступу?

Дискусійні теми:

– Чи можна виправдати порушення обмеженого доступу до інформації у випадках суспільної необхідності (*наприклад*, під час розслідувань)?

– Як, на вашу думку, зміниться регулювання доступу до інформації в епоху цифрових технологій та глобальної інформаційної взаємодії?

ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ

1. Дайте визначення поняттю "інформація".
2. Охарактеризуйте поняття "інформація" та "відомості" – спільне та відмінне.
3. Які існують юридично значимі ознаки інформації?
4. Опишіть властивості та характеристики інформації.
5. Як класифікують інформацію за ступенем доступу?
6. Які існують види інформації з обмеженим доступом?
7. Які відомості НЕ можуть бути віднесені до інформації з обмеженим доступом?
8. Яким законом врегульовано суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, її засекречуванням та охороною з метою захисту життєво важливих інтересів України?
9. Дайте визначення поняттю "державна таємниця".
10. Які існують ознаки державної таємниці?

11. Яка інформація належить до державної таємниці у сфері оборони у порядку, встановленому законом?
12. Яка інформація належить до державної таємниці у сфері економіки, науки і техніки у порядку, встановленому законом?
13. Яка інформація належить до державної таємниці у сфері зовнішніх відносин у порядку, встановленому законом?
14. Яка інформація належить до державної таємниці у сфері державної безпеки та охорони правопорядку у порядку, встановленому законом?
15. Які існують підходи до визначення поняття “комерційна таємниця”?
16. Якими законами та нормативними актами регулюються правовідносини щодо комерційної таємниці та її правової охорони?
17. Які існують юридично значимі ознаки, необхідні і достатні для визнання інформації комерційною таємницею суб’єкта господарювання?
18. Назвіть переваги охорони комерційної таємниці порівняно з іншими засобами охорони інтелектуальної власності.
19. Назвіть недоліки охорони комерційної таємниці порівняно з іншими засобами охорони інтелектуальної власності.
20. Дайте перелік інформації, що охороняється в режимі “комерційна таємниця”.
21. Назвіть дані (секретні відомості (інформація) науково-технологічного та комерційного характеру), що становлять комерційну таємницю згідно із частиною 2 статті 505 Цивільного кодексу України.
22. Як можна класифікувати види комерційної таємниці?
23. Відповідно до Постанови Кабінету Міністрів України “Про перелік відомостей, що не становлять комерційної таємниці”, які відомості не становлять комерційної таємниці?
24. Визначте, хто є суб’єктами права на комерційну таємницю?
25. Що являє собою “право на комерційну таємницю”?
26. Які основні можливості надає суб’єктам право на комерційну таємницю?

Рекомендована література: [1-3, 5, 7, 14, 21, 24-25].

ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ

1. Що є головною складовою інформаційної безпеки держави?
   а) Захист інформації, зокрема державної таємниці.
   б) Контроль за інформаційними потоками.
   в) Регулювання комерційної діяльності.
   г) Впровадження цифрових технологій.

2. Який закон України визначає поняття “інформація”?
   а) Закон України “Про інформацію”.
   б) Закон України “Про державну таємницю”.
   в) Закон України “Про комерційну таємницю”.
   г) Конституція України.

3. Що є ознакою державної таємниці?
   а) Відомості у сфері оборони, економіки, науки і техніки.
   б) Дані про діяльність приватних компаній.
   в) Загальнодоступна інформація.
   г) Комерційні секрети підприємств.

4. Яка інформація не може бути віднесена до державної таємниці?
   а) Про стан довкілля.
   б) Про військові операції.
   в) Про економічні показники держави.
   г) Про результати наукових досліджень.

5. Що таке комерційна таємниця?
   а) Інформація, що має комерційну цінність та охороняється підприємством.
   б) Відомості про державну політику.
   в) Загальнодоступна економічна статистика.
   г) Конфіденційна інформація про державні установи.

6. Яка основна мета захисту комерційної таємниці?
    а) Запобігання використанню конфіденційних відомостей конкурентами.
    б) Обмеження поширення інформації серед працівників.
    в) Контроль за діяльністю органів влади.
    г) Регулювання державних підприємств.

7. Які властивості має інформація з обмеженим доступом?
    а) Конфіденційність, цілісність, доступність.
    б) Загальнодоступність, наукова цінність, інноваційність.
    в) Відкритість, публічність, безоплатність.
    г) Структурованість, контрольованість, законність.

8. Яке твердження стосується конфіденційної інформації?
    а) Вона може поширюватися лише за згодою відповідної особи.
    б) Вона є загальнодоступною для всіх громадян.
    в) Вона містить державні секрети.
    г) Вона охоплює лише фінансові дані.

9. Яка відповідальність передбачена за розголошення державної таємниці?
    а) Кримінальна та адміністративна.
    б) Лише адміністративна.
    в) Тільки дисциплінарна.
    г) Лише фінансова компенсація.

10. Які основні критерії віднесення інформації до державної таємниці?
    а) Вона стосується національної безпеки.
    б) Вона є комерційно вигідною.
    в) Вона доступна лише посадовим особам.
    г) Вона використовується в наукових дослідженнях.

11. Які відомості можуть бути віднесені до комерційної таємниці?

а) Дані про стратегії розвитку компанії.

б) Відомості про стан довкілля.

в) Публічні економічні показники.

г) Загальнодоступна наукова інформація.

12. Який закон України містить визначення комерційної таємниці?

а) Цивільний кодекс України.

б) Закон України “Про державну таємницю”.

в) Конституція України.

г) Закон України “Про електронні комунікації”.

13. Яке твердження стосується службової інформації?

а) Вона міститься у внутрішніх документах державних органів.

б) Вона є загальнодоступною.

в) Вона підлягає обов’язковому оприлюдненню.

г) Вона не потребує захисту.

14. Яке визначення найкраще описує інформацію з обмеженим доступом?

а) Це інформація, доступ до якої обмежено законом.

б) Це загальнодоступні відомості.

в) Це виключно наукові дані.

г) Це інформація, яку можуть вільно використовувати підприємці.

15. Який критерій є визначальним для комерційної таємниці?

а) Вона має комерційну цінність.

б) Вона використовується у сфері оборони.

в) Вона є відкритою для громадськості.

г) Вона регулюється виключно міжнародним правом.

16. Яке покарання може бути застосоване за незаконне розголошення комерційної таємниці?
    а) Матеріальна відповідальність та штрафи.
    б) Позбавлення громадянства.
    в) Тільки усне попередження.
    г) Виключно адміністративне покарання.

17. Яка інформація належить до сфери державної таємниці?
    а) Дані про військові операції.
    б) Відомості про погодні умови.
    в) Плани розвитку туристичної галузі.
    г) Загальнодоступна статистика.

18. Що є основним критерієм віднесення інформації до таємної?
    а) Можливість заподіяння шкоди національній безпеці.
    б) Її наявність у державних органах.
    в) Її економічна вартість.
    г) Використання у судових процесах.

19. Які дані можуть бути включені до службової інформації?
    а) Внутрішні документи органів влади.
    б) Загальнодоступні відомості про природні ресурси.
    в) Прогнози економічного розвитку.
    г) Відомості про демографічну ситуацію.

20. Яке твердження є правильним щодо відкритої інформації?
    а) Вона доступна всім громадянам.
    б) Вона містить державні секрети.
    в) Вона потребує спеціального дозволу для доступу.
    г) Вона регулюється виключно комерційними підприємствами.

21. Який закон України визначає забезпечення інформаційної безпеки як одну з найважливіших функцій держави?
    а) Конституція України.
    б) Закон України “Про інформацію”.
    в) Цивільний кодекс України.
    г) Господарський кодекс України.

22. Яке поняття найчастіше використовується для розкриття змісту інформації?
    а) Відомості.
    б) Дані.
    в) Повідомлення.
    г) Факти.

23. Яка з наведених ознак не є юридично значущою ознакою інформації?
    а) Матеріальний характер.
    б) Збереження інформації за суб’єктом.
    в) Нематеріальний характер.
    г) Суб’єктивний характер.

24. Який закон України містить визначення інформації як будь-яких відомостей та/або даних, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді?
    а) Закон України “Про інформацію”.
    б) Цивільний кодекс України.
    в) Господарський кодекс України.
    г) Конституція України.

25. Які види інформації належать до інформації з обмеженим доступом?
    а) Конфіденційна, таємна та службова.
    б) Відкрита, закрита та запатентована.
    в) Державна, комерційна та банківська таємниця.
    г) Публічна інформація.

26. Яка стаття Цивільного кодексу України визначає інформацію як об’єкт цивільних прав?
    а) Стаття 177.
    б) Стаття 200.
    в) Стаття 505.
    г) Стаття 36.

27. Яка властивість інформації характеризує ступінь її відповідності потребам, цілям і цінностям користувачів?
    а) Якість інформації.
    б) Актуальність інформації.
    в) Цілісність інформації.
    г) Конфіденційність інформації.

28. Який вид таємної інформації охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку?
    а) Державна таємниця.
    б) Комерційна таємниця.
    в) Банківська таємниця.
    г) Професійна таємниця.

29. Яка ознака не характеризує поняття “державна таємниця”?
    а) Правове регулювання здійснюється постановою Кабінету Міністрів України.
    б) Її становлять відомості у сфері оборони, економіки, зовнішніх відносин, науки і техніки, державної безпеки і охорони правопорядку.
    в) Розголошення державної таємниці може завдати шкоди національній безпеці України.
    г) Існує механізм віднесення інформації до державної таємниці та її засекречування.

30. На які види поділяється інформація за ступенем доступу згідно з Законом України “Про інформацію”?
    а) Відкрита інформація та інформація з обмеженим доступом.
    б) Загальнодоступна інформація та закрита інформація.
    в) Запатентована інформація та незахищена інформація.
    г) Конфіденційна інформація та таємна інформація.

31. Яка інформація не може бути віднесена до інформації з обмеженим доступом?
    а) Про стан довкілля.
    б) Про персональні дані.
    в) Про комерційційну таємницю.
    г) Про таємницю слідства.

32. Яка властивість інформації полягає в її існуванні в незмінному вигляді певний проміжок часу?
    а) Цілісність.
    б) Доступність.
    в) Конфіденційність.
    г) Актуальність.

33. Який перелік інформації не може бути віднесений до комерційної таємниці?
    а) Установчі документи.
    б) Відомості про постачальників.
    в) Інформація про ціни та витрати.
    г) Відомості НДДКР.

34. Які відомості не можуть бути віднесені до державної таємниці?
    а) Про стан здоров’я населення.
    б) Про хід бойових дій.
    в) Про новітні розробки озброєння.
    г) Про зміст мобілізаційних планів.

35. Який нормативно-правовий акт має міжнародний статус і передбачив регулювання секретів виробництва?
    а) Угода ТРІПС.
    б) Паризька конвенція про охорону промислової власності.
    в) Бернська конвенція про охорону літературних і художніх творів.
    г) Женевська конвенція про охорону інтересів виробників фонограм.

36. Який термін використовується в німецькій доктрині для визначення конфіденційних відомостей?
    а) Торговий секрет (“Geschäftsgeheimnis”).
    б) Комерційна таємниця.
    в) Виробнича таємниця.
    г) Ноу-хау.

37. Які відомості можуть бути віднесені до комерційної таємниці згідно з Цивільним кодексом України?
    а) Відомості технічного, організаційного, комерційного, виробничого та іншого характеру.
    б) Відомості, що становлять державну таємницю.
    в) Відомості про особисте життя фізичної особи.
    г) Відомості, що підлягають обов’язковому оприлюдненню.

38. Яка стаття Цивільного кодексу України визначає інформацію, 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?
    а) Стаття 505.
    б) Стаття 177.
    в) Стаття 200.
    г) Стаття 36.

39. Який основний нормативно-правовий акт в Україні містить визначення комерційної таємниці?
    а) Цивільний кодекс України.
    б) Господарський кодекс України.
    в) Закон України “Про захист від недобросовісної конкуренції”.
    г) Закон України “Про інформацію”.

40. Який документ є єдиною формою реєстрації відомостей, що становлять державну таємницю в Україні?
    а) Звід відомостей, що становлять державну таємницю (ЗВДТ).
    б) Перелік відомостей, що становлять державну таємницю.
    в) Реєстр державної таємниці.
    г) Класифікатор державної таємниці.

41. Який основний критерій лежить в основі поділу інформації за режимом доступу?
    а) Ступінь обмеження доступу до інформації.
    б) Кількість користувачів інформації.
    в) Місце зберігання інформації.
    г) Форма подання інформації.

42. Що є визначальною ознакою державної таємниці?
    а) Належність відомостей до сфери національної безпеки та оборони.
    б) Її комерційна цінність для підприємства.
    в) Наявність авторського права на інформацію.
    г) Публікація в офіційних джерелах.

43. Яка з наведених характеристик є обов’язковою ознакою комерційної таємниці?
    а) Конфіденційність та наявність економічної цінності для власника.
    б) Віднесення інформації до службової.
    в) Використання інформації у сфері оборони.
    г) Доступність для широкого кола осіб.

ТЕМА. 2
ПРАВОВИЙ ЗАХИСТ ДЕРЖАВНОЇ ТАЄМНИЦІ

ПЛАН

1. Становлення системи державної таємниці в Україні.

2. Організаційно-правові заходи охорони та захисту державної таємниці.

3. Організаційно-правова структура системи охорони державної таємниці.

1. Становлення системи державної таємниці в Україні

Початком формування сучасного законодавства у сфері охорони державної таємниці наукові джерела визначають період кінця XIX початку XX століття.

Із кінця XIX століття:

– охорона державної таємниці набуває системних ознак, попри істотні недоліки;

– неналежна нормативно-правова база;

– відсутнє конкретне визначення самого терміну “державна таємниця”;

– відсутність детального переліку відомостей, що становлять державну таємницю.

Положення про покарання на протидію державній зраді і шпигунству розрізняє три види державної зради: загальну, військову, дипломатичну. Відомості виділяли в окремі групи, що мали гриф “ті, що повинні зберігатись у таємниці”, “...планів російських фортець й інших укріплених споруд, гаваней, портів, арсеналів”.

У жовтні 1909 року було заборонено публікувати у періодичних виданнях будь-яку інформацію про пересування військ і їх бойову підготовку. У червні 1911 р. було запроваджено Інструкцію начальникам контррозвідувальних відділень, яка регламентувала організацію боротьби зі шпигунством та іншими видами діяльності іноземних держав у Росії, що загрожували безпеці імперії.

Перелік відомостей з оборонних питань, що підлягали захисту:

а) склад, організація, дислокація, озброєння, комплектування збройних сил (сухопутних і морських), навчання сухопутних військ і флоту, внутрішній побут, командний склад і настрої в армії та на флоті;

б) відомості про армійські й морські установи, заклади, склади і магазини (портові, інтендантські, артилерійські, мінні, інженерні, санітарні тощо);

в) відомості про фортеці, укріплені пункти і бази флоту;

г) хід мобілізації й зосередження військ і флоту після оголошення війни;

д) накази та звіти про проведені маневри, стрільби і навчання сухопутних військ і флоту, статути, інструкції й розпорядження щодо різноманітних аспектів бойової підготовки армії і флоту;

е) військово-географічні, топографічні й статистичні відомості про прикордонні місцевості (як сухопутні, так і морські), зважаючи на їх стратегічне значення, особливо про розташування, властивості й прохідність місцевих природних перешкод та можливі місця висадки, так само як і про прилеглі до укріплених районів місцевості;

є) відомості про властивості й прохідність прилеглих до вітчизняних берегів морських, річкових і озерних водних просторів з усіма затоками, бухтами, пристанями, гаванями, рейдами й іншими місцями, придатними для стоянки і прибуття військових та комерційних кораблів;

ж) дані про ґрунтові шляхи сполучення в цих місцевостях, особливо про мережу шосейних доріг, природні перешкоди на них та перевізні засоби;

з) відомості про залізниці, їх вузлові пункти і, особливо, про важливі залізничні споруди, псування яких може істотно вплинути на рух (мости, тунелі, труби, насипи, водокачки, гаті тощо), та інформація щодо устаткування залізниць, котре впливає на їх пропускну спроможність (водопостачання, склади палива, кількість доріг, запаси устаткування станцій, майстерні, платформи, вантажувальні і розвантажувальні засоби, сигналізація, пакгаузи й ін.), склади переносних залізниць;

й) телеграфні та телефонні повідомлення;

к) прибережні й острівні спостережні пункти морського відомства і прикордонної варти;

л) голубино–поштові й радіотелеграфні станції;

м) військове повітроплавання;

н) характеризуючи дані командного складу військового і морського відомств.

3 березня 1912 року воєнний міністр та міністр юстиції підписали "Пояснюючу записку до проекту про зміни діючих законів про державну зраду шляхом шпигунства". 5 липня 1912 року, Закон "Про зміну діючих законів про державну зраду шляхом шпигунства у мирний час" було уведено нове визначення відомостей, що становили державну таємницю у воєнній сфері: "Це відомості або предмети, що стосуються зовнішньої безпеки Росії або її збройних сил, призначених для воєнної оборони країни". У грудні 1912 року складено перелік відомостей, заборонених до друку. Це і був перший у XX ст. Звід відомостей, що становлять державну таємницю.

Перелік інформації, що входила до Зводу відомостей, що становлять державну таємницю (грудень 1912 року):

1. Про боєготовність армії і флоту;

2. Хід ремонтних робіт на кораблях, озброєння і тактико-технічні характеристики як тих, що будуються, так і запланованих;

3. Кількість боєприпасів у військах, укріплених пунктах, фортах та військових кораблях, стан недоторканних запасів армії й флоту, відомості про збільшення обсягу робіт на заводах із виготовлення замовлень військового відомства;

4. Про нинішній стан і призначення фортець, укріплень, військових портів і опорних пунктів (баз), про роботи в них, розширення укріплених і опорних, пунктів, проектування нових і ліквідацію наявних;

5. Про бойове маневрування і стрільби на флоті;

6. Про здійснення перевірних і навчальних мобілізацій військових і флотських частин;

7. Про припинення звільнення воєнних чинів у відпустку, відкликання з відпусток, запасу, затримка у звільненні в запас, рух військ до кордону, про маневри і військові збори біля кордонів, фрахтовку і зосередження комерційних кораблів у портах;

8. Військові й воєнно-морські заходи Росії за кордоном.

У січні 1914 року уведено в дію новий варіант Зводу відомостей, що становлять державну таємницю:

1. Про очікувані й уведені зміни в озброєння армії і флоту;

2. Про формування нових військових частин і установ армії і флоту і про зміни в чисельності наявних;

3. Про озброєння тих, що будуються, і запланованих бойових кораблів;

4. Про ремонтні роботи на кораблях флоту, що тимчасово порушують їх боєготовність;

5. Про кількість боєприпасів й інших запасів призначених для потреб воєнного часу у військах, укріплених пунктах, портах і на воєнних кораблях;

6. Про сучасний бойовий стан і значення для воєнного часу фортець, укріплень, воєнних портів і опорних пунктів (баз), роботи з посилення їх боєготовності, пропозиції щодо створення нових і розширення або скорочення наявних;

7. Про бойове маневрування і стрільби на флоті;

8. Про здійснення і результат перевірних і навчальних мобілізацій військових та флотських частин;

9. Про хід маневрів і воєнних зборів у прикордонних губерніях і областях;

10. Про припинення звільнення воєнних чинів у відпустку, виклик із відпусток, запасу, затримання у звільнення в запас, рух військ до кордону, про маневри і військові збори біля кордонів, фрахтування й зосередження комерційних кораблів у портах.

Початок створення сучасної системи охорони державної таємниці – проголошення незалежності України. Так, у ст. 17 Конституції України проголошується, що “Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою усього Українського народу”. 2 жовтня 1992 р. Закон України “Про інформацію”, 21 січня 1994 р. Закон України “Про державну таємницю”, здійснено розподіл інформації, що може належати до державної таємниці за ступенями секретності: “Особливої важливості”, “Цілком таємно” і

“Таємно”. 12 серпня 2005 р. Звід відомостей, що становлять державну таємницю України, затверджений наказом СБУ.

Закони України:

– “Про основи національної безпеки України”;

– “Про оперативно-розшукову діяльність”;

– “Про захист інформації в автоматизованих системах”;

– “Про доступ до публічної інформації”.

Постанови Верховної Ради України:

– “Про затвердження Положення про порядок оформлення та використання прав на винаходи, корисні моделі і промислові зразки, що становлять державну таємницю”;

– “Про правила поводження народних депутатів України з таємними документами та інформацією”;

Підзаконні нормативно-правові акти: укази Президента, постанови Кабінету Міністрів:

– “Положення про порядок надання, переоформлення та скасування громадянам допуску до державної таємниці”, затверджене постановою Кабінету Міністрів України від 29 листопада 2001 р.;

– “Положення про порядок підготовки документів щодо передачі державної таємниці іноземній державі чи міжнародній організації” затверджене Указом Президента від 14 грудня 2004 р.;

– “Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства” затверджене Указом Президента від 17 серпня 2006 р.;

– Указ Президента України від 1 грудня 2009 р. “Про перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць”.

За порушення правил поводження з державною таємницею встановлюється:

– дисциплінарна;

– адміністративна;

– кримінальна відповідальність.

Відповідальність за злочини у сфері охорони державної таємниці передбачена Особливою частиною КК за такі діяння:

ст. 111 “Державна зрада” (у формі шпигунства);

ст. 114 “Шпигунство”, 328 “Розголошення державної таємниці”;

ст. 329 “Втрата документів, що містять державну таємницю”;

ст. 422 “Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості”.

Законодавчо закріплені вимоги до інформації, що містить ознаки державної таємниці, впроваджені з метою охорони державної таємниці.

Відповідно до Закону України “Про державну таємницю” (ст. 1) державна таємниця – 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.

Визначення державної таємниці має такі ознаки:

– обмеженість доступу до державної таємниці як виду таємної інформації, тобто відомості, що становлять таку таємницю, підлягають засекречуванню (обмеженню їх поширення і доступу до їх матеріальних носіїв);

– механізм віднесення інформації до державної таємниці та її засекречування передбачений спеціальним Законом;

– значущість, важливість такого роду відомостей у певний проміжок часу для інтересів держави, тобто в разі розголошення державної таємниці національній безпеці України може бути завдана суттєва шкода.

2. Організаційно-правові заходи охорони та захисту державної таємниці

Охорона державної таємниці включає комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативних заходів, спрямованих на запобігання розголошенню інформації, що становить державну таємницю.

З метою охорони державної таємниці впроваджуються:

– єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

– дозвільний порядок провадження органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею;

– обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

– обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;

– особливості здійснення органами державної влади їх функцій щодо органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею;

– режим секретності органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею;

– спеціальний порядок допуску та доступу громадян до державної таємниці;

– технічний та криптографічний захисти секретної інформації.

Єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передачі та транспортування матеріальних носіїв секретної інформації встановлюються Кабінетом Міністрів України.

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, надається органам державної влади, 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, використання державних шифрів та криптографічних засобів тощо;

– мають режимно-секретний орган, якщо інше не передбачено цим Законом.

Термін дії дозволу на провадження діяльності, пов'язаної з державною таємницею, встановлюється Службою безпеки України і не може перевищувати 5 років.

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, може бути скасований Службою безпеки України на підставі акта проведеної нею перевірки, висновки якого містять дані про недодержання органом державної влади, органом місцевого самоврядування, підприємством, установою, організацією умов.

Органам державної влади, органам місцевого самоврядування, підприємствам, установам, організаціям, що провадять діяльність, пов'язану з державною таємницею, за результатами спеціальної експертизи надаються відповідні категорії режиму секретності, що зазначаються Службою безпеки України у дозволах на провадження діяльності, пов'язаної з державною таємницею.

3. Організаційно-правова структура системи охорони державної таємниці

Система охорони державної таємниці – організована державою сукупність суб'єктів, що провадять діяльність, пов'язану з державною таємницею, повноваженнями яких, згідно чинного законодавства України, є розробка і реалізація організаційно-правових, інженерно-технічних, криптографічних, оперативно-розшукових та інших заходів, спрямованих на запобігання розголошенню відомостей, що становлять державну таємницю та втратам

матеріальних носіїв секретної інформації і використання цієї інформації на шкоду безпеці держави.

Перший рівень – вищі органи державної влади, другий – центральні органи державної влади, третій – місцевий рівень (виконання політики охорони державної таємниці).

Рівень 1. Президент України, Рада національної безпеки та оборони при Президентові України, Верховна Рада України, Кабінет Міністрів України.

Рівень 2. Міністерства та відомства (галузева охорона державної таємниці), Служба безпеки України (спеціально уповноважений орган у сфері охорони державної таємниці).

Рівень 3. Місцеві органи державної влади та місцевого самоврядування, режимно-секретні органи об'єктів інформаційної діяльності, на яких обробляється державна таємниця.

Підсистеми системи охорони державної таємниці: управління (керування), виконання, інформування, забезпечення та контролю.

До підсистеми управління відносяться такі рівні:

1) Вищі державні органи (визначення політики ОДТ та напрямків її реалізації, координація дій):

– Президент України (згідно із статтями 102, 106 Конституції України);

– Рада національної безпеки та оборони при Президентові України відповідно до Закону України "Про Раду національної безпеки і оборони України" (від 05.03.1998 р. № 183/98-ВР));

– Верховна Рада України (за статтею 4 Закону України "Про державну таємницю");

– Кабінет Міністрів України (відповідно до Закону України "Про Кабінет Міністрів України" (від 27.02.2014 № 794- VII));

– Конституційний суд України вирішує питання відповідності законів та інших правових актів у сфері охорони державної таємниці Конституції України;

– Державні експерти з питань таємниць – це посадові особи, які уповноважені Указом Президента України "Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць" (від

01.12.2009 р. №987/2009) здійснювати, у межах компетенції визначеної Законом України “Про державну таємницю”;

2) Міністерства і центральні ОВВ:

– Міністерство оборони України;

– Міністерство закордонних справ України;

– Міністерства внутрішніх справ України за “Положення про Міністерство внутрішніх справ України” від 06.04.2011 р. №383/2011;

– інші міністерства, національні комісії та центральні органи виконавчої влади (*наприклад* Державна прикордонна служба України веде розвідувальну, інформаційно-аналітичну та оперативно-розвідувальну діяльність в інтересах забезпечення захисту державного кордону України згідно із Законами України “Про розвідувальні органи України” та “Про оперативно-розшукову діяльність”;

– Державне космічне агентство України;

– інспекції, центральні органи виконавчої влади зі спеціальним статусом, інші центральні органи виконавчої влади).

До підсистеми виконання належать:

– Місцеві органи виконавчої влади;

– Органи місцевого самоврядування, підприємства, установи і організації, що провадять діяльність, пов’язану з державною таємницею;

– Режимно-секретні органи.

До підсистеми забезпечення та контролю належать:

– Суди загальної юрисдикції;

– Прокуратура України;

– Служба Безпеки України;

– Служба зовнішньої розвідки України.

До підсистеми інформування належать:

– департаменти та управління охорони державної таємниці;

– режимно-секретні управління;

– сектори, відділи, режимно–секретних органів вищих державних органів, міністерств та відомств, центральних і місцевих органів виконавчої влади, органів місцевого самоврядування, підприємств, установ та організацій у якості постачальників самої інформації про стан охорони державної таємниці.

СЕМІНАРСЬКЕ ЗАНЯТТЯ
ТЕМА 2
ПРАВОВИЙ ЗАХИСТ ДЕРЖАВНОЇ ТАЄМНИЦІ

План семінарського заняття

1. Законодавче забезпечення захисту державної таємниці.

2. Законодавчо закріплені вимоги до інформації, що містить ознаки державної таємниці, впроваджені з метою охорони державної таємниці.

3. Організаційно-правові заходи охорони та захисту державної таємниці.

4. Організаційно-правова структура системи охорони державної таємниці.

Ключові поняття та терміни: правовий режим, доступ до інформації, законодавче регулювання, відповідальність за розголошення, інформаційна безпека, охорона державної таємниці, спеціальний допуск, режим секретності, національна безпека.

Завдання для самостійної роботи над темою

Завдання 1. Опрацювати теоретичний матеріал теми 2 дистанційного курсу “Система охорони державної таємниці” у Віртуальному університеті ЛДУ БЖД.

Завдання 2. Користуючись рекомендованою літературою та ресурсами мережі Інтернет, самостійно опрацювати та коротко законспектувати відповіді на дискусійні питання:

1. Чому державна таємниця є важливим елементом національної безпеки?

2. Які категорії інформації можуть бути віднесені до державної таємниці?

3. Чи потрібно розширювати або обмежувати перелік відомостей, що підпадають під державну таємницю?

4. Як сучасні технології впливають на безпеку секретної інформації?

5. Чи завжди порушення режиму секретності має каратися кримінальною відповідальністю?

Завдання 3. Користуючись рекомендованою літературою та лекційним матеріалом, письмово сформулюйте відповіді на ситуаційні завдання.

Ситуаційне завдання 1. Співробітник державного підприємства випадково отримав доступ до документів з грифом “Таємно”, до яких він не має офіційного дозволу. Які його дії будуть правомірними, а які можуть спричинити відповідальність?

Ситуаційне завдання 2. Журналіст отримав від анонімного джерела інформацію, яка містить відомості про військові операції країни. Чи має він право її опублікувати? Які правові наслідки можуть настати в разі публікації?

Ситуаційне завдання 3. Відомий науковець під час міжнародної конференції випадково розповів колегам з іншої країни про деякі розробки свого інституту, які можуть становити державну таємницю. Чи є в його діях порушення закону? Яка відповідальність може настати?

ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ

1. Окресліть історичні витоки процесу формування сучасного законодавства у сфері охорони державної таємниці.
2. Відповідно до яких ознак охорона державної таємниці набуває системних ознак?
3. Відповідно до Наказу від червня 1911 р. які відомості з оборонних питань підлягали захисту?
4. Які відомості входили до першого у XX ст. Зводу відомостей, що становлять державну таємницю (від грудня 1912 року)?
5. Що призвело до неможливості чіткої градації між таємною інформацією й відкритою в часи Першої світової війни?
6. Назвіть характерні особливості загальнодержавної системи охорони державної таємниці, що успадкована Україною від колишнього СРСР.
7. Яку подію можна вважати початком створення сучасної системи охорони державної таємниці?
8. Які Законодавчі акти заклали фундамент демократичного розвитку інформаційної сфери України?

9. Які ознаки мають місце у визначенні державної таємниці?
10. Яка інформація відноситься до державної таємниці у порядку, встановленому Законом України “Про державну таємницю”?
11. Яку інформацію забороняється відносити до державної таємниці?
12. Назвіть перелік організаційно-правових заходів охорони та захисту державної таємниці?
13. Що являє собою система охорони державної таємниці в Україні?
14. Охарактеризуйте структуру системи охорони державної таємниці в Україні.
15. Які рівні відносяться до підсистеми управління системи охорони державної таємниці?
16. Які рівні відносяться до підсистеми виконання системи охорони державної таємниці?
17. Які рівні відносяться до підсистеми забезпечення та контролю системи охорони державної таємниці?
18. Які рівні відносяться до підсистеми інформування системи охорони державної таємниці?
19. Як політична трансформація України після здобуття незалежності вплинула на формування національної системи охорони державної таємниці та її відмінність від радянської моделі?
20. Яку роль відіграли міжнародні стандарти безпеки (наприклад, стандарти НАТО) у модернізації української системи захисту державної таємниці?
21. Чи існує ризик надмірної класифікації інформації в Україні, і як це може впливати на прозорість державного управління?
22. Як технологічний розвиток (зокрема використання хмарних обчислень та мобільних пристроїв) змінює підходи до захисту державної таємниці?
23. Які юридичні наслідки має порушення режиму секретності в умовах воєнного стану, і чим вони відрізняються від мирного часу?
24. Наскільки ефективною є взаємодія між Службою безпеки України та іншими органами державної влади у сфері охорони державної таємниці, і які структурні вдосконалення могли б підвищити її результативність?

Рекомендована література: [1-3, 5, 7, 14, 21, 24-25].

ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ

1. Який закон України визначає поняття “державна таємниця”?
    а) Закон України “Про державну таємницю”.
    б) Закон України “Про доступ до публічної інформації”.
    в) Конституція України.
    г) Закон України “Про інформацію”.

2. Яка інформація може бути віднесена до державної таємниці?
    а) Відомості у сфері оборони, економіки, науки і техніки.
    б) Дані про екологічний стан країни.
    в) Інформація про соціально-економічні показники.
    г) Відомості про якість харчових продуктів.

3. Що є головною метою законодавчого забезпечення захисту державної таємниці?
    а) Охорона інформації, розголошення якої може завдати шкоди національній безпеці.
    б) Обмеження доступу громадян до будь-якої інформації.
    в) Регулювання діяльності приватних компаній.
    г) Контроль за медіа та журналістськими розслідуваннями.

4. Що НЕ може бути віднесене до державної таємниці?
    а) Інформація про екологічний стан та стан здоров’я населення.
    б) Відомості про мобілізаційні плани.
    в) Дані про військові операції.
    г) Відомості про державні оборонні закупівлі.

5. Яка організація в Україні є спеціально уповноваженим органом у сфері державної таємниці?
    а) Служба безпеки України.
    б) Міністерство оборони України.
    в) Кабінет Міністрів України.
    г) Верховна Рада України.

6. Яке покарання передбачене за розголошення державної таємниці?
    а) Кримінальна відповідальність.
    б) Адміністративний штраф.
    в) Усне попередження.
    г) Позбавлення громадянства.

7. Які рівні має організаційно-правова структура системи охорони державної таємниці?
    а) Вищі органи державної влади, центральні органи державної влади, місцеві органи.
    б) Президент, міністри, місцеві депутати.
    в) Військові органи, наукові установи, приватні підприємства.
    г) Державна служба, політичні партії, правоохоронні органи.

8. Які види відповідальності передбачені за порушення правил поводження з державною таємницею?
    а) Дисциплінарна, адміністративна та кримінальна.
    б) Лише адміністративна.
    в) Тільки дисциплінарна.
    г) Лише фінансова компенсація.

9. Які відомості підлягали охороні як державна таємниця у XIX-XX столітті?
    а) Дані про фортеці, мобілізаційні плани, військові розробки.
    б) Інформація про економічний розвиток країни.
    в) Відомості про наукові відкриття.
    г) Дані про сільське господарство.

10. Яке поняття визначає інформацію, доступ до якої обмежено законом?
    а) Державна таємниця.
    б) Конфіденційна інформація.
    в) Загальнодоступна інформація.
    г) Особисті дані.

11. Яка система охорони державної таємниці діяла в Україні до проголошення незалежності?
    а) Радянська загальнодержавна система.
    б) Американська система національної безпеки.
    в) Європейська модель захисту інформації.
    г) Незалежна українська правова система.

12. Яка основна функція режимно-секретних органів?
    а) Контроль за дотриманням вимог збереження державної таємниці.
    б) Надання інформації про економічний розвиток.
    в) Регулювання доступу до відкритої інформації.
    г) Розробка державної політики у сфері освіти.

13. Яке міністерство відповідає за реалізацію державної політики у сфері охорони державної таємниці?
    а) Міністерство оборони України.
    б) Міністерство освіти і науки України.
    в) Міністерство фінансів України.
    г) Міністерство інфраструктури України.

14. Який орган влади визначає державну політику щодо державної таємниці?
    а) Верховна Рада України.
    б) Міністерство внутрішніх справ України.
    в) Рада національної безпеки і оборони.
    г) Міністерство економіки України.

15. Які рівні секретності існують для державної таємниці в Україні?
    а) “Особливої важливості”, “Цілком таємно”, “Таємно”.
    б) “Обмеженого доступу”, “Конфіденційно”, “Доступно всім”.
    в) “Для службового користування”, “Приватна”, “Засекречена”.
    г) “Закрита”, “Відкрита”, “Напівсекретна”.

16. Хто затверджує Звід відомостей, що становлять державну таємницю України?
    а) Служба безпеки України.
    б) Президент України.
    в) Верховна Рада України.
    г) Міністерство юстиції України.

17. Які заходи впроваджуються для охорони державної таємниці?
    а) Організаційно-правові, інженерно-технічні, криптографічні.
    б) Лише контроль з боку силових структур.
    в) Тільки введення адміністративних обмежень.
    г) Лише шифрування даних.

18. Що є головною метою охорони державної таємниці?
    а) Захист інформації, яка має стратегічне значення для держави.
    б) Обмеження свободи слова.
    в) Запобігання витоку будь-якої інформації.
    г) Регулювання економічних показників.

19. Хто має право провадити діяльність, пов’язану з державною таємницею?
    а) Органи державної влади, підприємства та організації, які отримали спеціальний дозвіл.
    б) Будь-яка фізична особа.
    в) Лише військові установи.
    г) Виключно державні підприємства.

20. Як визначається ступінь секретності інформації?
    а) За критерієм потенційної шкоди національній безпеці.
    б) За кількістю осіб, що мають доступ.
    в) За рішенням окремих посадових осіб.
    г) За рівнем економічної значущості.

ТЕМА 3
ПРОЦЕДУРА ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ

ПЛАН

1. Доекспертна стадія віднесення інформації до державної таємниці.

2. Стадія експертного розгляду інформації для прийняття рішення про віднесення її до державної таємниці.

3. Стадія формалізації рішення.

4. Основні засади віднесення відомостей, що містять ознаки державної таємниці до різних ступенів секретності.

1. Доекспертна стадія віднесення інформації до державної таємниці

Поняття "віднесення інформації до державної таємниці" відповідно до ст. 1 Закону України "Про державну таємницю" виокремлює три основні складові процесу віднесення. Нормативна визначеність віднесення як процесу із виокремленням конкретних послідовних етапів поряд із вимогою обов'язкового їх дотримання дасть змогу забезпечити *належне проходження інформації через нього, тобто унеможливить будь-які затягування чи інші зловживання на шляху розгляду інформації на предмет її належності до державної таємниці, а також убезпечить суспільство від незаконного здійснення віднесення інформації до державної таємниці, оскільки забезпечить прозорість у прийнятті рішень та можливість громадського контролю за ними.*

Відповідно до ч. 1 ст. 9 Закону України "Про державну таємницю" головна постать з питань засекречування інформації є державний експерт з питань таємниць. Процедура вирішення питань щодо засекречення інформації передбачає участь широкого кола суб'єктів – від органів державної влади до окремих громадян.

Виконання функцій державного експерта з питань таємниць на конкретних посадових осіб покладається: у Верховній Раді України – Головою Верховної Ради України; в інших державних органах, Національній академії наук України,

на підприємствах, в установах і організаціях – Президентом України за поданням Служби безпеки України на підставі пропозицій керівників відповідних державних органів, Національної академії наук України, підприємств, установ і організацій.

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

– підстави, за якими інформацію має бути віднесено до державної таємниці;

– підстави та доцільність віднесення до державної таємниці інформації про винаходи (корисні моделі);

– 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;

– орган державної влади (органи), якому надається право приймати рішення щодо кола суб'єктів, які матимуть доступ до секретної інформації.

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

– надає висновок щодо шкоди національній безпеці України у разі розголошення конкретної секретної інформації;

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

– дає Службі безпеки України висновки 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;

– 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;

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

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

– 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".

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

– у розробці критеріїв визначення шкоди, яку може бути завдано національній безпеці України у разі розголошення секретної інформації;

– у проведенні експертизи щодо визначення важливості секретної інформації за фактами її розголошення чи втрати матеріальних носіїв такої інформації.

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

– 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;

– подавати Службі безпеки України не пізніш як через десять днів з моменту підписання рішення про віднесення відомостей до державної таємниці та висновки про скасування цих рішень, а розгорнуті переліки відомостей, що становлять державну таємницю, – у той же строк з моменту їх затвердження;

– розглядати пропозиції Служби безпеки України про віднесення інформації до державної таємниці, її розсекречення, проведення експертизи щодо визначення ступеня секретності відомостей, прийняття рішень у зв'язку із закінченням строку дії рішення про віднесення інформації до державної таємниці;

– надавати відповідний гриф секретності рішенням про віднесення інформації до державної таємниці та висновкам про скасування цих рішень залежно від важливості їх змісту;

– брати участь у засіданнях державних експертів з питань таємниць.

Державний експерт з питань таємниць має право:

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

– створювати експертні комісії з фахівців і науковців, які мають допуск до державної таємниці, для підготовки проектів рішень про віднесення інформації до державної таємниці, зниження ступеня її секретності та скасування зазначених рішень;

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

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

– одержувати в установленому порядку від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій відомості, необхідні для виконання своїх функцій.

Відповідальність Державного експерта з питань таємниць. Державний експерт з питань таємниць несе персональну відповідальність за законність і обґрунтованість свого рішення про віднесення інформації до державної таємниці

або висновку 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.

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. При цьому кожен експерт має право викласти свою думку.

Рішення про віднесення інформації до державної таємниці приймається державним експертом з питань таємниць не пізніше одного місяця з дня одержання звернення відповідного органу державної влади, органів місцевого самоврядування, підприємств, установ, організацій чи громадянина.

Принципи віднесення відомостей до державної таємниці. Принципи законності, обґрунтованості і своєчасності віднесення відомостей до державної таємниці та їх засекречування.

Потреба у віднесенні відомостей до державної таємниці повинна відповідати таким ознакам:

– перебувати в належній сфері;

– бути актуальною на момент її виявлення;

– відповідати належному рівню потенційного завдання шкоди.

Вимога належної сфери – потреба у віднесенні повинна локалізуватися у сфері *оборони; економіки; науки і техніки; зовнішніх відносин; державної безпеки та охорони правопорядку.* Актуальність на момент виявлення – повинна відповідати реаліям, які панують у цей час у сфері забезпечення охорони державної таємниці і у разі її ігнорування може спричинити шкоду національній безпеці України.

Відповідність належному рівню це здатність унаслідок свого витоку завдати національній безпеці такого рівня шкоди, який свідчить про недостатність вжиття стосовно неї заходів охорони нижчого порядку (як службова таємниця, конфіденційна інформація тощо).

Суб'єктами виявлення віднесення відомостей до державної таємниці *можуть бути:* режимно-секретні органи підприємств, установ чи організацій, міністерства, державні агентства, комітети Верховної Ради України, окремі громадяни тощо.

На етапі ініціювання з метою виявлення чи підтвердження наявності потреби відбувається попередня оцінка інформації, яка, проте, не має юридичної сили. Попередня оцінка майже тотожна оцінці розгляду інформації державним експертом та експертною комісією, є її ніби стислим та не остаточним варіантом, що передує їй. Виявлення потреби може відбуватися лише через попередню оцінку, а, отже, завжди є її обов'язковим елементом.

Не можна говорити про зняття потреби у випадку відмови експертом у подальшому розгляді інформації на предмет її віднесення до державної таємниці.

По-перше, у рішеннях державних експертів з питань таємниць присутня суб'єктивність, по-друге, не кожен розгляд потреби у віднесенні повинен закінчуватися власне віднесенням до державної таємниці.

Наступним етапом віднесення відомостей до державної таємниці є подання на розгляд державному експерту з питань таємниць.

Воно відбувається як офіційне звернення, відповідь на яке експерт має дати згідно із ч. 2 ст. 11 Закону України "Про державну таємницю" протягом одного місяця.

2. Стадія експертного розгляду інформації для прийняття рішення про віднесення її до державної таємниці

Ст. 1 Закону України "Про державну таємницю" – "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".

Документальним закріпленням цієї стадії є *рішення державного експерта з питань таємниць про віднесення інформації до державної таємниці* або обґрунтована відмова у прийнятті такого рішення. Суб'єктами на стадії експертного розгляду є державні експерти та створені ними експертні комісії. Рекомендацію надає експертна комісія, як дорадчий орган державного експерта з питань таємниць, вона також готує проект рішення державного експерта.

Комісія здійснює оцінку шкоди національній безпеці у разі витоку такої інформації, визначається чи варто її засекречувати, а якщо так, то який ступінь обмеження доступу найбільше б відповідав її важливості, і на основі цього виносить рекомендації державному експерту.

Під час прийняття рішення експертом не виключається повторний ним аналіз інформації, під час якого інформація знову може проходити усі п'ять етапів відбору стадії експертного розгляду або лише деякі з них, до яких в експерта виникають зауваження.

Для успішного проходження інформацією стадії експертного розгляду слід дотримуватися низки вимог, а саме:

– питання про віднесення повинно розглядатися відповідним експертом;

– експертна комісія має формуватися обов'язково із фахівців галузі, із якої розглядається інформація на предмет її віднесення до державної таємниці;

– повинна використовуватися більш–менш досконала методика оцінювання шкоди національній безпеці у разі витоку такої інформації;

– державний експерт має мати достатні повноваження для збирання додаткової інформації, що потрібна для збирання рішення;

– часові строки стадії, які встановлюються законом, повинні бути не меншими за ті затрати часу, що реально необхідні для прийняття обґрунтованого рішення.

Після прийняття експертом остаточного рішення про віднесення інформації до державної таємниці, воно надсилається в СБ України.

3. Стадія формалізації рішення

На першому етапі – орган СБ України здійснює перевірку рішення державного експерта на предмет відповідності встановленим законодавством вимогам (передусім Конституції України, Закону України "Про державну таємницю" тощо).

За наявності недоліків (недостатня мотивувальна частина, відсутність обов'язкових реквізитів тощо) рішення повертається на доопрацювання.

За відсутності зауважень до формально-юридичної частини рішення, воно включається до ЗВДТ, про що видається відповідний наказ.

Етап узгодження рішення державного експерта із СБ України. Мета – не допустити набуття законної сили рішеннями, що прийнятті всупереч закону чи не відповідають його вимогам.

Етап внесення змін у ЗВДТ та їх юридичне оформлення. На основі нових рішень державних експертів СБ України вносить зміни протягом не більше як трьох місяців та надсилає його нову редакцію до Міністерства юстиції України на реєстрацію.

Етап віднесення інформації до державної таємниці – *оприлюднення змін до Зводу відомостей, що становлять державну таємницю.* Результатом цього етапу є набуття рішенням законної сили і тим самим завершення процесу віднесення інформації до державної таємниці України.

Приведення матеріальних носіїв інформації у відповідність із новим ЗВДТ чи змінами до нього.

Висновок державного експерта з питань таємниць про скасування рішення про віднесення інформації до державної таємниці є підставою для вилучення інформації зі Зводу відомостей, що становлять державну таємницю.

Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи зміни до нього.

У рішенні державного експерта з питань таємниць зазначаються:

– інформація, яка має становити державну таємницю;

– підстави для віднесення інформації до державної таємниці та обґрунтування шкоди національній безпеці України у разі її розголошення;

– ступінь секретності зазначеної інформації;

– обсяг фінансування заходів, необхідних для охорони такої інформації;

– орган державної влади, орган місцевого самоврядування, підприємство, установа, організація чи громадянин, який вніс пропозицію про віднесення цієї інформації до державної таємниці, та орган державної влади (органи), якому надається право визначати коло суб'єктів, які матимуть доступ до цієї інформації;

– строк, протягом якого діє рішення про віднесення інформації до державної таємниці.

Зміни до Зводу відомостей, що становлять державну таємницю, публікуються не пізніше трьох місяців з дня одержання Службою безпеки України відповідного рішення чи висновку державного експерта з питань таємниць.

Органи державної влади 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, що провадять діяльність, пов'язану із державною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю.

4. Основні засади віднесення відомостей, що містять ознаки державної таємниці, до різних ступенів секретності

Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації.

Для інформації із ступенем секретності:

– "*особливої важливості*" *– 30 років*;

– для інформації "*цілком таємно*" *– 10 років*;

– для інформації "*таємно*" *– 5 років.*

Після закінчення передбаченого строку дії – висновок про скасування рішення про віднесення її до державної таємниці або рішення про продовження строку дії зазначеного рішення в межах строків. Президент України може встановлювати більш тривалі строки дії рішень про віднесення інформації до державної таємниці. Підвищення або зниження ступеня секретності інформації

та скасування рішення про віднесення її до державної таємниці здійснюються на підставі висновку державного експерта з питань таємниць або на підставі рішення суду, оформляються Службою безпеки України шляхом внесення відповідних змін до Зводу відомостей, що становлять державну таємницю.

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.

Засекречування матеріальних носіїв інформації здійснюється шляхом надання відповідному документу, виробу або іншому матеріальному носію інформації *грифа секретності.*

Реквізити кожного матеріального носія секретної інформації мають містити гриф секретності, який відповідає: ступеню секретності інформації, встановленому рішенням державного експерта з питань таємниць, – "особливої важливості", "цілком таємно", "таємно", дату та строк засекречування матеріального носія секретної інформації, що встановлюється з урахуванням строків дії рішення про віднесення інформації до державної таємниці, підпис, його розшифрування та посаду особи, яка надала зазначений гриф, а також посилання на відповідний пункт (статтю) Зводу відомостей, що становлять державну таємницю.

Після закінчення встановлених строків засекречування матеріальних носіїв інформації та у разі підвищення чи зниження ступеня секретності такої інформації або скасування рішення про віднесення її до державної таємниці – зобов'язані протягом шести місяців забезпечити зміну грифа секретності або розсекречування цих матеріальних носіїв секретної інформації та письмово повідомити про це.

Громадяни та юридичні особи мають право внести *мотивовану пропозицію про розсекречування цього носія інформації.* Зазначені посадові особи повинні *протягом одного місяця* дати громадянину чи юридичній особі письмову відповідь з цього приводу.

СЕМІНАРСЬКЕ ЗАНЯТТЯ
ТЕМА 3
ПРОЦЕДУРА ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ

План семінарського заняття

1. Доекспертна стадія віднесення інформації до державної таємниці.

2. Стадія експертного розгляду інформації для прийняття рішення про віднесення її до державної таємниці.

3. Стадія формалізації рішення.

4. Основні засади віднесення відомостей що містять ознаки державної таємниці до різних ступенів секретності.

Ключові поняття та терміни: процедура засекречування, державний експерт з питань таємниць, Звід відомостей, гриф секретності, режим секретності.

Завдання для самостійної роботи над темою

Завдання 1. Опрацювати теоретичний матеріал теми 3 дистанційного курсу “Система охорони державної таємниці” у Віртуальному університеті ЛДУ БЖД.

Завдання 2. Користуючись рекомендованою літературою та теоретичним матеріалом лекції самостійно опрацювати та розв’язати ситуаційні завдання.

Ситуаційне завдання 1: Компанія випадково розкрила конфіденційну інформацію про новий продукт до офіційного релізу. Які можуть бути наслідки та як слід було б захистити ці дані?

Ситуаційне завдання 2: Вам стали відомі внутрішні фінансові дані компанії у якій ви працюєте. Що ви повинні зробити, щоб ці дані залишалися конфіденційними?

Ситуаційне завдання 3: У навчальному закладі обговорюються персональні дані студентів. Яких законодавчих та етичних принципів слід дотримуватися, щоб забезпечити їх захист?

Ситуаційне завдання 4: Ваш колега попросив доступ до документів компанії з грифом “Для службового користування”. Які ваші дії, якщо ця людина не має права доступу?

Завдання 3. Користуючись рекомендованою літературою та теотетичним матеріалом лекції підготувати аргументи для обговорення дискусійних тем.

Дискусійні теми:

– Чи можна виправдати порушення обмеженого доступу до інформації у випадках суспільної необхідності (*наприклад*, під час розслідувань)?

– Як, на вашу думку, зміниться регулювання доступу до інформації в епоху цифрових технологій та глобальної інформаційної взаємодії?

ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ

1. Охарактеризуйте складові процесу віднесення інформації до державної таємниці.
2. Окресліть теоретичні засади процедури віднесення інформації до державної таємниці.
3. Яка мета нормативної визначеності віднесення інформації до державної таємниці, як процесу із виокремленням конкретних послідовних етапів?
4. Окресліть мету діяльності, роль та функції державного експерта з питань таємниць.
5. Які органи мають повноваження покладати виконання функцій державного експерта з питань таємниць на конкретних посадових осіб?
6. Що визначає державний експерт з питань таємниць відповідно до покладених на нього завдань?
7. Які функції виконує державний експерт з питань таємниць відповідно до покладених на нього завдань? *(9 пунктів).
8. Назвіть права державного експерта з питань таємниць під час виконання покладених на нього функцій.
9. Назвіть обов’язки державного експерта з питань таємниць.

10. Окресліть персональну відповідальність державного експерта з питань таємниць під час виконання покладених на нього функцій.
11. Які терміни прийняття рішення про віднесення інформації до державної таємниці державним експертом з питань таємниць?
12. В чому полягають принципи законності, обґрунтованості і своєчасності при віднесенні відомостей до державної таємниці та їх засекречування?
13. Опишіть процес формування потреби у віднесенні відомостей до державної таємниці?
14. Охарактеризуйте етап подання інформації на розгляд державному експерту з питань таємниць при віднесенні відомостей до державної таємниці.
15. Охарактеризуйте стадію експертного розгляду інформації для прийняття рішення про віднесення її до державної таємниці.
16. Які вимоги висуваються до інформації для проходження нею стадії експертного розгляду?
17. Охарактеризуйте методику обрахування шкоди процесу віднесення відомостей до державної таємниці.
18. Охарактеризуйте Стадію формалізації рішення процесу віднесенні відомостей до державної таємниці.
19. Перерахуйте яка інформація зазначається у рішенні державного експерта з питань таємниць.
20. Охарактеризуйте процес публікації Зводу відомостей, що становлять державну таємницю.
21. Перерахуйте стадії та етапи процесу віднесення відомостей до державної таємниці.
22. Назвіть засади віднесення відомостей, що містять ознаки державної таємниці, до різних ступенів секретності.
23. Охарактеризуйте процес засекречування матеріальних носіїв інформації та надання грифа секретності.
24. Як відбувається зміна грифа секретності або розсекречування матеріальних носіїв секретної інформації?

Рекомендована література: [1-3, 5, 7, 14, 21, 24-25].

ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ

1. Який закон України визначає процедуру віднесення інформації до державної таємниці?
   а) Закон України “Про державну таємницю”.
   б) Закон України “Про інформацію”.
   в) Конституція України.
   г) Закон України “Про доступ до публічної інформації”.

2. Хто приймає рішення про віднесення інформації до державної таємниці?
   а) Державний експерт з питань таємниць.
   б) Міністр оборони України.
   в) Президент України.
   г) Голова Верховної Ради України.

3. Який етап є першим у процесі віднесення інформації до державної таємниці?
   а) Доекспертна стадія.
   б) Стадія експертного розгляду.
   в) Стадія формалізації рішення.
   г) Стадія публікації.

4. Яке рішення може прийняти державний експерт з питань таємниць щодо інформації?
   а) Віднесення до державної таємниці або відмова у засекреченні.
   б) Надання безстрокового статусу таємності.
   в) Засекречення без можливості перегляду.
   г) Визнання інформації відкритою для всіх.

5. Які рівні секретності встановлюються для державної таємниці?
   а) “Особливої важливості”, “Цілком таємно”, “Таємно”.
   б) “Конфіденційно”, “Службове використання”, “Загальнодоступно”.
   в) “Критично важливо”, “Таємно”, “Секретно”.
   г) “Державний доступ”, “Обмежений доступ”, “Конфіденційний”.

6. Яка головна мета процедури віднесення інформації до державної таємниці?
    а) Захист інформації, розголошення якої може завдати шкоди національній безпеці.
    б) Обмеження доступу громадян до інформації.
    в) Захист комерційних інтересів приватних компаній.
    г) Зменшення кількості інформаційних витоків.

7. Що є основним критерієм віднесення інформації до державної таємниці?
    а) Можлива шкода національній безпеці у разі її розголошення.
    б) Її висока наукова цінність.
    в) Великий суспільний інтерес.
    г) Державна власність на інформацію.

8. Який документ містить інформацію, що становить державну таємницю?
    а) Звід відомостей, що становлять державну таємницю.
    б) Кримінальний кодекс України.
    в) Закон України “Про доступ до публічної інформації”.
    г) Наказ Міністерства юстиції України.

9. Який суб’єкт є відповідальним за ведення Зводу відомостей, що становлять державну таємницю?
    а) Служба безпеки України.
    б) Міністерство юстиції України.
    в) Державне бюро розслідувань.
    г) Рада національної безпеки і оборони.

10. Що є результатом останнього етапу процедури віднесення інформації до державної таємниці?
    а) Оприлюднення змін до Зводу відомостей, що становлять державну таємницю.
    б) Засекречення всіх матеріальних носіїв інформації.
    в) Автоматичне продовження терміну секретності.
    г) Ухвалення закону про державну безпеку.

11. Який строк засекречування встановлений для інформації з грифом “особливої важливості”?
    а) 30 років.
    б) 10 років.
    в) 15 років.
    г) 5 років.

12. Який етап слідує після виявлення потреби у засекречуванні інформації?
    а) Передача питання державному експерту.
    б) Оприлюднення інформації у відкритих джерелах.
    в) Автоматичне віднесення інформації до державної таємниці.
    г) Надання дозволу на її комерційне використання.

13. Які органи можуть ініціювати процес віднесення інформації до державної таємниці?
    а) Органи державної влади, місцевого самоврядування, підприємства, громадяни.
    б) Лише Президент України.
    в) Лише Міністерство оборони України.
    г) Виключно Служба безпеки України.

14. Що відбувається на стадії експертного розгляду інформації?
    а) Оцінка можливої шкоди національній безпеці та прийняття рішення.
    б) Засекречення всіх державних документів.
    в) Видалення інформації з державних реєстрів.
    г) Виключення інформації із загального доступу.

15. Який орган контролює відповідність рішень державного експерта вимогам законодавства?
    а) Служба безпеки України.
    б) Міністерство фінансів України.
    в) Верховна Рада України.
    г) Конституційний Суд України.

16. Що є підставою для розсекречування інформації?
    а) Закінчення строку засекречування або рішення державного експерта.
    б) Запит будь-якого громадянина.
    в) Втрата інформації у процесі архівування.
    г) Публікація в засобах масової інформації.

17. Яка процедура є обов’язковою перед прийняттям рішення про засекречування інформації?
    а) Попередня оцінка можливої шкоди національній безпеці.
    б) Внесення змін до Конституції України.
    в) Узгодження з міжнародними партнерами.
    г) Отримання дозволу від Міністерства оборони.

18. Що визначає рівень секретності інформації?
    а) Ступінь можливої шкоди національній безпеці.
    б) Категорія державного органу, що її генерує.
    в) Кількість осіб, які мають до неї доступ.
    г) Важливість інформації для політичних рішень.

19. Як можна оскаржити рішення про засекречування інформації?
    а) Через суд або вищий орган влади.
    б) Через громадське обговорення.
    в) Через звернення до місцевої ради.
    г) Через міжнародні інстанції.

20. Що є кінцевим результатом всього процесу віднесення інформації до державної таємниці?
    а) Включення її до Зводу відомостей, що становлять державну таємницю.
    б) Присвоєння їй нового правового статусу.
    в) Надання грифа “особливої важливості” всій державній документації.
    г) Розробка нового законопроєкту щодо секретності.

ТЕМА 4
ДОСТУП ДО ІНФОРМАЦІЇ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЇЇ ВИКОРИСТАННЯ

ПЛАН

1. Поняття “допуск” та “доступ” до інформації з обмеженим доступом.

2. Форми допуску до державної таємниці.

3. Організація допуску до відомостей, що становлять державну таємницю.

4. Порядок отримання спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею.

5. Обов’язкові умови, пов’язані із забезпеченням безпеки використання, збереження та захисту державної таємниці.

6. Технічний захист інформації, що містить державну таємницю.

1. Поняття “допуск” та “доступ” до інформації з обмеженим доступом

Доступ до інформації – це передбачений правовими нормами порядок отримання, використання, поширення та зберігання інформації. Він визначає умови, за яких особа може ознайомитися з відомостями, необхідними для реалізації своїх прав, виконання обов’язків або здійснення певної діяльності. Правовий інститут доступу до інформації забезпечує баланс між відкритістю суспільного життя, правом громадян на інформацію та потребою держави у захисті інформації, що становить державну, комерційну чи іншу охоронювану законом таємницю.

Порядок доступу до інформації є різновидом спеціальних правових режимів, які встановлюють сукупність правил, закріплених у юридичних нормах, що регулюють певні види суспільних відносин у сфері інформаційної діяльності. Цей порядок визначає, хто, яким чином, у які строки та на яких умовах може отримати інформацію, а також передбачає відповідальність за порушення встановлених вимог.

Основні характеристики порядку доступу до інформації

Головними характеристиками порядку доступу до інформації є:

– Суб'єкт визначення доступності інформації – це орган державної влади, місцевого самоврядування, юридична чи фізична особа, яка володіє інформацією і має право визначати умови її поширення або обмеження. Саме цей суб'єкт приймає рішення про ступінь відкритості інформації, визначає, чи підлягає вона оприлюдненню, чи має статус обмеженого доступу.

– Коло суб'єктів, які мають доступ до інформації – це визначені законом або власником інформації особи, яким дозволено ознайомлюватися з відповідними даними. До таких суб'єктів можуть належати громадяни, посадові особи, представники юридичних осіб, державні службовці або інші категорії осіб, уповноважені законом чи договором.

– Особливі вимоги і правила збереження та поширення інформації – це комплекс норм, які визначають технічні, організаційні та правові заходи захисту інформації. Вони встановлюють порядок реєстрації, зберігання, передачі, копіювання та знищення інформаційних матеріалів. Залежно від виду інформації застосовуються різні рівні захисту – від загальнодоступного до цілком таємного.

– Термін дії порядку – визначається законом або рішенням суб'єкта, який встановлює режим доступу. Термін може бути постійним (для відкритої інформації) або обмеженим (для інформації з тимчасовим режимом секретності). Після закінчення встановленого строку інформація може бути розсекречена або переведена до архіву з іншим рівнем доступу.

Поняття суб'єкта доступу до інформації

Суб'єкт, який має доступ до інформації, – це фізична або юридична особа, якій надано право ознайомлення з матеріальними носіями інформації або їх використання. Надання доступу означає офіційне визнання того, що суб'єкт має законні підстави для ознайомлення з відповідними даними. Права таких суб'єктів можуть бути обмежені законом у разі, якщо доступ до певної інформації суперечить державним, суспільним або приватним інтересам.

Кожен суб'єкт, який отримав право доступу, несе персональну відповідальність за дотримання правил збереження, нерозголошення та

правильного використання отриманих відомостей. Ця відповідальність може мати дисциплінарний, адміністративний або кримінальний характер залежно від ступеня порушення.

Порядок доступу до інформації

Порядок доступу до інформації означає певну сукупність правил, якими позначені особливі вимоги і правила зберігання та поширення інформації. Він охоплює такі етапи:

– подання запиту на отримання інформації;

– розгляд запиту відповідним органом або суб'єктом;

– прийняття рішення про надання, обмеження чи відмову в наданні доступу;

– ознайомлення запитувача з інформацією у визначеній формі (усній, письмовій, електронній тощо);

– забезпечення збереження та обліку фактів надання доступу.

Порядок також визначає строки відповіді на запит, перелік підстав для відмови в доступі, процедуру оскарження рішень, а також гарантії дотримання прав громадян на інформацію.

Види доступу до інформації

Законодавство України розрізняє такі основні *види доступу до інформації*:

– Відкритий доступ, який забезпечує вільне отримання, використання та пош– ирення інформації без спеціального дозволу.

Обмежений доступ, що охоплює інформацію, яка становить державну, службову, комерційну або іншу таємницю, а також конфіденційні відомості про фізичних осіб.

– Спеціальний доступ, який надається за особливих процедур (наприклад, доступ до державної таємниці).

Критеріями віднесення інформації до обмеженого доступу є її зміст, можливі наслідки розголошення, рівень важливості для безпеки держави чи інтересів осіб.

Допуск та доступ до державної таємниці

Допуск до державної таємниці – це оформлення права громадянина на доступ до секретної інформації. Він надається за результатами спеціальної перевірки, яка визначає надійність, доброчесність та відсутність підстав для

обмеження доступу. Допуск оформлюється шляхом видачі відповідного документа (допуску) визначеного ступеня секретності.

Доступ до державної таємниці – це фактичне надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею. Такий доступ може надаватися як на підставі виданого допуску, так і відповідно до службових повноважень особи, якщо її посада передбачає роботу з секретними матеріалами.

Процедура допуску і доступу передбачає дотримання ряду етапів: подання заяви, проведення перевірки, прийняття рішення компетентним органом, оформлення зобов'язання про нерозголошення, а також інструктаж з правил роботи із секретними матеріалами.

Обмеження та відповідальність

Доступ до інформації може бути обмежений у випадках, коли її розголошення може завдати шкоди:

– національній безпеці;

– громадському порядку;

– правам і свободам інших осіб;

– інтересам правосуддя або розслідування.

Особи, які порушують встановлений порядок доступу, несуть відповідальність згідно із законодавством України. Залежно від характеру порушення це може бути:

– дисциплінарна відповідальність (для посадових осіб);

– адміністративна відповідальність (за неналежне зберігання або розголошення інформації);

– кримінальна відповідальність (за розголошення державної таємниці або використання інформації на шкоду державі).

Таким чином, порядок доступу до інформації – це комплексна система правових, організаційних і технічних заходів, спрямованих на забезпечення реалізації права громадян на інформацію та захист державних і приватних інтересів. Вона базується на принципах законності, обґрунтованості, пропорційності та відповідальності. Дотримання цих принципів є запорукою

прозорості управлінських процесів, довіри громадян до держави і стабільності інформаційної безпеки суспільства.

2. Форми допуску до державної таємниці

Загальні положення

Допуск до державної таємниці є складовою частиною системи охорони секретної інформації та одним із найважливіших елементів державної політики у сфері національної безпеки. Він передбачає надання громадянину України права на доступ до інформації з певним ступенем секретності з метою виконання службових або професійних обов'язків.

Відповідно до статті 22 Закону України "Про державну таємницю", допуск до державної таємниці із ступенями секретності "особливої важливості", "цілком таємно" та "таємно" надається дієздатним громадянам України віком від 18 років, які потребують такого допуску за умовами своєї службової, виробничої, наукової, науково-дослідної діяльності або навчання. Рішення про надання допуску оформлюється наказом чи письмовим розпорядженням керівника установи, де працює або навчається громадянин, за погодженням із відповідними органами Служби безпеки України.

Допуск є індивідуальним і персоніфікованим правом, що підтверджується офіційним документом встановленого зразка. Він не передається іншим особам і не може бути використаний поза межами визначених повноважень чи службових обов'язків.

Принципи надання допуску

Процедура надання допуску до державної таємниці базується на низці основоположних принципів, серед яких:

Законність – усі дії щодо оформлення, надання, продовження або анулювання допуску здійснюються виключно на підставі норм законодавства.

Персональна відповідальність – кожна особа, якій надано допуск, несе індивідуальну відповідальність за дотримання вимог режиму секретності.

Необхідність і достатність – допуск надається лише тим особам, для яких ознайомлення з державною таємницею є необхідним для виконання конкретних завдань.

Обґрунтованість – рішення про надання допуску приймається після перевірки обставин, що свідчать про благонадійність особи та відсутність підстав для відмови.

Конфіденційність – сама інформація про факт оформлення допуску, його форму, строк дії чи ступінь секретності також підлягає захисту.

Форми допуску до державної таємниці

В Україні встановлено три основні форми допуску до державної таємниці, які визначаються залежно від ступеня секретності інформації, до якої передбачається доступ, та строку дії такого допуску.

Форма 1 – для роботи з секретною інформацією із ступенем секретності «особливої важливості», «цілком таємно» і «таємно».

Строк дії: 5 років.

Характеристика: найвищий рівень перевірки особи, що передбачає всебічне дослідження біографічних, професійних, фінансових та морально-етичних аспектів її діяльності. Перевіряються також близькі родичі, місце проживання, коло спілкування та можливі ризики компрометації.

Сфера застосування: робота у вищих органах державної влади, структурах сектору безпеки та оборони, спеціальних службах, стратегічних підприємствах, у наукових установах, які здійснюють дослідження з питань оборони та технологій подвійного призначення.

Форма 2 – для роботи з секретною інформацією із ступенем секретності «цілком таємно» і «таємно».

Строк дії: 10 років.

Характеристика: передбачає проведення спеціальної перевірки, однак із дещо меншими обсягами, ніж для форми 1. Застосовується для осіб, які мають постійний доступ до службових документів підвищеної секретності, але не до найвищого рівня державних секретів.

Сфера застосування: робота у військових частинах, на оборонних підприємствах, у наукових організаціях, підрозділах внутрішніх справ, установах, що здійснюють оперативну або технічну діяльність із захисту державної безпеки.

Форма 3 – для роботи з секретною інформацією із ступенем секретності «таємно».

Строк дії: 15 років.

Характеристика: базовий рівень перевірки, який дає можливість ознайомлюватися з інформацією, що має нижчий ступінь секретності, але все ж потребує захисту від несанкціонованого розголошення.

Сфера застосування: робота у державних органах, підприємствах, навчальних закладах, які залучаються до виконання оборонних замовлень або реалізації проектів, пов'язаних з безпековою інфраструктурою.

Порядок оформлення допуску

Процедура оформлення допуску до державної таємниці включає низку послідовних етапів:

Підготовчий етап – визначення необхідності допуску та форми, відповідно до характеру виконуваної діяльності. Керівник установи готує подання до уповноваженого органу.

Проведення спеціальної перевірки – здійснюється органами Служби безпеки України. Перевіряються:

– достовірність поданих анкетних даних;

– наявність чи відсутність судимостей;

– факти притягнення до кримінальної чи адміністративної відповідальності;

– участь у діяльності, що може суперечити інтересам держави;

– можливі зв'язки з іноземними громадянами або організаціями.

Прийняття рішення – за результатами перевірки СБУ готує висновок, на підставі якого керівник установи видає наказ (розпорядження) про надання або відмову в допуску.

Ознайомлення особи з вимогами режиму секретності – включає проведення спеціального інструктажу, підписання письмового зобов'язання про нерозголошення державної таємниці та правил поводження з носіями інформації.

Оформлення документів – особі видається допуск відповідної форми, а інформація про нього вноситься до спеціального реєстру.

Обмеження та припинення дії допуску

Дія допуску до державної таємниці може бути тимчасово зупинена або анульована у таких випадках:

– закінчення строку дії допуску;

– переведення або звільнення особи з посади, яка потребує доступу;

– зміна обставин, що впливають на благонадійність (наприклад, встановлення зв’язків з іноземними структурами);

– виявлення порушень правил поводження з секретною інформацією;

– рішення компетентного органу за результатами повторної перевірки.

Особа, у якої анульовано або призупинено допуск, повинна негайно здати всі носії секретної інформації, документи та пропуски, які давали їй доступ до режимних об’єктів.

Відповідальність осіб, допущених до державної таємниці

Особи, які мають допуск до державної таємниці, несуть підвищену юридичну відповідальність за дотримання вимог законодавства. Порушення режиму секретності, умисне чи необережне розголошення секретної інформації, втрату носіїв, а також недбале ставлення до їх збереження кваліфікують як кримінальні правопорушення.

Відповідальність може бути:

– дисциплінарною – за незначні порушення внутрішнього режиму;

– адміністративною – за порушення правил охорони державної таємниці;

– кримінальною – за розголошення відомостей, що становлять державну таємницю (статті 328–330 Кримінального кодексу України).

Інститут допуску до державної таємниці є невід’ємною складовою системи національної безпеки та забезпечує контрольований доступ до чутливої інформації. Законодавчо визначені форми допуску – це механізм, який дозволяє державі регулювати рівень відкритості певних відомостей, зберігаючи баланс між інтересами безпеки та потребами ефективного управління.

Чітке дотримання порядку оформлення, перевірки, обліку та контролю за дією допусків сприяє запобіганню витоку інформації, зміцненню довіри до державних інституцій та підтриманню стабільності системи захисту державної таємниці України.

3. Організація допуску до відомостей, що становлять державну таємницю

Відповідно до статті 27 Закону України “Про державну таємницю” доступ до державної таємниці 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 Президентові України, Голові Верховної Ради України, Прем’єр-міністрові України, Голові Верховного Суду України, Голові Конституційного Суду України, Генеральному прокурору України, Голові Служби безпеки України доступ до державної таємниці усіх ступенів секретності надається за посадою після взяття *письмового зобов’язання щодо збереження державної таємниці*.

Іноземцям та особам без громадянства доступ до державної таємниці надається: на підставі міжнародних договорів України, письмового розпорядження Президента України.

Громадянам: віком від 16 років може надаватись допуск до державної таємниці із степенем секретності “цілком таємно”, “таємно”, віком від 17 років також до державної таємниці із ступеням секретності “особливої важливості”.

Надання допуску до секретної інформації передбачає:

– визначення необхідності роботи працівника установи із секретною інформацією;

– перевірку працівника установи у зв’язку з допуском до державної таємниці;

– взяття працівником управління на себе письмового зобов’язання щодо збереження державної таємниці, яка буде йому довірена;

– одержання в письмовій формі згоди працівника установи 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.

Допуск до державної таємниці НЕ оформлюється у разі:

– відсутності обґрунтованої необхідності в роботі із секретною інформацією;

– відмови працівника взяти на себе письмове зобов'язання щодо збереження державної таємниці, а також за відсутністю його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці;

– сприяння громадянином діяльності іноземної держави, іноземної організації чи 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 Законом;

– наявності у громадянина психічних захворювань, які можуть завдати шкоди охороні державної таємниці, відповідно до переліку Міністерства охорони здоров'я України і Служби безпеки України.

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

– повідомлення громадянином під час оформлення допуску недостовірних відомостей про себе;

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

– невиконання громадянином обов'язків щодо збереження державної таємниці, яка йому довірена, або довірялась раніше.

Для надання допуску до державної таємниці громадянин заповнює:

– анкету за відповідною формою, що заповнюється власноручно, підрозділ РСО та начальник відділу кадрів разом звіряють зазначені в анкеті біографічні

дані з відповідними документами, відповідно до вимог Переліку, проводять співбесіду з метою попереднього з'ясування відсутності чи наявності обставин, за яких працівнику установи, організації, підприємства може бути відмовлено у наданні допуску до державної таємниці;

– подає дві фотокартки розміром 4,5 × 6 см;

– письмове зобов'язання щодо збереження державної таємниці, яка буде йому довірена;

– підтвердження, що він ознайомлений з мірою відповідальності за порушення законодавства про державну таємницю.

Перед оформленням документів для отримання допуску до державної таємниці працівники установ, організацій чи підприємств проходять обов'язкову медичну перевірку. Її метою є визначення стану психічного здоров'я особи та виявлення можливих захворювань, які можуть негативно впливати на здатність дотримуватися вимог режиму секретності. Згідно зі спільним наказом Міністерства охорони здоров'я України та Служби безпеки України від 13 травня 2002 року № 174/136 "Про затвердження Переліку психічних захворювань (розладів), які можуть завдати шкоди охороні державної таємниці і за наявності яких допуск до державної таємниці громадянину не надається", встановлено конкретні медичні критерії, що визначають придатність особи до роботи з секретною інформацією.

До таких станів належать тяжкі форми психічних розладів, хронічні захворювання центральної нервової системи, психопатії, розлади поведінки, залежності, що можуть зумовлювати неадекватну оцінку ситуацій, порушення самоконтролю, підвищену сугестивність або агресивність. Медичний огляд проводиться спеціальною комісією, до складу якої входять психіатр, невропатолог та інші фахівці, уповноважені Міністерством охорони здоров'я.

Висновок медичної комісії є обов'язковою складовою пакета документів, необхідного для оформлення допуску. У разі виявлення розладів, передбачених у Переліку, громадянину відмовляють у наданні допуску до державної таємниці незалежно від посади чи службової потреби. Така вимога спрямована на запобігання витоку інформації, ненавмисному розголошенню або неналежному поводженню з секретними матеріалами, що може створити загрозу національній безпеці України.

Готуються та відправляються в підрозділ Управління СБ України такі документи:

– мотивований запит, підписаний начальником, у якому:

• обґрунтовується необхідність надання працівнику установи допуску до державної таємниці з посиланням на відповідну номенклатуру посад із зазначенням порядкового номера посади та форми допуску, а також зазначається кількість працівників, яким за цим порядковим номером посади вже надано допуск до державної таємниці;

• викладається отримана під час співбесіди з працівником попередня інформація, яка може мати значення для прийняття рішення про надання допуску до державної таємниці;

• повідомляються відомості, що підтверджують відсутність у працівника, щодо якого розглядається питання про надання допуску до державної таємниці, психічних захворювань, які можуть завдавати шкоди охороні державної таємниці;

– заповнену і завірену у встановленому порядку анкету з фотокарткою громадянина, щодо якого розглядається питання про надання допуску до державної таємниці, розміром 4,5 × 6 сантиметрів;

– один примірник облікової картки з фотокарткою громадянина, щодо якого розглядається питання про надання допуску до державної таємниці, розміром 4,5 × 6 сантиметрів, засвідченої, працівником РСО та скріпленої його печаткою;

– два примірники картки, у якій зазначаються результати перевірки працівника управління у зв'язку з допуском до державної таємниці. Картки заповнюються на друкарській машинці РСО установи, підписами посадових осіб картка не засвідчується;

– по два примірники інформаційного запиту, на громадянина, щодо якого розглядається питання про надання допуску до державної таємниці, та на кожного з його близьких родичів: батька, матір, рідних братів, сестер, дітей віком понад 16 років, а також на дружину (чоловіка).

Перевірка громадян у зв'язку з допуском до державної таємниці здійснюється органами СБУ у місячний строк у порядку, встановленому Законом України "Про оперативну розшукову діяльність" та "Про державну таємницю".

За результатами перевірки громадянина орган СБУ, який проводив перевірку, виносить ***мотивований висновок*** щодо надання допуску до державної таємниці чи відмову у наданні допуску. Запис: “У результаті перевірки не виявлено обставин, які перешкоджають наданню (зазначається прізвище, ім’я та по батькові) допуску до державної таємниці за формою (зазначається форма допуску)”.

Матеріали перевірок громадян, на підставі яких орган СБУ дійшов висновку про неможливість надання їм допуску до державної таємниці, зберігаються у відповідному органі СБУ протягом 10 років.

Рішення про надання громадянинові допуску до державної таємниці приймається керівником установи не пізніше ніж через 10 днів після отримання схвального висновку органу СБУ та облікової картки.

4. Порядок отримання спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею

Відповідь на це питання ми знаходимо у ст. 20 Закону України “Про державну таємницю” (далі – Закон) та Порядок організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18.12.2013 р. № 939 (далі – Порядок-939).

Спеціальний дозвіл надається органами СБУ підприємствам, установам, організаціям за умови, що вони:

– провадять або планують провадити діяльність, пов’язану з державною таємницею, відповідно до повноважень, державних завдань, програм, замовлень, договорів (контрактів);

– мають режимні приміщення та сховища матеріальних носіїв секретної інформації, які відповідають вимогам до забезпечення режиму секретності, виключають можливість доступу до них сторонніх осіб (тобто таких осіб, що не мають наданого в установленому порядку доступу до матеріальних носіїв секретної інформації) та гарантують збереження таких матеріальних носіїв;

– дотримуються передбачених законодавством вимог щодо забезпечення режиму секретності під час проведення секретних робіт і здійснення заходів, пов'язаних з використанням секретної інформації, а також порядку допуску та доступу осіб до державної таємниці, прийому іноземних громадян та іноземних делегацій, здійснення технічного та криптографічного захисту секретної інформації;

– мають режимно-секретний орган (далі – РСО) або режим секретності забезпечується його керівником чи працівником, призначеним для цього наказом керівника підприємства, установи, організації.

До складу РСО входять підрозділи: режиму, криптографічного, технічного захисту інформації, секретного діловодства, інші підрозділи.

Призначення осіб на посади заступників керівників підприємств, установ, організацій з питань режиму, начальників РСО та їх заступників, а також видання наказу про покладення на окремого працівника обов'язків щодо забезпечення режиму секретності здійснюється після погодження з органами СБУ та РСО підприємств, установ, організацій вищого рівня або підприємств, установ, організацій, що є замовниками секретних робіт.

Для розгляду питання про погодження призначення осіб на посади заступників керівників підприємств, установ, організацій з питань режиму, начальників РСО та їх заступників до органу СБУ подається підписаний керівником підприємства, установи, організації вмотивований запит.

До вмотивованого запиту додаються:

– копія документа, який містить інформацію про функціональні обов'язки, що передбачені за посадою, призначення на яку погоджується;

– копії документів, які містять інформацію про функціональні обов'язки за основною посадою;

– анкета для погодження призначення на посаду заступника керівника установи з питань режиму, начальника або заступника начальника РСО.

Для отримання спеціального дозволу підприємство, установа, організація подає органу СБУ заявку, в якій зазначаються:

– найменування підприємства, установи, організації; найменування підприємства, установи, організації, яке координує та спрямовує або до сфери

управління чи відання якого належить підприємство, установа, організація, якому надається спеціальний дозвіл;

– організаційно-правова форма;

– місцезнаходження підприємства, установи, організації, приміщень РСО та інших режимних приміщень (зон, територій), визначених для постійного зберігання матеріальних носіїв секретної інформації;

– підстави для отримання спеціального дозволу (обґрунтування).

Для проведення перевірки стану режиму секретності на підприємстві, в установі, організації наказом (розпорядженням) керівника утворюється комісія. До складу комісії включаються працівники РСО та представники інших структурних підрозділів підприємства, установи, організації, яким надано допуск до державної таємниці за відповідною формою. Комісія перевіряє стан забезпечення режиму секретності на підприємстві, в установі, організації, з'ясовує наявність умов, необхідних для провадження діяльності, пов'язаної з державною таємницею, та складає акт перевірки стану режиму секретності.

Акт перевірки стану режиму секретності повинен містити інформацію про:

– діяльність, пов'язану з державною таємницею, яку провадить чи провадитиме підприємство, установа, організація, характеристику та обсяг секретних відомостей, які використовуються або будуть використовуватися у зв'язку з провадженням такої діяльності, стан режиму секретності, його відповідність вимогам законодавства у сфері охорони державної таємниці;

– структуру РСО, його підпорядкованість, штатну чисельність працівників та їх функціональні обов'язки, призначення на посаду начальника РСО або працівника, відповідального за ведення обліку і зберігання секретних документів та здійснення заходів щодо забезпечення режиму секретності;

– наявність та місцезнаходження спеціально обладнаних приміщень (зон, територій) для проведення секретних робіт, необхідної кількості сховищ матеріальних носіїв секретної інформації, їх відповідність вимогам щодо забезпечення режиму секретності;

– номенклатуру посад працівників підприємства, установи, організації, перебування на яких потребує оформлення допуску та надання доступу до

державної таємниці (далі – номенклатура посад), кількість передбачених нею посад і фактичну чисельність працівників, яким вже надано допуск до державної таємниці;

– організацію і стан пропускного та внутрішньо об'єктового режиму, перелік інженерно-технічних засобів охорони із зазначенням їх відповідності вимогам до забезпечення режиму секретності;

– наявність перспективних і поточних планів забезпечення режиму секретності, в тому числі під час прийому іноземних делегацій та здійснення міжнародного співробітництва, стан їх виконання;

– наявність спеціальних засобів зв'язку та органу спеціального зв'язку, використання державних шифрів і криптографічних засобів, стан їх обліку;

– організацію і стан секретного діловодства, забезпечення технічного захисту секретної інформації;

– результати здійснення контролю за забезпеченням охорони державної таємниці (коли і ким проводилася остання перевірка, яких заходів вжито для усунення виявлених недоліків, виконання пропозицій і рекомендацій, із зазначенням номера та дати відповідного рішення щодо усунення недоліків тощо);

– пропозиції щодо надання підприємству, установі, організації спеціального дозволу.

У разі коли спеціальний дозвіл надається підприємству, установі, організації ***вперше****, в акті перевірки зазначаються такі відомості:*

– діяльність, пов'язану з державною таємницею, яку провадить чи провадитиме підприємство, установа, організація, характеристику та обсяг секретних відомостей, які використовуються або будуть використовуватися у зв'язку з провадженням такої діяльності, стан режиму секретності, його відповідність вимогам законодавства у сфері охорони державної таємниці;

– структуру РСО, його підпорядкованість, штатну чисельність працівників та їх функціональні обов'язки, призначення на посаду начальника РСО або працівника, відповідального за ведення обліку і зберігання секретних документів та здійснення заходів щодо забезпечення режиму секретності;

– наявність та місцезнаходження спеціально обладнаних приміщень (зон, територій) для проведення секретних робіт, необхідної кількості сховищ

матеріальних носіїв секретної інформації, їх відповідність вимогам щодо забезпечення режиму секретності;

– пропозиції щодо надання підприємству, установі, організації спеціального дозволу.

Питання про надання підприємству, установі, організації *спеціального дозволу та встановлення категорії режиму секретності* розглядається органом СБУ протягом *місяця* з дня отримання відповідної заявки. У разі виникнення кризової ситуації, що загрожує національній безпеці України – розглядається органом СБУ у *десятиденний термін* з дня отримання відповідних документів. Для проведення спеціальної експертизи орган СБУ утворює спеціальну експертну комісію. Результати спеціальної експертизи оформляються актом спеціальної експертизи, який подається на розгляд керівнику органу СБУ для прийняття рішення. На підставі поданих документів і акта спеціальної експертизи орган СБУ приймає *рішення про надання підприємству, установі, організації дозволу та встановлення категорії режиму секретності.*

Відмова в наданні спеціального дозволу приймається органом СБУ за відсутності умов, необхідних для провадження діяльності, пов'язаної з державною таємницею, про що зазначається в *акті спеціальної експертизи* з посиланням на нормативно-правові акти у сфері охорони державної таємниці.

5. Обов'язкові умови, пов'язані із забезпеченням безпеки використання, збереження та захисту державної таємниці

Під загрозами інформації з обмеженим доступом прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного оволодіння інформацією.

Джерелами зовнішніх загроз є: несумлінні конкуренти; злочинні угруповання і формування; окремі особи та організації адміністративно-управлінського апарату. Джерелами внутрішніх загроз можуть бути: адміністрація підприємства; персонал; технічні засоби забезпечення виробничої та трудової діяльності.

Співвідношення зовнішніх і внутрішніх загроз: 82 % загроз створюються співробітниками фірми або за їх прямої чи опосередкованої участі; 17 % загроз надходить ззовні – зовнішні загрози; 1 % загроз створюється випадковими особами.

Основними загрозами інформації є: *розголошення, витік, несанкціонований доступ.* Реалізується *розголошення формальними і неформальними* каналами поширення інформації.

До формальних каналів поширення інформації належать: ділові зустрічі, наради, переговори та інші форми спілкування; обмін офіційними діловими, науковими і технічними документами, засобами передачі офіційної інформації (пошта, телефон, телеграф, факс тощо).

Неформальними каналами поширення інформації є: особисте спілкування (зустрічі, переписка, телефонні переговори тощо); виставки, семінари, конференції, з'їзди, колоквіуми та інші масові заходи; засоби масової інформації (преса, інтерв'ю, радіо, телебачення тощо).

Причиною розголошення конфіденційної інформації є: слабке знання (або незнання) вимог захисту конфіденційної інформації; помилковість дій персоналу через низьку виробничу кваліфікацію; відсутність системи контролю за оформленням документів, підготовкою виступів, реклами і публікацій; злісне, навмисне невиконання вимог захисту комерційної таємниці.

Витік інформації можна розглядати як неправомірний вихід конфіденційної інформації за межі організації або кола осіб, яким ця інформація була довірена. Витік інформації завжди припускає *протиправне (таємне або явне, усвідомлене або випадкове) оволод*іння конфіденційною інформацією, незалежно від того, яким шляхом це досягається.

До факторів і обставин, які створюють передумови для витоку комерційних секретів належать:

– недостатнє знання працівниками підприємства правил захисту комерційної таємниці та нерозуміння (або неусвідомлення) необхідності їх ретельного дотримання;

– використання неатестованих технічних засобів обробки конфіденційної інформації;

– слабкий контроль за дотриманням правил захисту інформації правовими, організаційними та інженерно–технічними засобами;

– плинність кадрів, у тому числі таких, які володіють інформацією, що становить комерційну таємницю.

Несанкціонований доступ можна визначити як сукупність прийомів і порядок дій з метою одержання (добування) охоронюваних даних протиправним шляхом (таємне спостереження, перехоплення телеграфних повідомлень, підслуховування телефонних переговорів, крадіжки креслень, зразків, документів тощо).

До способів несанкціонованого доступу до інформації, які не порушують норм закону, але перебувають на межі такої ситуації, можна віднести:

– співбесіди про наймання на роботу зі службовцями конкуруючих фірм (хоча опитувач зовсім не має наміру приймати цю людини на роботу);

– так звані "помилкові" переговори з фірмою-конкурентом щодо придбання ліцензії, створення спільного підприємства, підписання партнерської угоди;

– наймання на роботу службовця конкуруючої фірми для одержання необхідної інформації;

– працевлаштування "свого" працівника на підприємство-конкурента.

Джерелами інформації, що є таємницею, а отже, потенційними джерелами витоку, можуть бути:

– документація підприємства або просто документи (вхідні-вихідні, накази, бізнес-плани, ділова переписка тощо);

– робочий персонал або просто особи (до цього поняття належать усі без винятку працівники підприємства);

– партнери, контрагенти або клієнти;

– продукція підприємства або послуги, що надаються;

– технічні засоби забезпечення виробничої діяльності;

– непрямі джерела (сміття, реклама, публікації).

Забезпечення інформаційної безпеки можна поділити на такі основні напрями:

– розробляти і вводити просту систему класифікації ступеня конфіденційності інформації, що обробляється (гриф обмеження доступу);

– встановити процедуру передання конфіденційної інформації від одного співробітника іншому, порядок її обробки і збереження залежно від ступеня таємності;

– проводити з персоналом компанії розмови про правила поводження з конфіденційною інформацією.

6. Технічний захист інформації, що містить державну таємницю

Загальні положення

Технічні заходи захисту інформації становлять комплекс організаційних, інженерних, електронних та програмно-апаратних дій, спрямованих на попередження, виявлення та нейтралізацію можливих каналів витоку, несанкціонованого доступу або знищення інформаційних ресурсів. Вони є складовою системи інформаційної безпеки установи, підприємства чи організації та мають забезпечити стабільність функціонування її інформаційно-телекомунікаційної інфраструктури.

Основою технічного захисту є використання *електронних пристроїв і спеціалізованого програмного забезпечення*, які вбудовуються у систему обробки інформації та виконують функції контролю, фільтрації, блокування або маскування даних. Ці заходи спрямовані на протидію як технічним, так і інформаційно-психологічним загрозам, забезпечуючи надійне збереження відомостей, що становлять службову, комерційну або державну таємницю.

Основні види технічних засобів захисту

До технічних засобів захисту належать різноманітні електронні системи, прилади та програмно-апаратні комплекси, які реалізують конкретні функції безпеки. Зокрема:

– *пошукові прилади* для виявлення несанкціонованих електронних пристроїв – диктофонів, мікрофонів, радіопередавачів, GPS-маячків тощо;

– *прилади охорони провідних комунікацій*, які контролюють кабельні лінії зв’язку, виявляючи спроби їх підключення чи перехоплення сигналів;

– *спеціалізоване програмне забезпечення* для моніторингу активності інформаційних систем, виявлення підозрілих процесів, шкідливого коду чи спроб несанкціонованого доступу;

– *апаратура для виявлення диктофонів та радіозакладок*, здатна фіксувати електромагнітні випромінювання у широкому діапазоні частот;

– *системи акустичного та віброакустичного зашумлення*, які створюють фоновий шум для унеможливлення прослуховування приміщень або переговорів;

– *скануючі засоби контролю електромагнітного середовища* – визначають наявність випромінювань від електронних пристроїв, які можуть використовуватися для шпигунських цілей;

– *засоби виявлення каналів витоку інформації*, що аналізують фізичні поля, акустичні коливання, теплові сигнали тощо;

– *системи спостереження та контролю за приміщеннями*, які дозволяють забезпечити оперативний моніторинг зон, де зберігається або обробляється конфіденційна інформація.

Ці засоби утворюють єдину багаторівневу систему, що охоплює як *пасивний захист* (екранування, зашумлення, фільтрація), так і *активний захист* (виявлення, реагування, блокування загроз).

Призначення апаратних засобів захисту

Апаратні засоби захисту інформації застосовуються для виконання комплексу завдань, спрямованих на недопущення несанкціонованого доступу до носіїв інформації або інформаційних систем. *Основними завданнями є:*

– *Перешкоджання візуальному спостереженню та дистанційному підслуховуванню.* Для цього використовуються засоби затемнення, екрани, шторки, системи зашумлення, генератори білого шуму, ультразвукові пристрої тощо. Вони запобігають можливості отримання даних через оптичні або акустичні канали.

– *Нейтралізація паразитних електромагнітних випромінювань і наводок.* Будь-яке електронне обладнання під час роботи генерує побічні електромагнітні сигнали, які потенційно можуть бути перехоплені. Тому використовуються екрани, фільтри, лінії із захисним заземленням, спеціальні корпуси з матеріалів, що поглинають випромінювання.

– *Виявлення технічних засобів підслуховування і магнітного запису.* Установи, що працюють із конфіденційними матеріалами, регулярно проводять технічне обстеження приміщень, під час якого за допомогою детекторів, аналізаторів спектру, металошукачів або інфрачервоних сканерів виявляють приховані пристрої запису чи передавання інформації.

– Захист інформації, що передається засобами зв'язку та знаходиться в системах автоматизованої обробки даних. Для цього застосовуються криптографічні засоби, міжмережеві екрани, шлюзи безпеки, системи контролю доступу, шифратори, апаратні токени, а також протоколи захищеного зв'язку (VPN, SSL/TLS тощо).

Класифікація апаратних засобів захисту

За своїм функціональним призначенням апаратні засоби захисту умовно поділяються на дві великі групи:

Засоби виявлення несанкціонованого доступу. До них належать системи сигналізації, сенсорні детектори, монітори цілісності кабельних ліній, датчики руху, системи відеоспостереження. Їх завдання – оперативно фіксувати факт вторгнення або спробу отримати доступ до інформаційних ресурсів.

Засоби захисту від несанкціонованого доступу. Це апаратно-програмні механізми, які запобігають безпосередньому отриманню або зміні інформації: біометричні зчитувачі, смарт-картки, криптопроцесори, захищені накопичувачі, системи багатофакторної автентифікації.

Зазначені засоби можуть функціонувати автономно або бути інтегрованими у загальну систему інформаційної безпеки підприємства, забезпечуючи комплексний контроль за всіма етапами обробки даних – від введення до зберігання і передавання.

Захист інформації від копіювання та несанкціонованого відтворення

Одним із найважливіших аспектів технічного захисту є *запобігання копіюванню інформації або програмного забезпечення* без дозволу власника. Це особливо актуально для систем, що містять службові або комерційні відомості, інтелектуальні розробки, вихідний код програм тощо.

Захист інформації від копіювання реалізується через виконання таких функцій:

Ідентифікація середовища, з якого може запускатись програма. Система перевіряє унікальні параметри апаратного середовища – серійні номери пристроїв, конфігурацію процесора, мережеві адреси тощо. Якщо середовище не збігається з авторизованим, програма не запускається.

Аутентифікація середовища, із якого запущена програма. Здійснюється перевірка цифрових підписів, сертифікатів або токенів, що підтверджують легальність програмного середовища.

Реакція на запуск із несанкціонованого середовища. У випадку спроби копіювання або незаконного запуску система може виконати блокування доступу, шифрування даних або навіть знищення робочої копії для запобігання витоку інформації.

Реєстрація санкціонованого копіювання. Кожна спроба копіювання чи перенесення даних реєструється у спеціальному журналі подій із фіксацією дати, часу, користувача та пристрою.

Протидія вивченню алгоритмів роботи системи. Застосовуються технології обфускації коду, апаратне шифрування, використання віртуальних машин або криптографічного захисту, що ускладнює аналіз алгоритмів роботи та декомпіляцію програм.

Значення технічних заходів у системі інформаційної безпеки

Технічні заходи відіграють ключову роль у забезпеченні цілісності, конфіденційності та доступності інформації. Їх ефективність залежить від узгодженості з організаційними та правовими заходами – нормативним регламентуванням, інструкціями, розмежуванням повноважень, контролем персоналу.

В умовах сучасного інформаційного суспільства технічні засоби захисту стають невід’ємним елементом діяльності державних структур, фінансових установ, оборонних підприємств, науково-дослідних центрів та інших суб’єктів, які працюють з критичною інформацією.

Комплексний підхід до їх застосування дозволяє не лише попередити витік або знищення даних, а й створити *багаторівневу систему безпеки*, здатну адаптуватися до нових технологічних викликів, у тому числі кіберзагроз, технічної розвідки, електромагнітного шпигунства та соціальної інженерії.

СЕМІНАРСЬКЕ ЗАНЯТТЯ
ТЕМА 4
ДОСТУП ДО ІНФОРМАЦІЇ
ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЇХ ВИКОРИСТАННЯ

План семінарського заняття

1. Поняття "допуск" та "доступ" до інформації з обмеженим доступом.

2. Форми допуску до державної таємниці.

3. Організація допуску до відомостей, що становлять державну таємницю.

4. Порядок отримання спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею.

5. Обов'язкові умови, пов'язані із забезпеченням безпеки використання, збереження та захисту державної таємниці.

6. Технічний захист інформації, що містить державну таємницю.

Ключові поняття та терміни: допуск до державної таємниці, доступ до відомостей, що становлять державну таємницю, служба режиму секретності, обмежувальний гриф, технічний захист інформації (ТЗІ), службова перевірка, режим секретності.

Завдання для самостійної роботи над темою

Завдання 1. Опрацювати теоретичний матеріал теми 4 дистанційного курсу "Система охорони державної таємниці" у Віртуальному університеті ЛДУ БЖД.

Завдання 2. Користуючись рекомендованою літературою та теоретичним матеріалом лекції, самостійно опрацювати та розв'язати ситуаційні завдання.

Ситуаційне завдання 1. Працівник державного органу отримав завдання ознайомитися з документами з грифом "таємно". У нього є допуск до державної

таємниці 3-ї форми. Завдання: Визначте, чи має він право отримати доступ до цих документів. Які додаткові умови повинні бути дотримані?

Ситуаційне завдання 2. Комерційна компанія планує укласти договір на виконання робіт, пов'язаних із державною таємницею. Завдання: Опишіть порядок отримання спеціального дозволу для такої діяльності та основні вимоги до організації режиму секретності в компанії.

Ситуаційне завдання 3. У приміщенні зберігаються документи з державною таємницею. Під час перевірки виявлено, що частина сейфів несправна, а система контролю доступу не працює. Завдання: Визначте, які норми та умови безпеки порушено. Запропонуйте заходи з відновлення належного рівня захисту.

Ситуаційне завдання 4. У державному органі новий співробітник випадково отримав доступ до інформації з обмеженим доступом, хоча офіційного допуску ще не мав. Завдання: Які наслідки передбачені законодавством? Які заходи має вжити керівництво?

Завдання 3. Користуючись рекомендованою літературою та теоретичним матеріалом лекції, підготувати аргументи для обговорення дискусійних тем.

Дискусійні теми:

– Чи є чинна процедура отримання допуску до державної таємниці оптимальною, чи вона потребує спрощення?

– Як співвідносити принцип відкритості державної інформації та необхідність охорони державної таємниці?

– Які сучасні технології ТЗІ (шифрування, DLP-системи, блокчейн) можуть бути застосовані для захисту державної таємниці?

ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ

1. Дайте визначення поняттям “допуск” та “доступ” до інформації з обмеженим доступом.
2. Охарактеризуйте порядок доступу до інформації з обмеженим доступом.
3. Назвіть суб’єкта, який має доступ до інформації з обмеженим доступом та його повноваження.
4. Відповідно до чого керівником установи визначаються необхідність роботи із секретною інформацією та форма допуску до державної таємниці?
5. Які форми допуску до державної таємниці встановлюються залежно від ступеня секретності інформації?
6. Яким посадовим особам доступ до державної таємниці усіх ступенів секретності надається за посадою після взяття ними письмового зобов’язання щодо збереження державної таємниці?
7. Опишіть процес прийняття рішення про надання доступу до конкретної секретної інформації та її матеріальних носіїв.
8. Опишіть процес надання доступу до державної таємниці іноземцям та особам без громадянства.
9. З якого віку громадянам України може надаватись допуск до державної таємниці?
10. Які обставини передбачають надання допуску до секретної інформації?
11. Опишіть причини відмови у наданні допуску до державної таємниці.
12. Які документи потрібні для надання допуску до державної таємниці?
13. Опишіть встановлений порядок перевірки громадян у зв’язку з допуском до державної таємниці.
14. Яким законом визначено процедуру і перелік документів для скерування до органів СБ України з метою отримання спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею?

15. Які умови надання спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею?
16. Опишіть суть, процедуру створення та функціонування режимно-секретного органу (РСО).
17. Опишіть процедуру проведення перевірки стану режиму секретності на підприємстві, в установі, організації.
18. Яка інформація міститься у Акті перевірки стану режиму секретності?
19. Які терміни передбачено для розгляду питання про надання підприємству, установі, організації спеціального дозволу та встановлення категорії режиму секретності?
20. У якому випадку надається відмова в наданні спеціального дозволу для провадження діяльності, пов’язаної з державною таємницею?
21. Дайте визначення поняттю “загрози інформації, що охороняється” та опишіть їх.
22. Опишіть загрозу інформації, що охороняється – розголошення.
23. Опишіть загрозу інформації, що охороняється – витік інформації.
24. Опишіть загрозу інформації, що охороняється – несанкціонований доступ.
25. Перерахуйте потенційні джерела витоку інформації.
26. Опишіть основні напрями забезпечення інформаційної безпеки.
27. Що являють собою технічні заходи захисту, наведіть приклад.
28. З якою метою використовуються апаратні засоби захисту інформації?
29. Наведіть класифікацію апаратних засобів захисту інформації.

Рекомендована література: [1-3, 5, 7, 14, 21, 24-25].

ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ

1. Що означає термін “допуск” до державної таємниці?
   а) Оформлення права громадянина на доступ до секретної інформації.
   б) Надання дозволу на зберігання секретної інформації.
   в) Надання доступу до загальнодоступної інформації.
   г) Проведення заходів із захисту інформації.

2. Яка основна характеристика доступу до інформації?
   а) Отримання дозволу компетентного органу на одержання інформації.
   б) Можливість передавання інформації третім особам.
   в) Автоматичний доступ до будь-якої інформації.
   г) Відсутність контролю за поширенням інформації.

3. Хто визначає доступність інформації?
   а) Особи, в компетенцію яких входить встановлення обмежень.
   б) Кожен громадянин України.
   в) Будь-яка юридична особа.
   г) Органи місцевого самоврядування.

4. Які особи можуть мати доступ до державної таємниці?
   а) Дієздатні громадяни України, яким надано допуск.
   б) Будь-які державні службовці.
   в) Лише працівники СБУ.
   г) Особи, що підписали договір про нерозголошення.

5. Яка форма допуску дає право на роботу з інформацією ступеня “особливої важливості”?
   а) Форма 1.
   б) Форма 2.
   в) Форма 3.
   г) Форма 4.

6. Хто ухвалює рішення про надання доступу до секретної інформації?
    а) Керівники органів державної влади.
    б) Будь-який посадовець.
    в) Громадянин, який запитує інформацію.
    г) Незалежна комісія.

7. Яким особам за посадою надається доступ до державної таємниці?
    а) Президентові України, Прем’єр-міністру, Голові Верховної Ради.
    б) Будь-якому державному службовцю.
    в) Виключно військовослужбовцям.
    г) Головам приватних підприємств.

8. У яких випадках може бути відмовлено в допуску до державної таємниці?
    а) За наявності психічних захворювань, які можуть загрожувати охороні державної таємниці.
    б) За наявності будь-якого медичного діагнозу.
    в) Якщо особа відмовилася подавати фотографії.
    г) Якщо особа має освіту нижче бакалавра.

9. Які джерела можуть бути причиною витоку інформації?
    а) Документація підприємства, працівники, партнери.
    б) Лише документи.
    в) Лише персонал.
    г) Лише комп’ютерні мережі.

10. Що є основною загрозою інформації?
    а) Розголошення, витік, несанкціонований доступ.
    б) Лише технічні збої.
    в) Виключно атаки хакерів.
    г) Перевантаження системи.

11. Який документ має заповнювати громадянин для отримання допуску до державної таємниці?
    а) Анкету за відповідною формою.
    б) Паспорт.
    в) Будь-який офіційний лист.
    г) Витяг з трудової книжки.

12. Які обов’язкові умови забезпечення безпеки державної таємниці?
    а) Використання криптографічного захисту.
    б) Доступ усіх співробітників до секретної інформації.
    в) Автоматичне резервне копіювання.
    г) Розголошення інформації за необхідності.

13. Що передбачає технічний захист інформації?
    а) Використання електронних пристроїв і спеціальних програм.
    б) Виключно фізичний контроль співробітників.
    в) Лише шифрування документів.
    г) Встановлення паролів на всі комп’ютери.

14. Яке співвідношення внутрішніх і зовнішніх загроз встановлюють фахівці?
    а) 82% загроз від співробітників, 17% – ззовні.
    б) 50% зовнішніх, 50% внутрішніх.
    в) 90% загроз від хакерів, 10% від персоналу.
    г) 100% загроз від третіх осіб.

15. Яке основне завдання апаратних засобів захисту?
    а) Запобігання візуальному спостереженню та дистанційному підслуховуванню.
    б) Лише шифрування документів.
    в) Захист від вірусів.
    г) Фізичний контроль приміщень.

16. Як називається процес, який забезпечує охорону інформації від незаконного вилучення?
    а) Несанкціонований доступ.
    б) Захищений доступ.
    в) Відкритий доступ.
    г) Дозволений доступ.

17. Чим відрізняється допуск від доступу до державної таємниці?
    а) Допуск – оформлення права, доступ – безпосереднє ознайомлення.
    б) Це синоніми.
    в) Допуск дається всім громадянам.
    г) Доступ дається без перевірки.

18. Яка організація видає спеціальні дозволи для роботи з державною таємницею?
    а) Служба безпеки України.
    б) Міністерство освіти.
    в) Міністерство цифрової трансформації.
    г) Верховна Рада України.

19. Що таке витік інформації?
    а) Неправомірний вихід конфіденційної інформації за межі організації.
    б) Перевірка системи захисту інформації.
    в) Офіційне оприлюднення даних.
    г) Тимчасовий збій у системі.

20. Яка головна мета забезпечення інформаційної безпеки?
    а) Захист інформації від розголошення, витоку та несанкціонованого доступу.
    б) Контроль доступу до Інтернету.
    в) Регулювання використання комп’ютерної техніки.
    г) Автоматичне блокування всіх інформаційних каналів.

ТЕМА 5
ОРГАНІЗАЦІЯ ВНУТРІШНЬООБ'ЄКТНОГО ТА ПРОПУСКНОГО РЕЖИМУ НА ПІДПРИЄМСТВАХ, ЩО ПРАЦЮЮТЬ З ВІДОМОСТЯМИ, ВИЗНАЧЕНИМИ ДЕРЖАВНОЮ ТАЄМНИЦЕЮ

ПЛАН

1. Структура та повноваження режимно-секретних органів.

2. Внутрішньооб'єктовий режим та його задачі.

3. Підрозділи підприємства, які вирішують завдання з організації внутрішньооб'єктового режиму.

4. Організаційні засоби захисту інформації.

1. Структура та повноваження режимно-секретних органів

Режимно-секретні органи (далі – РСО) підпорядковуються безпосередньо керівнику державного органу, органу місцевого самоврядування, підприємства, установи, організації.

Створення, реорганізація чи ліквідація РСО здійснюються за погодженням із Службою безпеки України. До складу режимно-секретного органу входять *підрозділи режиму, секретного діловодства та інші підрозділи*, що безпосередньо забезпечують охорону державної таємниці. Вводиться посада *заступника керівника з питань режиму*, на якого покладаються обов'язки та права керівника РСО.

Якщо штатним розписом не передбачене створення РСО, та облік і зберігання секретних документів, а також заходи щодо забезпечення режиму секретності *здійснюються особисто їх керівниками або спеціально призначеним наказом керівника працівником* після створення необхідних умов, що забезпечують режим секретності. *Призначення осіб* на посади заступників керівників з питань режиму, начальників РСО та їх заступників здійснюється за погодженням з органами Служби безпеки України та РСО вищестоящих державних органів. *РСО комплектуються спеціалістами*, яким надано допуск до державної таємниці із ступенем секретності "*цілком таємно*", якщо характер

виконуваних робіт не потребує допуску до державної таємниці із ступенем *секретності "особливої важливості"*.

Основними завданнями РСО є:

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.

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 проектів 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 і організаціями та їх РСО з питань забезпечення режиму секретності;

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

2. Внутрішньооб'єктовий режим та його задачі

Внутрішньооб'єктовий і пропускний режими встановлюються на підприємствах, що працюють з відомостями, які становлять державну таємницю. Внутрішньооб'єктовий і пропускний режими є основнимі елементом системи захисту інформації підприємства. Організація внутрішньооб'єктового і пропускного режиму – *обов'язкова вимога нормативно-методичних документів* щодо захисту державної таємниці. *Внутрішньооб'єктовий і пропускний режими на підприємстві організовуються з метою виключення:*

– проникнення сторонніх осіб на територію, що охороняється, територію та об'єкти підприємства, а також у службові приміщення, в яких проводяться роботи з використанням відомостей, що становлять державну таємницю;

– відвідування режимних приміщень без службової необхідності співробітниками підприємства, які не мають до них прямого відношення, а також відрядженими особами, яким не надано право на їх відвідування (роботу в них);

– вносити (ввезення) на територію підприємства особистих технічних засобів (кіно-, фото-, відео-, звукозапису апаратури та інших технічних засобів);

– несанкціонованого виносу (вивозу) з території підприємства носіїв відомостей, що становлять державну таємницю;

– порушень встановленого регламенту службового часу, розпорядку роботи структурних підрозділів із захисту державної таємниці, а також встановленого порядку та режиму роботи співробітників підприємства і відряджених осіб з носіями відомостей, що становлять державну таємницю.

Режим секретності – це встановлений нормативними актами єдиний порядок забезпечення захисту відомостей, що становлять державну таємницю, включаючи систему адміністративно-правових, організаційних, інженерно-технічних та інших засобів. *Внутрішньооб'єктовий режим* – комплекс заходів, спрямованих на забезпечення встановленого режиму секретності безпосередньо в структурних підрозділах, на об'єктах і в службових приміщеннях підприємства.

Основними напрямками роботи по організації внутрішньооб'єктового режиму на підприємстві є:

– визначення загальних вимог режиму секретності на підприємстві відповідно до положень нормативних правових актів і вказівок вищих органів державної влади організацій);

– обмеження кола осіб, що допускаються до відомостей, що становлять державну таємницю, і їх носіям;

– регламентація безпосередньої роботи співробітників підприємства, а також відряджених осіб, з носіями відомостей, що становлять державну таємницю;

– планування комплексу заходів, спрямованих на виключення витоку відомостей, що становлять державну таємницю, і втрат носіїв цих відомостей; організація контролю з боку посадових осіб підприємства і структурних підрозділів із захисту державної таємниці за виконанням вимог по режиму секретності на підприємстві;

– організація роботи з персоналом підприємства, допущеним до відомостей, що становлять державну таємницю, а також з громадянами, які приймаються на роботу.

Завдання з організації внутрішньооб'єктового режиму на підприємстві покладаються на заступника керівника підприємства, який відповідає за питання захисту державної таємниці. Заступник керівника підприємства з роботи по формуванню системи внутрішньооб'єктового режиму *організовує на основі всебічного аналізу можливих каналів витоку відомостей, що становлять державну таємницю*, при проведенні підприємством всіх видів робіт.

Керівництво підприємства використовує такі основні підходи до організації внутрішньооб'єктового режиму:

– визначення відповідальності керівників підрозділів посадових осіб за захист державної таємниці;

– чітке розмежування функцій, покладених на відповідні структурні підрозділи підприємства (служба безпеки, режимно-секретний підрозділ, підрозділ протидії іноземним технічним розвідкам, служба охорони та ін.);

– створення ефективної системи контролю за виконанням заходів щодо режиму секретності і забезпечення збереження носіїв відомостей, що становлять державну таємницю.

Принципи формування системи внутрішньооб'єктового режиму:

– принцип персональної відповідальності;

– принцип комплексного використання наявних сил і засобів;

– принцип повного охоплення всіх напрямків діяльності підприємства.

Внутрішньооб'єктовий режим передбачає такі заходи:

– виявлення можливих каналів витоку відомостей, що становлять державну таємницю, і реалізація заходів, спрямованих на закриття цих каналів;

– віднесення відомостей до державної таємниці, засекречування та розсекречування відомостей та їх носіїв;

– ліцензування та сертифікація діяльності в області захисту інформації;

– підбір і вивчення кандидатур осіб для призначення на посади, що вимагають допуску до державної таємниці, оформлення необхідних документів;

– розподіл обов'язків в області захисту державної таємниці між посадовими особами і співробітниками підприємства;

– визначення кола посадових осіб, які мають право дозволяти ознайомлення (роботу) персоналу з відомостями, що становлять державну таємницю;

– створення структурних підрозділів, які вирішують завдання із захисту державної таємниці, і визначення їх функцій;

– надання співробітникам підприємства і відрядженим особам тільки того обсягу інформації, який необхідний їм для виконання їхніх посадових (функціональних) обов'язків;

– допуск і безпосередній доступ співробітників підприємства до відомостей, що становлять державну таємницю (їх носіям), обмеження кола осіб, що допускаються до цих відомостей;

– проведення роботи серед співробітників, допущених до державної таємниці, щодо роз'яснення вимог режиму секретності, підвищення пильності і персональної відповідальності за збереження довірених відомостей;

– облік, зберігання, розмноження, знищення носіїв відомостей, що становлять державну таємницю, встановлення режиму та порядку роботи співробітників підприємства з цими носіями відомостей;

– протидія іноземним технічним розвідкам і технічний захист інформації;

– організація підготовки, перепідготовки і підвищення кваліфікації співробітників підприємства, допущених до державної таємниці;

– організація та проведення нарад, в ході яких обговорюються питання, які містять відомості, що становлять державну таємницю;

– захист державної таємниці в ході співпраці підприємства з іноземними партнерами (фірмами), в тому числі при підготовці і проведенні прийому іноземних делегацій на підприємстві;

– захист державної таємниці при виконанні науково-дослідних, дослідно-конструкторських і інших видів спільних робіт, пов'язаних з передачею відомостей, що становлять державну таємницю, іншим підприємствам;

– фінансове, матеріально-технічне та інші види забезпечення захисту державної таємниці;

– виключення витоку відомостей, що становлять державну таємницю, в ході видавничої і рекламної діяльності підприємства;

– виділення і обладнання режимних приміщень, здійснення контролю доступу персоналу і відвідувачів в ці приміщення, виключення можливості безконтрольного доступу до них;

– проведення аналітичної роботи, вироблення на основі її результатів перспективних (прогнозних) оцінок стану справ в області захисту державної таємниці;

– визначення внутрішнього розпорядку та регламенту підприємства;

– контроль порядку використання технічних засобів передачі та обробки інформації, засобів розмноження, копіювання носіїв відомостей, що становлять державну таємницю, та інших технічних засобів і пристроїв;

– контроль ефективності вирішення завдань щодо захисту державної таємниці посадовими особами та структурними підрозділами підприємства;

– контроль наявності носіїв відомостей, що становлять державну таємницю.

В межах діяльності з організації внутрішньооб'єктового режиму керівник підприємства зобов'язаний:

– проявляти високу вимогливість до посадових осіб і співробітників підприємства, вживати заходів щодо недопущення розголошення відомостей, що становлять державну таємницю, втрат носіїв відомостей, застосовувати суворі стягнення з працівників підприємства, що допускають факти безвідповідальності і недбальства в роботі з відомостями, що становлять державну таємницю;

– оцінювати діяльність співробітників підприємства в області захисту державної таємниці;

– націлювати роботу посадових осіб і співробітників підприємства на суворе дотримання вимог режиму секретності.

В межах діяльності з організації внутрішньооб'єктового режиму заступник керівника підприємства виконує такі основні функції:

– безпосередньо керує розробкою організаційно-планових документів підприємства щодо захисту державної таємниці, організовує контроль за виконанням вимог, що містяться в них;

– максимально обмежує коло посадових осіб, що допускаються до відомостей, які становлять державну таємницю;

– особисто очолює роботу на підприємстві із захисту державної таємниці;

– організовує проведення систематичного аналізу діяльності структурних підрозділів та посадових осіб підприємства, спрямованої на забезпечення захисту державної таємниці;

– організовує і підтримує суворий порядок в розробці, обліку, зберіганні та знищенні носіїв відомостей, що становлять державну таємницю, і в поводженні з ними;

– організовує захист інформації при використанні засобів автоматизації;

– організовує підбір, розстановку і навчання співробітників структурних підрозділів із захисту державної таємниці;

– забезпечує необхідні умови для правильної організації режиму секретності, обліку, зберігання, знищення носіїв відомостей, що становлять державну таємницю, і поводження з ними;

– вживає заходів щодо захисту державної таємниці при взаємодії підприємства з іноземними партнерами;

– особисто інструктує членів комісій підприємства з перевірки наявності носіїв відомостей, що становлять державну таємницю, відбору та знищення носіїв, які втратили актуальність і практичне значення, а також які не потрібні в роботі.

3. Підрозділи підприємства, які вирішують завдання з організації внутрішньооб'єктового режиму

В організації внутрішньооб'єктового режиму беруть участь такі основні структурні підрозділи підприємства:

– режимно-секретний підрозділ;

– служба безпеки підприємства;

– підрозділ протидії іноземним технічним розвідкам;

– підрозділ охорони (в частині питань контролю внутрішніх об'єктів і службових приміщень підприємства).

Режимно-секретний підрозділ виконує такі основні завдання:

– розробка спільно з іншими підрозділами підприємства заходів щодо організації внутрішньооб'єктового режиму;

– підготовка пропозицій керівництву підприємства щодо обмеження кола осіб, які допускаються до конкретних відомостей, що становлять державну таємницю, і їх носіїв;

– організація та облік, забезпечення зберігання, своєчасне знищення носіїв відомостей, що становлять державну таємницю;

– контроль за порядком роботи співробітників підприємства з носіями відомостей, що становлять державну таємницю;

– участь у виробленні заходів із виключення витоку відомостей, що становлять державну таємницю, при взаємодії підприємства з іноземними підприємствами та організаціями, прийом іноземних делегацій;

– комплексний аналіз стану роботи на підприємстві із захисту державної таємниці, ефективності прийнятих посадовими особами та структурними підрозділами заходів;

– участь в розробці розгорнутих переліків відомостей, що підлягають засекречуванню, в роботі експертних комісій з розсекречування відомостей та їх носіїв;

– безпосередню участь в оформленні допуску до державної таємниці для співробітників підприємства, розробка номенклатури посад підприємства, що підлягають оформленню на допуск до відомостей, що становлять державну таємницю;

– організація та облік порушень вимог режиму секретності, аналіз причин цих порушень;

– координація діяльності структурних підрозділів підприємства в області захисту державної таємниці;

– участь у проведенні службових розслідувань у разі втрати або розкрадання носіїв відомостей, що становлять державну таємницю, за фактами розголошення таких відомостей;

– проведення інструктажу працівників підприємства, допущених до відомостей, що становлять державну таємницю, в тому числі що виїжджають за кордон, контроль рівня знань ними положень нормативних актів з питань режиму секретності;

– організація та облік обізнаності осіб у відомостях, що становлять державну таємницю;

– участь в організації та забезпеченні пропускного режиму і охорони підприємства та його об'єктів.

Співробітники режимно-секретного підрозділу мають право:

– вимагати від усіх співробітників підприємства дотримання режиму секретності;

– перевіряти стан режиму секретності в структурних підрозділах підприємства і підлеглих організаціях (філіях, представництвах);

– вимагати від співробітників підприємства письмових пояснень у разі розголошення відомостей, втрати носіїв відомостей або інших порушень режиму секретності;

– виробляти рекомендації керівникам структурних підрозділів підприємства з питань захисту державної таємниці;

– готувати керівнику підприємства мотивовані пропозиції про заборону ведення тих чи інших робіт у разі відсутності необхідних умов для забезпечення захисту державної таємниці або про притягнення до відповідальності працівників, які допустили порушення режиму таємності.

Служба безпеки створюється рішенням керівника на підприємствах, що виконують роботи одночасно з декількома видами конфіденційної інформації, в тому числі і з відомостями, що становлять державну таємницю.

Завдання служби безпеки підприємства в області організації внутрішньооб'єктового режиму:

– забезпечення економічної безпеки, охорони власності підприємства;

– організація конфіденційного діловодства, обліку, зберігання і знищення документів (матеріалів), що містять конфіденційну інформацію;

– захист конфіденційної інформації під час зовнішньоекономічної діяльності підприємства;

– контроль за виконанням вимог нормативно-методичних і внутрішніх організаційно-розпорядчих документів підприємства щодо забезпечення захисту інформації, що зберігається;

– виявлення і закриття можливих каналів витоку конфіденційної інформації;

– розробка системи організаційних і технічних заходів, що регламентують внутрішньооб'єктовий режим підприємства, і контроль за їх виконанням;

– контроль за порядком виготовлення, обліку, зберігання, використання бланків службових посвідчень, печаток, штампів підприємства, а також печаток з індивідуальними обліковими номерами;

– організація прийому і передачі інформації і відкритої кореспонденції з використанням різних технічних засобів зв'язку (телетайп, телефакс, електронна пошта тощо);

– розробка вимог до режимних приміщень, проведення їх атестації, організація установки і експлуатації технічних засобів захисту інформації;

– участь в експертизі матеріалів, призначених для відкритого опублікування;

– організація та проведення службових розслідувань за фактами порушень вимог, що стосуються захисту інформації, що охороняється, а також внутрішньооб'єктового режиму на підприємстві;

– взаємодія з правоохоронними та іншими державними органами з питань безпеки підприємства.

4. Організаційні засоби захисту інформації

Найефективніші заходи із захисту інформації:

– організація розробки, впровадження та використання різних засобів і систем захисту інформації;

– організація розробки, розмноження, обліку та знищення носіїв конфіденційної інформації з використанням технічних засобів;

– контроль за дотриманням персоналом підприємства встановлених вимог при використанні об’єктів інформатизації;

– аналіз ефективності функціонування технічних систем і засобів захисту інформації;

– розробка та впровадження в практику інструкцій та інших документів, що регламентують порядок і правила поводження з конфіденційною інформацією.

Співробітники, допущені до конфіденційної інформації, зобов’язані:

– знати порядок віднесення інформації до категорії конфіденційної, порядок засекречування відомостей, що становлять державну таємницю, а також положення чинного на підприємстві розгорнутого переліку відомостей, що підлягають засекречуванню;

– дотримуватися встановленого порядку роботи з відомостями конфіденційного характеру і їх носіями;

– суворо зберігати інформацію, що стала відома їм в силу виконання посадових (функціональних) обов’язків;

– вживати заходів щодо недопущення розголошення іншими співробітниками підприємства конфіденційної інформації, інформувати службу безпеки (режимно-секретного підрозділу) про можливі випадки порушення режиму секретності з боку інших осіб;

– знайомитися (працювати) тільки з тією конфіденційною інформацією (її носіями), до якої вони мають оформлений в установленому порядку допуск;

– знати ступінь секретності (конфіденційності) робіт (заходів), що проводяться, розроблених документів (матеріалів), дотримуватися встановлених правил роботи та поводження з цими документами (матеріалами).

Співробітники, допущені до конфіденційної інформації, зобов’язані:

– дотримуватися встановленого порядку прийому-передачі, зберігання носіїв конфіденційної інформації, не допускати безконтрольного користування ними;

– забезпечувати на своєму робочому місці таке розташування носіїв конфіденційної інформації, яке виключатиме несанкціоноване ознайомлення з

ними (їхнім змістом) сторонніх осіб, а також співробітників підприємства, які не мають до них безпосереднього відношення;

– в порядку, визначеному нормативними актами, забезпечувати облік носіїв конфіденційної інформації, а також нанесення на зазначені носії необхідних реквізитів;

– у визначеному керівником підприємства (структурного підрозділу) обсязі ознайомлювати співробітників свого підприємства і відряджених осіб з вмістом носіїв конфіденційної інформації, а також з тематикою і змістом проведених робіт;

– інформувати керівника підприємства і його заступника про дії сторонніх осіб, представників інших підприємств, іноземних громадян про спроби отримання конфіденційної інформації;

– питання виїзду за кордон у службові відрядження, у приватних справах і з іншими цілями вирішувати відповідно до нормативних актів і вказівок органу державної влади керівника підприємства.

Співробітникам, допущеним до конфіденційної інформації, забороняється:

– порушувати встановлений порядок поводження з носіями конфіденційної інформації;

– виконувати роботи з носіями конфіденційної інформації поза службовими приміщеннями і робочими місцями;

– повідомляти відомості конфіденційного характеру співробітникам підприємства, які не мають до них безпосереднього відношення, і стороннім особам;

– виконувати записи конфіденційного характеру на носіях, що спеціально для цього не призначенні;

– повідомляти конфіденційні відомості за допомогою відкритих засобів зв’язку (телефон, факс, мобільний зв’язок, електронна пошта і т.п.);

– зберігати носії конфіденційної інформації на столах, відкритих стелажах, в незамкнених сховищах, шафах, сейфах, залишати не замкненими службові кабінети, в яких зберігаються носії конфіденційної інформації;

– накопичувати відомості конфіденційного характеру на своєму робочому місці, на відкритих носіях (в тому числі в електронному вигляді), у відкритих матеріалах.

Вимоги до приміщень режиму секретності:

– вхідні двері обладнуються замками, що гарантують надійне закривання приміщень в неробочий час, в них також можуть встановлюватися кодові і електронні замки і автоматичні турнікети;

– режимні приміщення, в яких у неробочий час зберігаються носії конфіденційної інформації, оснащуються охоронною сигналізацією, зв'язаною з вартовим приміщенням, пультом централізованого спостереження за сигналізацією служби охорони і з черговим по підприємству;

– режимні приміщення, в яких є технічні засоби, розробляються, випробовуються або експлуатуються спеціальні вироби, мають охоронювані характеристики, обладнуються відповідно до вимог з протидії іноземним технічним розвідкам та технічного захисту інформації.

Режимні приміщення є важливою складовою системи захисту інформації з обмеженим доступом, тому до їх облаштування та експлуатації висуваються підвищені вимоги. Такі приміщення обов'язково *обстежуються спеціально створеною комісією* з метою визначення їх відповідності встановленим нормам і вимогам щодо безпеки, технічного захисту інформації та дотримання режиму секретності.

За результатами перевірки комісія *оформлює акт придатності приміщення*, у якому зазначаються види робіт, що можуть проводитися у ньому, а також виявлені недоліки та рекомендації щодо їх усунення. Лише після позитивної атестації приміщення може бути допущене до роботи з носіями секретної або конфіденційної інформації.

Обстеження та атестація режимних приміщень здійснюються *не рідше одного разу на п'ять років*, а також *після проведення ремонту, реконструкції, переобладнання чи зміни їх функціонального призначення*. Такий підхід дозволяє забезпечити постійний контроль за станом технічного захисту і гарантувати дотримання вимог безпеки на всіх етапах експлуатації.

Для забезпечення *контрольованого прийому та видачі носіїв конфіденційної інформації* у режимних приміщеннях облаштовуються спеціальні вікна, які не виходять у загальний коридор або інші приміщення загального користування. За необхідності у робочій кімнаті виділяється окрема ізольована частина, відмежована фізичним бар'єром, що забезпечує неможливість несанкціонованого доступу сторонніх осіб.

Дотримання таких вимог створює умови для ефективного функціонування режиму секретності, мінімізації ризиків витоку інформації та підвищення загального рівня безпеки на об'єктах, де здійснюється робота з інформацією, що становить державну або службову таємницю.

Приміщення забезпечуються необхідною кількістю сховищ, замки яких обладнуються *пристосуваннями для опечатування*. Сховища і ключі від сховищ зберігаються і обліковуються в службі безпеки. Сховища, а також вхідні двері приміщень, в яких вони зоблаштовані, обладнані замками з двома примірниками ключів. У неробочий час ключі від сховищ і від вхідних дверей режимних приміщень, зберігаються в окремих пеналах, опечатаних черговим зі служби безпеки (режимно-секретного підрозділу), передаються на зберігання службі охорони або черговому по підприємству. Після закінчення робочого дня всі сховища і режимні приміщення закривають і опечатують. Сховища і вхідні двері приміщень, в яких вони облаштовані, опечатують різними печатками.

Порядок прийому-здачі під охорону режимних приміщень визначається *інструкцією, що спеціально розробляється службою безпеки* (режимно-секретним підрозділом) і затверджується керівником підприємства. Здачу під охорону і відкриття приміщень здійснюють відповідальні за ці приміщення співробітники підприємства на підставі затверджених керівником підприємства списків цих співробітників *із зразками їхніх підписів*. Списки знаходяться в службі охорони або у чергового по підприємству. Співробітники підприємства, яким надано право на відкривання, здачу під охорону та опечатування приміщень, відповідають за дотримання в цих приміщеннях встановлених вимог режиму секретності.

СЕМІНАРСЬКЕ ЗАНЯТТЯ
ТЕМА 5
ОРГАНІЗАЦІЯ ВНУТРІШНЬООБ'ЄКТОВОГО ТА ПРОПУСКНОГО РЕЖИМУ НА ПІДПРИЄМСТВАХ, ЩО ПРАЦЮЮТЬ З ВІДОМОСТЯМИ, ВИЗНАЧЕНИМИ ДЕРЖАВНОЮ ТАЄМНИЦЕЮ

План семінарського заняття

1. Структура та повноваження режимно-секретних органів.

2. Внутрішньооб'єктовий режим та його задачі.

3. Підрозділи підприємства, які вирішують завдання з організації внутрішньооб'єктового режиму.

4. Організаційні засоби захисту інформації.

Ключові поняття та терміни: режимно-секретний орган, внутрішньооб'єктовий режим, пропускний режим, перепустка, ідентифікація, автентифікація, контроль доступу, секретне діловодство, охорона об'єкта, обмежена зона, матеріальні носії інформації, організаційні заходи захисту, режим конфіденційності, технічні засоби охорони, відповідальність за порушення режиму.

Завдання для самостійної роботи над темою

Завдання 1. Опрацювати теоретичний матеріал теми 5 дистанційного курсу "Система охорони державної таємниці" у Віртуальному університеті ЛДУ БЖД.

Завдання 2. Користуючись рекомендованою літературою та теоретичним матеріалом лекції, самостійно опрацювати та розв'язати ситуаційні завдання.

Ситуаційне завдання 1. На підприємстві виявлено відсутність перепустки у співробітника, який працює з документами з грифом "Таємно". Запропонуйте алгоритм дій режимно-секретного органу та охорони.

Ситуаційне завдання 2. На об’єкті спостерігається збій у роботі системи відеоспостереження, через що порушується контроль за доступом сторонніх осіб. Визначте, яких організаційних та технічних заходів слід вжити негайно.

Ситуаційне завдання 3. До приміщення із секретними матеріалами намагався потрапити сторонній працівник, мотивуючи це необхідністю технічного ремонту обладнання. Як має діяти черговий по об’єкта та які документи перевірити?

Ситуаційне завдання 4. Виявлено факт винесення співробітником робочих матеріалів без належного оформлення перепустки на винос. Розробіть схему реагування підприємства та заходи із запобігання повторним випадкам.

Завдання 3. Користуючись рекомендованою літературою та теоретичним матеріалом лекції, підготувати аргументи для обговорення дискусійних тем.

Дискусійні теми:

– Чи можна забезпечити ефективний пропускний режим лише технічними засобами без участі людини?

– Наскільки внутрішньооб’єктовий режим впливає на продуктивність працівників і чи не створює він надмірних обмежень?

– Які виклики сьогодні виникають у зв’язку з цифровізацією процесів і чи достатньо традиційних методів режимно-секретного захисту?

ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ

1. Яка мета створення режимно-секретних органів (РСО)?
2. Які підрозділи входять до складу режимно-секретного органу?
3. За яких умов вводиться посада заступника керівника з питань режиму?
4. Які органи погоджують призначення осіб на посади заступників керівників з питань режиму, начальників РСО та їх заступників?
5. За якими критеріями обираються спеціалісти до РСО із різними ступенями секретності допуску до державної таємниці?
6. Які основні завдання РСО.
7. Назвіть права РСО (3 доповіді).
8. Що являють собою внутрішньооб'єктовий і пропускний режими?
9. З якою метою на підприємстві організовують внутрішньооб'єктовий і пропускний режими?
10. Що таке режим секретності?
11. Назвіть основні напрями роботи з організації внутрішньооб'єктового режиму на підприємстві.
12. Перерахуйте завдання з організації внутрішньооб'єктового режиму.
13. Окресліть основні підходи до організації внутрішньооб'єктового режиму.
14. Назвіть основні принципи формування системи внутрішньооб'єктового режиму.
15. Які заходи передбачає внутрішньооб'єктовий режим? (3 доповіді).
16. Яку роль в організації внутрішньооб'єктового режиму відіграють керівник підприємства і його заступник?
17. Назвіть обов'язки керівника підприємства.
18. Які функції в організації внутрішньооб'єктового режиму виконує заступник керівника підприємства?
19. Які структурні підрозділи підприємства беруть участь в організації внутрішньооб'єктового режиму?
20. Які основні завдання в організації внутрішньооб'єктового режиму виконує режимно-секретний підрозділ? (2 доповіді).

21. Назвіть права співробітників режимно-секретного підрозділу при вирішенні покладених на них завдань.
22. Яку роль в організації внутрішньооб'єктового режиму на підприємстві відіграє служба безпеки?
23. Які завдання служби безпеки підприємства в області організації внутрішньооб'єктового режиму за умови, що в структурі підприємства діє самостійний режимно-секретний підрозділ?
24. Що розуміють під організаційними засобами захисту інформації?
25. Які заходи щодо захисту інформації є найефективнішими?
26. Які обов'язки співробітників, допущених до конфіденційної інформації? (2 доповіді).
27. Що забороняється співробітникам, допущеним до конфіденційної інформації?
28. Які вимоги висуваються до приміщень, призначених для робіт з використанням відомостей, що становлять державну таємницю, або для зберігання їх носіїв?
29. Опишіть процедуру обстеження режимних приміщень перед початком експлуатації.
30. Опишіть процедуру прийому і видачі носіїв конфіденційної інформації у режимних приміщеннях.
31. Опишіть умови зберігання носіїв конфіденційної інформації у режимних приміщеннях.
32. Опишіть процес здачі під охорону режимних приміщень, в яких зберігаються носії конфіденційної інформації.
33. Які дії при виявленні можливого проникнення в режимні приміщення або сховища сторонніх осіб?

Рекомендована література: [1-3, 5, 7, 14, 21, 24-25].

ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ

1. Що є основним завданням режимно-секретних органів (РСО)?
    а) Забезпечення режиму секретності.
    б) Контроль за виробничими процесами.
    в) Видача дозволів на доступ до підприємства.
    г) Організація фінансових перевірок.

2. Хто здійснює контроль за створенням, реорганізацією та ліквідацією РСО?
    а) Служба безпеки України.
    б) Міністерство внутрішніх справ.
    в) Органи місцевого самоврядування.
    г) Прокуратура України.

3. Який орган на підприємстві відповідає за забезпечення охорони державної таємниці?
    а) Режимно-секретний орган.
    б) Відділ кадрів.
    в) Фінансовий відділ.
    г) Господарський департамент.

4. Хто має право бути призначеним на посаду керівника РСО?
    а) Особи, які мають допуск до державної таємниці.
    б) Будь-який співробітник підприємства.
    в) Працівник бухгалтерії.
    г) Лише керівник підприємства.

5. Які основні завдання виконує РСО?
    а) Недопущення необґрунтованого доступу до секретної інформації.
    б) Організація харчування працівників.
    в) Контроль за виплатою заробітної плати.
    г) Проведення технічного обслуговування офісів.

6. Хто погоджує призначення начальника РСО?
    а) Служба безпеки України.
    б) Міністерство освіти України.
    в) Державна фіскальна служба.
    г) Верховна Рада.

7. Що включає внутрішньооб’єктовий режим?
    а) Комплекс заходів із забезпечення секретності на підприємстві.
    б) Правила трудової дисципліни.
    в) План евакуації у разі надзвичайної ситуації.
    г) Організацію робочих місць.

8. Яка основна мета пропускного режиму?
    а) Запобігання проникненню сторонніх осіб.
    б) Ведення кадрового обліку.
    в) Регулювання часу обідніх перерв.
    г) Організація корпоративних заходів.

9. Що забороняється проносити на територію підприємства з обмеженим доступом?
    а) Кіно-, фото-, відео-, звукозаписувальну апаратуру.
    б) Особисті блокноти.
    в) Книги та журнали.
    г) Канцелярські предмети.

10. Які заходи передбачає режим секретності?
    а) Організаційні, адміністративно-правові та технічні.
    б) Лише фізичний контроль доступу.
    в) Виключно відеоспостереження.
    г) Використання пропусків для співробітників.

11. Що передбачає функціонування режимних приміщень?

а) Обмеження доступу до секретної інформації.

б) Вільний доступ для всіх працівників.

в) Використання для відпочинку персоналу.

г) Організацію культурних заходів.

12. Хто відповідає за дотримання пропускного режиму на підприємстві?

а) Підрозділ охорони.

б) Відділ кадрів.

в) Юридичний відділ.

г) Господарський департамент.

13. Яке основне завдання внутрішньооб’єктового режиму?

а) Запобігання витоку інформації.

б) Контроль за робочим часом.

в) Організація харчування працівників.

г) Видача сертифікатів якості.

14. Хто має право перевіряти виконання заходів щодо захисту державної таємниці?

а) Режимно-секретний орган.

б) Будь-який співробітник.

в) Громадські організації.

г) Виробничий відділ.

15. Яке з цих тверджень є правильним щодо організації роботи РСО?

а) РСО підпорядковується керівнику підприємства.

б) РСО керується наказами відділу кадрів.

в) РСО займається тільки фінансовими перевірками.

г) РСО відповідає за постачання канцелярських товарів.

16. Що має забезпечувати режимно-секретний підрозділ?
    а) Контроль за доступом до секретної інформації.
    б) Охорону будівлі.
    в) Надання фінансових консультацій.
    г) Видачу перепусток.

17. Яка відповідальність покладається на керівника підприємства у сфері внутрішньооб’єктового режиму?
    а) Забезпечення режиму секретності.
    б) Призначення співробітників на посади.
    в) Контроль виробничих процесів.
    г) Організація дозвілля працівників.

18. Як відбувається контроль за виконанням заходів внутрішньооб’єктового режиму?
    а) Шляхом регулярних перевірок і службових розслідувань.
    б) Через щорічні звіти.
    в) Безперервне відеоспостереження у всіх приміщеннях.
    г) Відсутність будь-якого контролю.

ТЕМА 6
ВЕДЕННЯ ДОКУМЕНТІВ З ГРИФОМ “ТАЄМНО”

ПЛАН

1. Ведення документів з грифом секретності.

2. Складання номенклатури секретних справ. Формування, облік, зберігання та видача секретних справ.

1. Ведення документів з грифом секретності

Відповідно до Закону “Про інформацію” вона поділяється на відкриту інформацію та інформацію з обмеженим доступом. Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну (ст. 30).

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних та юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Таємна інформація – це інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю (банківську, комерційну, службову, професійну, адвокатську тощо), розголошення якої завдає шкоди особі, суспільству і державі).

Державна таємниця – 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 такою (державною таємницею) у порядку, встановленому Законом України “Про державну таємницю” і підлягають охороні державою.

Державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики визначає Верховна Рада України. Єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передачі та транспортування матеріальних носіїв секретної інформації встановлюються Кабінетом Міністрів України.

Порядок обліку, одержання, використання, поширення, зберігання та знищення документів, справ, видань, магнітних та інших матеріальних носіїв інформації, які містять інформацію з грифом.

Для службового користування, що є власністю держави – установлює Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, затвердженою Постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893.

Переліки відомостей, які містять конфіденційну інформацію і яким надається гриф обмеженого доступу "Для службового користування" розробляється експертними комісіями згідно з орієнтованими критеріями віднесення інформації до конфіденційної інформації, що є власністю держави.

Інформація вважається такою, що належить до категорії конфіденційної, з моменту прийняття рішення про це її власником чи уповноваженою ним особою. Володіння, користування або розпорядження інформацією на законних підставах особою, яка не є власником такої інформації, не дає їй права встановлювати або змінювати режим доступу до цієї інформації, якщо зазначена особа окремо не уповноважена на це власником інформації.

Обмеження доступу до інформації, що належить до категорії конфіденційної, вважаються такими, що зняті:

– з наступного дня після закінчення терміну дії обмеження доступу до інформації, що визначений власником такої інформації;

– з моменту прийняття відповідного рішення власником такої інформації;

– з моменту оприлюднення за згодою власника;

– з моменту надходження інформації до загальнодоступних баз даних за згодою її власника.

Не може бути віднесена до категорії конфіденційної:

– інформація, приховування якої загрожує безпеці, життю та здоров'ю людей;

– інформація про стан довкілля, екологічної безпеки та захворюваності населення, якість харчових продуктів та предметів побуту, життєвий рівень

населення, медичне обслуговування та соціальне забезпечення, соціально-демографічні показники, стан освіти та культури, стан правопорядку;

– інформація про злочини та інші правопорушення, неправомірні дії органів державної влади, органів місцевого самоврядування та посадових осіб;

– інформація, яка відповідно до законів України та міжнародних договорів України не може бути віднесена до конфіденційної.

На документах у правому верхньому куті першої сторінки, а для видань – на обкладинці та на титулі, проставляють гриф “Для службового користування” і номер примірника. Керівники організацій несуть відповідальність за забезпечення правильного ведення обліку, зберігання та використання документів з грифом “Для службового користування” Облік, зберігання, розмноження та використання документів з грифом “Для службового користування”, а також контроль за дотриманням Постанови Кабінету Міністрів в України від 27 листопада 1998 р № 1853 покладається на управління справами, загальні відділи, канцелярії організацій. Запобігання розголошенню відомостей, що містяться в документах з грифом “Для службового користування”, та випадкам втрат таких документів покладається на режимно-секретні підрозділи організацій.

Служба безпеки України здійснює контроль за обігом документів, які містять конфіденційну інформацію, що є власністю держави.

Виконавці, які працюють з документами з грифом “Для службового користування”, обов’язково ознайомлюються під розписку із Інструкцією про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави.

Секретне діловодство в установах організовується та ведеться режимно-секретним органом. Обліку підлягають усі рукописні, машинописні, підготовлені з використанням засобів обчислювальної техніки секретні документи, робочі зошити для ведення записів, що містять секретну інформацію, машинні та інші матеріальні носії секретної інформації, робочі папки.

Облік секретних документів ведеться у журнальній або у картковій формах. Секретні документи справи, а також інші матеріальні носії секретної інформації видаються виконавцям безпосередньо режимно-секретним органом за підписом в картці обліку видачі документа (справи) (показати картку) і підлягають поверненню того самого дня.

Реєстраційний номер секретним документам за кожним видом обліку надається один раз. Під реєстрацією секретних документів, інших матеріальних носіїв секретної інформації розуміється надання ім реєстраційних номерів шляхом нанесення на них умовного позначення з подальшим записом відомостей про ці документи або інші матеріальні носії секретної інформації у журналах чи картках обліку за відповідною формою.

Гриф обмеження доступу – реквізит матеріального носія інформації з обмеженим доступом, який вказує на обмеження доступу до зазначеної інформації, а також відповідає категорії та виду інформації, яку зафіксовано на конкретному матеріальному носієві.

Реєстрація (облік) документів, що мають гриф секретності, поділяється на такі види:

– попередній облік;

– облік підготовлених (вихідних) секретних документів;

– облік пакетів;

– облік вхідних секретних документів;

– облік секретних документів виділеного зберігання (інвентарний облік).

Реєстрація (облік) підготовлених вихідних документів охоплює всі друковані (в тому числі виготовлені за допомогою автоматизованої системи) та рукописні документи, які пройшли реєстрацію за журналами (картками) попереднього обліку.

Реєстрація (облік) пакетів з грифом секретності охоплює всі одержані установою та зареєстровані у пакетно-контрольному журналі пакети та документи. Реєстрація (облік) вхідних документів з грифом секретності охоплює одержані установою документи, які пройшли журнальний (картковий, автоматизований) облік вхідних документів. Реєстрація (облік) документів

інвентарного обліку охоплює всі документи, які не підлягають підшиванню до справ, переведені з інших видів обліку або такі, яким надано номер за журналом інвентарного обліку технічних документів, журналом обліку секретних видань, журналом інвентарного обліку письмових зброшурованих матеріалів в момент їх створення (заведення) або надходження (після реєстрації в пакетно-контрольному журналі).

Гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності цієї інформації. Ступінь секретності (“особливої важливості”, “цілком таємно”, “таємно”) – категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою.

Форми реєстрації (обліку) документів, які ведуть протягом календарного року і по закінченні його роблять підсумковий запис про кількість взятих на облік документів:

– пакетно-контрольний журнал;

– журнал (картка) обліку підготовлених документів;

– журнал (картка) обліку вхідних документів з грифом секретності;

– журнал обліку документів, надрукованих у друкарському підрозділі;

– журнал обліку вхідних, надрукованих вихідних і інвентарних документів;

– журнал обліку розпорядчих документів;

– журнал обліку видачі працівникам довідок про допуск;

– журнал обліку осіб, які прибули у відрядження.

У формах реєстрації (обліку) документів з грифом секретності заборонено робити підчищення та виправлення із застосуванням засобів типу коректуючої рідини. Кожне виправлення, внесене працівником режимно-секретного органу засвідчується його підписом із зазначенням дати та скріплюється печаткою режимно-секретного органу.

На документах у правому верхньому куті першої сторінки, а для видань – на обкладинці та на титулі, проставляють гриф “Для службового користування” і номер примірника.

Відповідно до Закону “Про інформацію” вона поділяється на відкриту інформацію та інформацію з обмеженим доступом. Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну (ст. 30).

Конфіденційна інформація – це відомості, якими володіють, користуються або розпоряджаються окремі фізичні та юридичні особи і поширюють їх за бажанням, відповідно до передбачених ними умов. *Захист секретної інформації в автоматизованій системі забезпечується шляхом:*

– атестації засобів обчислювальної техніки, програмного забезпечення, засобів зв’язку і автоматизованої системи в цілому;

– дотримання норм, вимог та правил організаційного і технічного характеру;

– здійснення контролю.

Рекомендований алгоритм обстеження містить такі процедури:

– аналіз потоків секретної інформації у технічних засобах;

– визначення складу основних і допоміжних технічних засобів та систем на об’єкті;

– визначення складу кабельних ліній, що виходять за межі контрольованої території і мають паралельний пробіг з кабелями автоматизованої системи;

– виявлення комунікацій, що проходять через територію об`єкта і мають вихід за межі контрольованої території;

– інструментальне вимірювання інформативних побічних електромагнітних випромінювань та наводок;

– оцінка відповідності рівнів сигналів і параметрів полів, які є носіями інформації з обмеженим доступом, норм ефективності захисту.

Оброблення секретної інформації в автоматизованій системі дозволяється тільки після завершення робіт із створення комплексної системи захисту інформації, проведення випробувань та оцінки рівня захищеності інформації на відповідність до вимог нормативних документів системи технічного захисту інформації, за результатами якої надається атестат відповідності.

Атестат засвідчує наявність в автоматизованій системі необхідних умов для обробки інформації відповідно до грифа секретності та достатність вжитих заходів.

Дозвіл на експлуатацію автоматизованої системи надається наказом керівника установи на підставі атестата відповідності.

2. Складання номенклатури секретних справ. Формування, облік, зберігання та видача секретних справ

З метою *правильного формування справ, забезпечення їх систематизації, надійного зберігання документів та оперативного їх пошуку в установах розробляється номенклатура справ*. Вона є основним обліковим документом діловодної служби, що відображає структуру установи, напрями її діяльності та функції окремих структурних підрозділів.

Номенклатура справ визначає перелік усіх документів, які створюються в процесі роботи установи, та встановлює *єдину систему їх індексації, оформлення, зберігання і передачі в архів*. Вона формується на підставі положення про установу, її структурних підрозділів, штатного розпису, посадових інструкцій, а також аналізу видів документів, що виникають у результаті виконання основних і допоміжних функцій.

Під час розроблення номенклатури обов'язково враховуються *завдання, функції та компетенція установи*, щоб забезпечити повноту відображення її діяльності у документаційних масивах. Кожна справа вноситься до номенклатури з коротким описом змісту, зазначенням структурного підрозділу – відповідального за її ведення, а також із вказівкою *терміну зберігання документів.*

Основним нормативним документом при визначенні термінів зберігання та відбору документів на державне зберігання є "*Перелік типових документів, що утворюються в діяльності органів державної влади та місцевого самоврядування, інших установ, організацій і підприємств, із зазначенням термінів зберігання документів*". Цей Перелік встановлює *єдині правила зберігання, добору, експертизи цінності та передавання документів до*

державних архівів, а також забезпечує уніфікацію підходів до організації діловодства в різних установах.

Дотримання вимог щодо розроблення та ведення номенклатури справ гарантує *збереження документів, що мають юридичне, наукове, історичне або практичне значення*, полегшує роботу з інформацією, забезпечує швидкий доступ до потрібних матеріалів і створює необхідні умови для ефективного управління документами в установі.

Номенклатура справ є обов'язковим для кожного РСО документом, який складається для створення єдиної системи формування справ, забезпечення їх обліку, швидкого розшуку за його змістом та видом, відбору документів на державне зберігання у процесі діловодства. Номенклатура є основним обліковим документом секретних справ календарного року та підставою для їх обліку.

Є три види номенклатур справ: типова, примірна та індивідуальна.

Типова номенклатура справ встановлює типовий склад справ для режимно-секретного органу однорідних за характером діяльності, з єдиною системою індексації і є нормативним актом.

Примірна номенклатура справ встановлює примірний склад справ для режимно-секретного органу, що однорідні за характером діяльності, але різних за структурою, і має рекомендаційний характер.

Незалежно від наявності типової чи примірної номенклатури справ кожен режимно-секретний орган повинен мати індивідуальну номенклатуру справ.

Кожна справа, включена до номенклатури справ, повинна мати умовне позначення (арабськими цифрами) – індекс. Індекс справ структурного підрозділу складається з індексу структурного підрозділу (за штатним розписом) та порядкового номера справи в межах підрозділу.

До номенклатури справ не включаються друковані видання, брошури, довідники, бюлетені, реферативні журнали, експрес-інформація тощо.

Номенклатура справ підлягає перепогодженню з відповідним державним архівним підрозділом один раз на п'ять років або у разі змін у структурі, функціях та характері роботи РСО.

Формування справ – це групування виконаних документів у справи відповідно до номенклатури справ.

Під час формування справ слід дотримуватися таких правил:

– групувати у справи тільки оригінали (у разі їх відсутності – засвідчені в установленому порядку копії) правильно оформлених і виконаних документів, не допускати включення до справ чорнових, особистих, дублетних документів, документів, що підлягають поверненню, та розмножених копій;

– групувати у справи документи одного діловодного року (за винятком перехідних справ); групувати у справи окремо документи постійного і тимчасового строків зберігання.

Справи, передбачені номенклатурою справ, заводять за такими ознаками:

– предметно-показниковою або тематичною, коли документи групують у справи за їх змістом, тобто відносяться до одного й того ж питання чи до однієї й тієї ж теми;

– номінальною (за видами документів: накази, звіти, протоколи, акти тощо);

– кореспондентською, коли у справи об'єднуються документи з листування з однією чи кількома установами, та за іншими ознаками.

Приблизна пам`ятка виконавцю про користування справою:

1. При одержанні справи перевірити кількість аркушів у справі.

2. Під час бесіди із сторонньою людиною закрити справу і перевернути її титульною стороною донизу.

3. Своєчасно повернути справу до РСО.

4. При поверненні справи переконайтеся у тому, що справу з вас списано.

ЗАБОРОНЕНО:

а) розшивати справу;

б) вилучати із справи документи і окремі аркуші;

в) підшивати до справи документи і аркуші;

г) передавати справу іншому працівнику без відома РСО;

д) залишати справу на робочому місці.

Всі закінчені справи обліковуються у журналі обліку журналів, карток і завершених виробництвом справ. Цей журнал є основним обліковим документом справ, карток та журналів і включається до номенклатури справ.

СЕМІНАРСЬКЕ ЗАНЯТТЯ
ТЕМА 6
ВЕДЕННЯ ДОКУМЕНТІВ З ГРИФОМ ТАЄМНО

План семінарського заняття

1. Ведення документів з грифом секретності.

2. Складання номенклатури секретних справ. Формування, облік, зберігання та видача секретних справ.

Ключові поняття та терміни: гриф секретності, документ з обмеженим доступом, номенклатура секретних справ, секретне діловодство, облік секретних документів, формування справ, зберігання секретних документів, видача секретних справ, контроль доступу, журнал обліку, режимно-секретний орган, розсекречування, знищення секретних документів, відповідальність за порушення режиму.

Завдання для самостійної роботи над темою

Завдання 1. Опрацювати теоретичний матеріал теми 6 дистанційного курсу “Система охорони державної таємниці” у Віртуальному університеті ЛДУ БЖД.

Завдання 2. Користуючись рекомендованою літературою та теоретичним матеріалом лекції, самостійно опрацювати та розв’язати ситуаційні завдання.

Ситуаційне завдання 1. У журналі обліку секретних документів виявлено відсутність підпису отримувача під час видачі справи. Визначте дії режимно-секретного органу та відповідальність працівника.

Ситуаційне завдання 2. Працівник помилково відніс документ з грифом “Таємно” до загальної номенклатури справ. Як виправити ситуацію та які ризики це створює?

Ситуаційне завдання 3. На підприємстві під час перевірки з’ясувалося, що частина секретних документів зберігається у шафі без спеціального замка. Запропонуйте план усунення порушення.

Ситуаційне завдання 4. Документ з грифом “Цілком таємно” втратив свій фізичний носій (зник аркуш). Які першочергові дії необхідно вжити, і хто має бути повідомлений?

Ситуаційне завдання 5. До секретного відділу установи надійшов документ з позначкою «Для службового користування» (ДСК). Під час аналізу змісту виявлено, що він містить відомості, які згідно з Зводом відомостей, що становлять державну таємницю, підлягають грифу «Таємно». Завдання: Визначте, які дії має вжити відповідальний за секретне діловодство. Поясніть, які ризики виникають у разі залишення документа з неправильним грифом. Обґрунтуйте, яким чином здійснюється процедура зміни грифа секретності.

Ситуаційне завдання 6. Працівник державної установи отримав електронний лист з вкладенням – документом, що має гриф «Таємно». Для зручності він переслав цей лист на свою особисту електронну пошту, щоб відкрити його вдома. Завдання: Визначте, які порушення режиму секретності були допущені. Вкажіть, які дисциплінарні або кримінальні наслідки може мати така дія. Запропонуйте правильний алгоритм роботи з електронними секретними документами.

Ситуаційне завдання 7. Під час планової ревізії секретного архіву виявлено справу з грифом «Таємно», термін зберігання якої минув. Співробітник відділу вирішив самостійно знищити документи, не склавши відповідного акта. Завдання: Опишіть, які процедури знищення секретних документів передбачає нормативно-правова база України. Поясніть, чому самовільне знищення матеріалів є порушенням режиму секретності. Розробіть правильну послідовність дій для законного вилучення та знищення таких документів.

Завдання 3. Користуючись рекомендованою літературою та теоретичним матеріалом лекції, підготувати аргументи для обговорення дискусійних тем.

Дискусійні теми:

– Чи можна в умовах цифровізації замінити паперове секретне діловодство електронними системами без ризику для безпеки?

– Наскільки номенклатура секретних справ обмежує оперативність управлінських рішень?

– Чи завжди жорсткі правила зберігання документів з грифом “Таємно” є виправданими в умовах сучасних загроз?

ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ СТУДЕНТІВ

1. Хто відповідає за ведення документів з грифом секретності на підприємстві?
2. Які основні вимоги пред’являються до ведення документів з грифом секретності?
3. Що таке номенклатура секретних справ і для чого вона призначена?
4. Хто затверджує номенклатуру секретних справ на підприємстві?
5. Які розділи має містити номенклатура секретних справ?
6. Як часто переглядається та оновлюється номенклатура секретних справ?
7. Які правила формування секретних справ?
8. Як здійснюється облік секретних справ?
9. Де зберігаються секретні справи на підприємстві?
10. Хто має право видавати секретні справи для роботи?
11. Як оформлюється видача секретних справ для роботи?
12. Які заходи безпеки вживаються при роботі з секретними справами?
13. Як повертаються секретні справи після роботи?
14. Що робити у разі втрати або пошкодження секретної справи?
15. Які вимоги пред’являються до знищення секретних справ?
16. Які типові порушення виникають під час оформлення документів з грифом секретності, і як вони можуть призвести до витоку конфіденційної інформації?
17. Як впровадження електронного документообігу впливає на вимоги щодо оброблення, зберігання та контролю доступу до секретних документів?
18. У чому полягає різниця між позначенням «таємно», «цілком таємно» та «особливої важливості», і як ці рівні впливають на порядок роботи з документами?
19. Які принципи слід враховувати при складанні номенклатури секретних справ, щоб забезпечити її відповідність як правовим, так і практичним вимогам безпеки?
20. Як здійснюється облік і контроль руху секретних справ у сучасних установах, що використовують автоматизовані системи управління документами?
21. Які ризики виникають при передачі або видачі секретних справ між підрозділами, і які заходи необхідно впровадити для мінімізації цих ризиків?

Рекомендована література: [1-3, 5, 7, 14, 21, 24-25].

ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ

1. Що таке конфіденційна інформація?
   а) Відомості, які знаходяться у володінні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням.
   б) Інформація, що містить державну таємницю.
   в) Дані, що підлягають обов'язковому розголошенню.
   г) Відомості, доступ до яких є відкритим для всіх громадян.

2. Що таке таємна інформація?
   а) Інформація, що містить відомості, які становлять державну або іншу передбачену законом таємницю.
   б) Відомості, які можна вільно поширювати.
   в) Дані, що розміщені у відкритих державних реєстрах.
   г) Інформація, що стосується лише комерційних компаній.

3. Що встановлює порядок обліку та використання документів з грифом "Для службового користування"?
   а) Інструкція про порядок обліку, зберігання і використання документів, що містять конфіденційну інформацію.
   б) Закон України "Про доступ до публічної інформації".
   в) Адміністративний кодекс України.
   г) Державний стандарт України.

4. Що є державною таємницею?
   а) Відомості у сфері оборони, економіки, науки, техніки, зовнішніх відносин, державної безпеки та охорони правопорядку.
   б) Дані про погодні умови.
   в) Інформація про демографічні показники населення.
   г) Відомості про спортивні заходи.

5. Який нормативний документ регулює питання державної таємниці?
   а) Закон України “Про державну таємницю”.
   б) Закон України “Про інформацію”.
   в) Кримінальний кодекс України.
   г) Конституція України.

6. Хто визначає державну політику щодо державної таємниці?
   а) Верховна Рада України.
   б) Служба безпеки України.
   в) Міністерство внутрішніх справ.
   г) Міністерство цифрової трансформації.

7. Який орган встановлює єдині вимоги до виготовлення, обліку та зберігання матеріальних носіїв секретної інформації?
   а) Кабінет Міністрів України.
   б) Верховна Рада України.
   в) Міністерство юстиції України.
   г) Державна податкова служба.

8. Як позначаються документи з грифом “Для службового користування”?
   а) В правому верхньому куті першої сторінки проставляється відповідний гриф.
   б) На будь-якому місці документа ставиться спеціальна позначка.
   в) Гриф проставляється в кінці документа.
   г) Позначення грифа є необов’язковим.

9. Який орган здійснює контроль за обігом документів, що містять конфіденційну інформацію?
   а) Служба безпеки України.
   б) Міністерство внутрішніх справ.
   в) Органи місцевого самоврядування.
   г) Національна поліція.

10. Хто розробляє переліки відомостей, які містять конфіденційну інформацію?
    а) Експертні комісії.
    б) Верховна Рада України.
    в) Суди України.
    г) Державні підприємства.

11. Хто відповідає за правильне ведення обліку документів з грифом “Для службового користування”?
    а) Керівники організацій.
    б) Міністерство юстиції.
    в) Прокуратура України.
    г) Звичайні співробітники без відповідних повноважень.

12. Яким чином ведеться облік секретних документів?
    а) У журнальній або картковій формах.
    б) Лише у цифровому форматі.
    в) Без фіксації у спеціальних реєстрах.
    г) На усному рівні без документування.

13. Що таке реєстрація секретних документів?
    а) Надання реєстраційних номерів документам та їх запис у відповідні журнали або картки.
    б) Оприлюднення секретної інформації.
    в) Відправка документів у відкритий доступ.
    г) Переведення секретних документів у публічні реєстри.

14. Які існують види обліку документів з грифом секретності?
    а) Попередній облік, облік вихідних, вхідних документів, інвентарний облік.
    б) Лише попередній облік.
    в) Тільки фінансовий облік.
    г) Облік лише у разі розсекречення документів.

15. Що заборонено робити у формах реєстрації секретних документів?
    а) Вносити виправлення без засвідчення відповідальними особами.
    б) Використовувати кольорові маркери.
    в) Робити записи друкованими літерами.
    г) Зберігати журнали у захищених сейфах.

16. Як має вестися облік секретних документів у разі їх невеликої кількості?
    а) В одному журналі обліку вхідних, вихідних та інвентарних документів.
    б) В окремих журналах для кожного виду документації.
    в) Лише у цифровому форматі.
    г) У спеціальних базах даних з обмеженим доступом.

17. Як маркується секретний документ після реєстрації?
    а) Позначається реєстраційним номером та відповідним грифом секретності.
    б) Отримує серійний номер без додаткових позначень.
    в) Позначається штампом “Обмежений доступ”.
    г) Не потребує маркування.

18. Що відбувається із секретним документом після завершення терміну його зберігання?
    а) Він підлягає знищенню або передається до архіву.
    б) Він автоматично стає відкритою інформацією.
    в) Його передають до комерційних структур.
    г) Він оприлюднюється у відкритих джерелах.

19. Які документи мають проходити обов’язкову реєстрацію у режимно-секретних органах?
    а) Всі документи, що містять секретну інформацію.
    б) Тільки фінансові звіти.
    в) Лише листи внутрішнього користування.
    г) Документи, що стосуються охорони здоров’я.

ТЕМА 7
ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ. СПОСОБИ НЕСАНКЦІОНОВАНОГО ЗНЯТТЯ ІНФОРМАЦІЇ З ТЕХНІЧНИХ КАНАЛІВ ЇЇ ВИТОКУ

ПЛАН

1. Поняття технічного каналу витоку інформації.

2. Загальний підхід до технічного захисту інформації.

3. Фізичні основи утворення технічних каналів витоку інформації.

4. Організаційно-технічні заходи щодо ТЗІ на об'єкті.

5. Основи несанкціонованого зняття інформації способом та засобами високочастотного нав' язування.

6. Класифікація каналів витоку інформації.

1. Поняття технічного каналу витоку інформації та їхня класифікація

У сучасному інформаційному суспільстві захист інформації набуває особливого значення. Активне використання комп'ютерних систем, мережевих технологій та засобів електронної комунікації створює сприятливі умови не лише для ефективної обробки й збереження даних, але й для виникнення нових каналів їх витоку. Особливу небезпеку становлять технічні канали витоку інформації (ТКВІ), через які зловмисники можуть здійснювати перехоплення конфіденційних відомостей. В умовах зростання кіберзагроз і ускладнення методів технічної розвідки питання виявлення, класифікації та блокування ТКВІ є одним із ключових завдань систем технічного захисту інформації (ТЗІ).

Поняття технічного каналу витоку інформації

Технічний канал витоку інформації можна визначити як сукупність небезпечних фізичних сигналів, середовища їх розповсюдження і зберігання, об'єкта технічної розвідки та способів і засобів зняття інформації, що дозволяють реалізувати несанкціонований доступ до даних.

Небезпечним сигналом вважається будь-який фізичний процес або відбитий/перетворений сигнал, що містить інформацію з обмеженим доступом і

може бути використаний для її відновлення. На практиці це можуть бути акустичні хвилі, електромагнітні випромінювання, оптичні сигнали, а також матеріальні носії, до яких має доступ людський фактор.

Таким чином, ТКВІ слід розглядати як комплексний феномен, що включає фізичну основу сигналу, технічні засоби його перехоплення та організаційні умови, які роблять можливим витік даних.

Класифікація технічних каналів витоку інформації

ТКВІ традиційно поділяють на кілька основних груп залежно від фізичної природи сигналів і засобів їх перехоплення.

– *Акустичні канали.* Цей тип охоплює витік інформації через звукові коливання. Джерелом витоку можуть бути розмови, шум від обладнання або навіть акустичні вібрації будівельних конструкцій. Особливу небезпеку становлять акустично-електричні перетворення, коли звук трансформується в електричні сигнали (наприклад, через мікрофони або телефонні лінії), що можуть бути непомітно перехоплені.

– *Радіотехнічні канали – поділяються на:*

- *відкриті канали зв 'язку,* коли перехоплення можливе через бездротові комунікації, Wi-Fi, радіостанції чи мобільний зв'язок;
- *паразитні випромінювання та наводки,* що виникають як побічні ефекти роботи електронного обладнання. Такі випромінювання можуть містити відбиту інформацію і бути використані для реконструкції змісту переданих даних.

– *Оптичні канали.* Інформація може витікати через оптичні відображення або випромінювання. Прикладом є можливість спостереження за екраном комп'ютера через відбиття в склі чи використання лазерних мікрофонів для зчитування вібрацій віконних поверхонь.

– *Речовий канал.* Цей канал безпосередньо пов'язаний з людським фактором. Ненавмисне або навмисне винесення носіїв інформації, документів, флеш-накопичувачів або інших фізичних носіїв може стати причиною витоку. Речовий канал є одним із найважче контрольованих, оскільки потребує високого рівня організаційних заходів і контролю персоналу.

Крім того, ТКВІ можуть бути *природними* (що виникають внаслідок фізичних властивостей обладнання та середовища) та *штучними* (створеними свідомо шляхом розміщення апаратури технічної розвідки).

Апаратура технічної розвідки. Апаратура технічної розвідки відіграє ключову роль у реалізації витоку інформації. Вона може бути як дистанційною (наприклад, перехоплення радіовипромінювань), так і безпосередньо інтегрованою в об'єкт (приховані мікрофони, камери, передавачі). Якщо такі пристрої розміщені в зоні охоронюваного об'єкта, вони утворюють навмисний канал витоку.

З огляду на розвиток сучасних технологій, апаратура технічної розвідки стає дедалі мініатюрнішою, що ускладнює її виявлення та потребує впровадження регулярного технічного контролю.

Організаційно-технічні заходи протидії. Побудова системи технічного захисту інформації (ТЗІ) потребує комплексного підходу, який включає:

– *виявлення потенційних каналів витоку* – здійснюється шляхом аудиту технічних систем, аналізу середовища, проведення спеціальних перевірок і тестування обладнання;

– *блокування каналів витоку* – застосовують екранування приміщень, акустичні та електромагнітні фільтри, шифрування комунікаційних каналів, контроль доступу до інформації;

– *перевірка працездатності системи ТЗІ* – регулярні тестування дозволяють виявляти нові вразливості та підтверджувати ефективність заходів захисту;

– *організаційні заходи* – охоплюють підготовку персоналу, контроль доступу до об'єктів та носіїв інформації, формування політик безпеки.

Особливу роль відіграє принцип багаторівневого захисту, коли використовується поєднання технічних і організаційних методів, що забезпечує стійкість системи навіть у разі прориву окремих рубежів оборони.

Значення протидії ТКВІ для національної безпеки. Оскільки критична інфраструктура держави (енергетика, транспорт, зв'язок, фінансовий сектор, оборона) значною мірою залежить від інформаційних технологій, витік даних

через технічні канали може призвести до масштабних наслідків. Це включає не лише економічні збитки, а й створює загрозу національній безпеці. Тому системи захисту інформації на таких об'єктах повинні проектуватися з урахуванням максимально широкого спектра можливих ТКВІ та методів їх нейтралізації.

Технічні канали витоку інформації становлять одну з найбільших загроз у сфері захисту даних. Вони охоплюють широкий спектр фізичних процесів – від акустичних хвиль і електромагнітних випромінювань до оптичних відображень і людського фактора. Сучасні засоби технічної розвідки забезпечують високий рівень ефективності перехоплення, що робить питання запобігання ТКВІ критично важливим.

Ефективна система ТЗІ повинна включати як технічні рішення (екранування, шифрування, захист від наводок), так і організаційні заходи (контроль персоналу, управління доступом, моніторинг). Комплексний підхід до захисту дозволяє значно знизити ймовірність витоку конфіденційних даних та забезпечує стабільність функціонування інформаційних систем.

2. Загальний підхід до технічного захисту інформації

У сучасному інформаційному суспільстві питання забезпечення конфіденційності, цілісності та доступності даних є стратегічно важливими. Швидке зростання обсягів інформаційних ресурсів, розвиток систем автоматизованого управління та комунікаційних технологій призводять до збільшення ризиків несанкціонованого доступу, витоку та знищення інформації. В умовах кіберзагроз та технічної розвідки актуальною стає побудова ефективних систем технічного захисту інформації (ТЗІ), які поєднують у собі організаційні, інженерно-технічні та програмно-апаратні рішення.

Канал зв'язку як об'єкт захисту. Класична схема обробки та розповсюдження інформації включає три основні складові: *передавач, канал зв'язку та приймач.* При цьому найбільш уразливою ділянкою системи є саме канал зв'язку, оскільки він може бути використаний як для передачі даних до легітимного користувача, так і для їх перехоплення сторонніми суб'єктами.

З погляду технічного захисту інформації канал зв ’язку може розглядатися у двох аспектах:

– *як канал витоку інформації,* тобто як потенційне середовище для несанкціонованого зняття чи модифікації даних;

– *як ділянка для реалізації захисних заходів,* у якій застосовуються методи шифрування, екранування, кодування сигналів, моніторингу та контролю за доступом.

Таким чином, канал зв’язку виступає одночасно і слабкою ланкою інформаційної системи, і основним полем для впровадження засобів ТЗІ.

Об’єкти захисту інформації. Загальний підхід до побудови систем технічного захисту передбачає чітке визначення об’єктів, що підлягають охороні, *до них належать:*

– *інформаційні ресурси* – відомості, віднесені до категорії таємної, службової чи конфіденційної інформації;

– *засоби та системи інформатизації,* включно з інформаційно-обчислювальними комплексами, які безпосередньо здійснюють збирання, обробку та збереження даних;

– *програмне забезпечення* – операційні системи, системи управління базами даних, прикладні програми, які можуть містити вразливості та потребують захисту від несанкціонованих змін;

– *автоматизовані системи управління (АСУ),* що застосовуються в промисловості, транспорті, енергетиці та інших сферах, де помилка чи витік інформації може спричинити критичні наслідки;

– *системи зв’язку та передачі даних,* які забезпечують функціонування внутрішніх і зовнішніх комунікацій організацій;

– *технічні засоби прийому, передачі та обробки інформації обмеженого доступу,* включаючи їх інформативні фізичні поля, що можуть бути використані як джерела технічних каналів витоку.

Окрему категорію становлять системи та обладнання, що *не відносяться безпосередньо до засобів обробки інформації,* але розташовані у приміщеннях, де циркулює конфіденційна інформація.

Додаткові технічні засоби і системи (ДТЗС)

– засоби відкритого телефонного зв'язку;

– системи оповіщення та сигналізації (пожежної, охоронної);

– радіофікаційні системи;

– системи годинофікації та синхронізації часу;

– електропобутові прилади;

– інші технічні засоби, що функціонують у приміщеннях з обмеженим доступом.

Важливо зазначити, що самі приміщення, призначені для обробки інформації, також виступають об'єктами захисту, оскільки їхні конструктивні особливості (стінові панелі, вікна, двері, системи вентиляції) можуть стати каналами поширення небезпечних фізичних сигналів.

Основні завдання технічного захисту. Загальний підхід до ТЗІ полягає у створенні комплексної системи, яка забезпечує:

– *виявлення та блокування каналів витоку інформації* – акустичних, електромагнітних, оптичних тощо.

– *забезпечення цілісності та достовірності інформаційних потоків* шляхом застосування криптографічних та технічних засобів захисту.

– *регулярний контроль і перевірку працездатності систем ТЗІ,* включно з аудитом та сертифікацією.

– *поєднання організаційних та технічних заходів,* що передбачає підготовку персоналу, обмеження доступу та фізичний захист об'єктів.

Технічний захист інформації є системним процесом, що охоплює як матеріальні ресурси, так і інформаційні потоки. Класична модель передавання даних через канал зв'язку демонструє, що саме цей елемент є найбільш уразливим та потребує комплексних заходів захисту.

Загальний підхід до ТЗІ базується на чіткому визначенні об'єктів захисту, серед яких не лише інформаційні ресурси та системи інформатизації, але й додаткові технічні засоби, що можуть створювати непрямі канали витоку. Інтеграція інженерно-технічних рішень із організаційними заходами дозволяє сформувати стійку систему безпеки, здатну протистояти сучасним загрозам.

3. Фізичні основи утворення технічних каналів витоку інформації

Акустичний сигнал – це механічні коливання часток пружного середовища. Людина сприймає акустичні коливання у діапазоні частот від 20 до 20000 Гц (Герц). Цей діапазон зветься звуковим діапазоном частот. Для того, щоб передати звук каналами зв'язку або запам'ятати у приладах звукозапису, акустичний сигнал необхідно перетворити у адекватний йому електричний сигнал. Для такого перетворення використовується спеціальний перетворювач – мікрофон. Сьогодні використовуються: динамічні, конденсаторні, електретні мікрофони.

Радіотехнічні канали витоку інформації. Відкриті канали радіозв'язку. Головною особливістю радіозв'язку є використання процесу модуляції для передавання інформаційних (корисних) сигналів. Його сутність полягає у тому, що для переносу на відстань корисного сигналу використовується сигнал-переносник, на який "садять" інформаційний сигнал. Сигнал-переносник називають сигналом, що модулюється (інколи несучим сигналом або коливанням), а інформаційний сигнал – модулюючим сигналом.

Існують основні три види модуляції: амплітудна, частотна та фазова. При амплітудній модуляції інформаційний сигнал у модульованому коливанні проявляється у зміні амплітуди несучого коливання, при частотній – у змінах частоти, при фазовій – у змінах фази. З переходом на цифрові методи зв'язку використовується також амплітудно-імпульсна модуляція, але вона застосовується лише при перетвореннях безперервних сигналів у цифрові та не використовується при випромінюванні радіосигналів у ефір.

Припустимо, що інформаційний сигнал визначається функцією $s_1(t) = A_m \sin \Omega t$, а сигнал-переносник – функцією $s_2(t) = B_m \cos \omega t$. Тоді модульований сигнал слід записати як,

$$s_M(t) = A_m \sin \Omega t \bullet B_m \cos \omega t = \frac{A_m B_m}{2}\left[\sin(\Omega + \omega)t + \sin(\Omega - \omega)t\right]$$

де, Ω – частота інформаційного сигналу;

ω – частота сигнала-переносника;

A_m – амплітуда інформаційного сигналу;

B_m – амплітуда сигнала-переносника.

Фізичні основи каналів витоку, утворюються через паразитні випромінювання та наведення. Електронний прилад генерує паразитне випромінювання на суто індивідуальній власній частоті. Це явище викликається паразитними ємнісними зв'язками, що обов'язково утворюються між дротами, друкованими струмопроводами, ніжками електрорадіоелементів тощо. Виникають нові паразитні ланцюги, появу яких передбачити неможливо при проектуванні приладів та у процесі їх виробництва.

Паразитні ланцюги призводять до появи паразитних позитивних зворотних зв'язків, що й перетворює будь-який (навіть низькочастотний) електронний прилад (*наприклад*, підсилювач) у передавач, який випромінює в ефір паразитні коливання на високих та надвисоких частотах.

Наводка – це сигнал, що утворюється у будь-якій струмопровідній конструкції (*наприклад*, на трубах центрального опалення) через явище самоіндукції.

4. Організаційно-технічні заходи щодо ТЗІ на об'єкті

Організаційний захід – це захід із захисту інформації, проведення якого не потребує застосування спеціально розроблених технічних засобів. Технічний захід – це дія із захисту інформації, яка передбачає застосування спеціальних технічних засобів, а також реалізацію технічних рішень. ТЗПІ – технічні засоби прийому, обробки, зберігання та передачі інформації. ДТЗС – допоміжні технічні засоби та системи.

До основних організаційних і режимних заходів відносяться:

– проведення робіт із захисту інформації організаціями, які мають ліцензію на діяльність в сфері захисту інформації, видану відповідними органами;

– категоріювання та атестація об'єктів ТЗПІ і виділених приміщень для проведення закритих заходів із виконання вимог забезпечення захисту інформації при проведенні робіт з відомостями відповідного ступеня таємності;

– використання на об'єкті сертифікованих ТЗПІ та ДТЗС;

– встановлення контрольованої зони біля об'єкта;

– залучення до робіт з будівництва, реконструкції об’єктів ТЗПІ, монтажу апаратури організацій, що мають ліцензію на діяльність в сфері захисту інформації по відповідних пунктах;

– організація контролю і обмеження доступу на об’єкти ТЗПІ та у виділені приміщення;

– введення територіальних, частотних, енергетичних, просторових і часових обмежень в режимах використання технічних засобів, що підлягають захисту;

– відключення на період закритих заходів технічних засобів, що мають елементи, які виконують роль електроакустичних перетворювачів (лінії зв’язку тощо).

Технічні заходи включають:

– встановлення за допомогою технічних засобів потенційних каналів витоку інформації та визначення методів та засобів для їх блокування;

– перевірку техніки, яка використовується, на відповідність величини паразитних випромінювань допустимим рівням;

– екранування приміщень або техніки, яка використовується;

– перемонтаж окремих мереж, кабелів та ліній зв’язку;

– застосування спеціальних пристроїв і засобів захисту;

– використання засобів активного захисту;

– перевірку адекватності та надійності функціонування застосованих технічних засобів рівню потенційних загроз.

Необхідно:

– визначити види інформації та від якого роду загроз треба захищатися, з цією метою насамперед визначають категорію приміщення;

– заміряти відстань до іноземних установ, автостоянок, приватних фірм і визначати охоронну зону, в межах якої несанкціоноване зняття інформації вважається неможливим;

– з’ясовувати типи та ступінь можливих загроз та встановити відповідну категорію захисту інформації;

– складати акт про встановлення категорійності приміщення;

– складати план робіт з ТЗІ, в якому визначаються обсяги та напрямки проведення робіт з ТЗІ, термін їх проведення, необхідні технічні засоби для захисту інформації на об’єкті.

Під час проведення робіт з ТЗІ необхідно вживати ряд заходів, зокрема:

– визначити та змонтувати необхідні технічні засоби, що потрібні для захисту інформації на об’єкті;

– провести необхідні вимірювання, які б підтвердили ефективність застосування обраних технічних засобів захисту та їх правильне функціонування.

Технічний захист інформації від її несанкціонованого зняття полягає в застосуванні спеціальних технічних методів її захисту, які блокують потенційні канали витоку інформації, тобто заважають спробам її незаконного отримання.

5. Основи несанкціонованого зняття інформації способом та засобами високочастотного нав’язування

Високочастотне нав’язування (ВЧ-нав’язування) с одним із найбільш витончених методів технічної розвідки, що використовується для несанкціонованого зняття інформації. Сутність цього методу полягає у введенні в електричні кола об’єкта стороннього високочастотного сигналу, який, взаємодіючи з елементами системи, модулюється акустичними коливаннями, що виникають у приміщенні. Таким чином, інформація, що мас конфіденційний характер, може бути передана за межі контрольованої території без встановлення спеціальних акустичних або радіотехнічних датчиків.

Теоретичні основи методу

Будь-яке електричне коло в процесі експлуатації може виконувати роль антени, здатної випромінювати або приймати електромагнітні хвилі. Введений у це коло високочастотний сигнал, збуджуючи паразитні коливання, піддається модуляції низькочастотними звуковими сигналами, що виникають в акустичному середовищі приміщення. У результаті формується новий сигнал, який містить у собі модульовану інформацію, що може бути виділена й відновлена за допомогою спеціальних приймальних пристроїв.

Така технологія дозволяє використовувати існуючі інженерні комунікації

– телефонні лінії, електричні мережі, лінії сигналізації або навіть елементи офісної техніки – як приховані мікрофони. При цьому сам об'єкт технічної розвідки може навіть не підозрювати про факт впровадження сторонніх високочастотних коливань.

Технічна реалізація

Для реалізації ВЧ-нав'язування застосовуються спеціальні генератори, здатні формувати стабільний сигнал у діапазоні від кількох сотень кілогерц до десятків мегагерц. Цей сигнал через провідникові структури об'єкта вводиться у контрольоване середовище. У процесі взаємодії з акустичними коливаннями приміщення він піддасться амплітудній або частотній модуляції.

Отриманий сигнал випромінюється або поширюється по комунікаційних лініях і може бути зафіксований розвідувальною апаратурою. Далі відбувається його демодуляція, у результаті чого зловмисник отримує доступ до мовної інформації, шумів обладнання чи інших акустичних подій, що мають конфіденційне значення.

Потенційні об'єкти впливу. Особливу небезпеку становить використання ВЧ-нав'язування у відношенні таких систем.

– *лінії телефонного зв'язку* – навіть вимкнені апарати можуть виконувати роль мікрофона;

– *електричні мережі* – будь-який кабель, що має доступ за межі приміщення, потенційно може бути використаний для витоку;

– *системи сигналізації та охоронні комплекси* – їхні провідникові структури часто не враховуються як можливі канали витоку;

– *офісна техніка* (комп'ютери, принтери, копіювальні апарати) – паразитні елементи їхніх електричних схем здатні підсилювати ефект нав'язування.

Методи протидії

Високочастотне нав'язування відноситься до складних методів витоку інформації, а тому потребує комплексного підходу до захисту. *Серед основних заходів протидії можна виокремити:*

– *використання* фільтрів – спеціальні LC-фільтри, феритові кільця та інші пристрої, які блокують проникнення сторонніх високочастотних сигналів у електричні мережі;

– *екранування приміщень і кабельних трас* – металеві сітки та екрани зменшують рівень випромінювання та перешкоджають введенню сигналу;

– *застосування активних засобів завад* – генератори шуму в широкому діапазоні частот, які перекривають канали зв'язку й роблять модулювання неефективним;

– *регулярний контроль інженерних систем* – використання апаратури технічного контролю, що дозволяє виявляти наявність сторонніх високочастотних сигналів у мережах;

– *організаційні заходи* – обмеження доступу до технічних комунікацій, використання захищених приміщень для обробки секретної інформації.

Практичне значення та загрози. Метод ВЧ-нав'язування є особливо небезпечним у сфері функціонування державних органів, підприємств оборонно-промислового комплексу та об'єктів критичної інфраструктури. Його застосування дає змогу противнику отримати доступ до стратегічної інформації без фізичного встановлення пристроїв прослуховування, що ускладнює виявлення витоку.

Загроза зростає в умовах використання сучасних цифрових технологій, коли навіть короткочасне перехоплення може містити значний обсяг важливих даних. У зв'язку з цим дослідження механізмів високочастотного нав'язування та вдосконалення методів захисту від нього є актуальним завданням для системи технічного захисту інформації.

6. Класифікація каналів витоку інформації

Під технічним каналом витоку інформації розуміють сукупність об'єкта розвідки, технічного засобу розвідки (ТЗР), за допомогою якого збирається інформація про об'єкт, і фізичного середовища, де розповсюджується інформаційний сигнал.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх розповсюдження і способів перехоплення ТЗР *більш детально технічні канали витоку інформації можна поділити на:*

– радіоканали (електромагнітне випромінювання радіодіапазону);

– електричні (засоби провідникового зв’язку та різні струмопровідні комунікації);

– акустичні (розповсюдження звукових коливань);

– оптичні (електромагнітне випромінювання в інфрачервоній і ультрафіолетовій частини спектра).

Канали витоку інформації – це шляхи, якими конфіденційна інформація може покинути захищену зону. Вони поділяються на технічні (електромагнітні, акустичні, вібраційні) та нетехнічні (візуальні, документальні, агентурні), кожен з яких потребує специфічних методів захисту.

Комбіновані методи зняття акустичної інформації поєднують різні технічні засоби для підвищення ефективності перехоплення. *Наприклад*, використання лазерного мікрофона для зняття вібрацій з віконного скла разом із спрямованим мікрофоном для прослуховування звуків у приміщенні. Також, можливе застосування віброакустичних датчиків на будівельних конструкціях у поєднанні з аналізом електромагнітного випромінювання від технічних засобів обробки інформації.

Зняття акустичної інформації з будівельних конструкцій здійснюється за допомогою віброакустичних датчиків, що перетворюють механічні коливання на електричні сигнали. Ці датчики встановлюються на стіни, вікна, труби та інші конструкції, через які поширюються звукові хвилі. Отримана інформація може бути посилена та проаналізована для відновлення звуків, що поширюються в приміщенні.

Зняття акустичної інформації з засобів та ліній зв’язку здійснюється шляхом підключення до ліній зв’язку спеціальних пристроїв для перехоплення звукових сигналів. Ці пристрої можуть бути як пасивними, що просто приймають сигнали, так і активними, що модулюють сигнал для його подальшого аналізу. Також використовуються методи індукційного зняття інформації, які не потребують фізичного підключення до лінії зв’язку.

Радіомікрофони для зняття акустичної інформації поділяються на мініатюрні (закладні) та стаціонарні, залежно від розміру та способу встановлення. Мініатюрні пристрої маскуються під побутові предмети або

елементи інтер’єру, а стаціонарні встановлюються в місцях передбачуваного ведення розмов. Також, вони класифікуються за частотним діапазоном передачі сигналу, що впливає на дальність та якість перехоплення.

Канали зняття електромагнітної та електронної інформації включають побічні електромагнітні випромінювання (ПЕМВ), що виникають під час роботи електронних пристроїв, та наведення на лінії електроживлення та зв’язку. Для зняття інформації використовуються радіоприймачі, аналізатори спектра, а також спеціалізовані пристрої, здатні декодувати сигнали з ПЕМВ. Також, можливе використання методів несанкціонованого підключення до ліній зв’язку для перехоплення електронних сигналів.

Несанкціонований доступ до письмової інформації може здійснюватися шляхом фізичного викрадення документів, їх копіювання без дозволу або перехоплення поштових відправлень. У цифровому середовищі це може бути злам електронної пошти, файлообмінних сервісів або перехоплення повідомлень у месенджерах. Також, можливе використання соціальної інженерії для отримання доступу до інформації через обман або маніпуляції.

Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Цей Перелік формується відповідно до п. 17 Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 р. № 1229. Перелік призначений для використання суб’єктами системи технічного захисту інформації (ТЗІ) під час розроблення, модернізації та впровадження комплексів ТЗІ на об’єктах інформаційної діяльності (ОІД) та комплексних систем захисту інформації (КСЗІ) в автоматизованих системах (АС).

Перелік містить номенклатуру засобів ТЗІ (технічних засобів, основним функціональним призначенням яких є захист інформації від загроз витоку, порушення цілісності та блокування; технічних засобів, в яких додатково до основного призначення передбачено функції захисту інформації; засобів, які призначені, спеціально розроблені або пристосовані для пошуку закладних пристроїв і які створюють загрозу для інформації; засобів, які спеціально

розроблені або пристосовані для оцінювання захищеності інформації), відповідність яких вимогам нормативних документів з питань ТЗІ засвідчено сертифікатом відповідності або позитивним експертним висновком, одержаними у порядку, який встановлено нормативно-правовими актами: Правилами проведення робіт із сертифікації засобів захисту інформації, затвердженими спільним наказом Адміністрації Держспецзв'язку та Держспоживстандарту України від 25.04.2007 р. № 75/91 і зареєстрованими в Міністерстві юстиції України 14.05.2007 р. за № 498/13765, та Положенням про державну експертизу в сфері технічного захисту інформації, затвердженим наказом Адміністрації Держспецзв'язку України від 16.05.2007 р. № 93 і зареєстрованим в Міністерстві юстиції України 16.07.2007 р. за № 820/14087.

Використання засобів цього Переліку під час створення, модернізації та впровадження комплексів ТЗІ на ОІД та КСЗІ в АС не звільняє від необхідності оцінювання відповідності досягнутого рівня захисту інформації до встановленого вимогами нормативних документів з ТЗІ, яке здійснюється шляхом атестації комплексів ТЗІ на ОІД або експертизи КСЗІ в АС. Порядок використання засобів ТЗІ, які не ввійшли до цього Переліку, в комплексах ТЗІ на ОІД та КСЗІ в АС визначається нормативними документами у сфері ТЗІ.

Оновлення інформації, яка міститься в Переліку, здійснюється шляхом періодичного внесення змін до попередньої редакції. Перелік та його доповнення розміщуються на WEB-сайті www.dsszzi.gov.ua. За додатковими відомостями про засоби з цього Переліку, стан їх виробництва та порядок постачання необхідно звертатися до виробника (постачальника).

СЕМІНАРСЬКЕ ЗАНЯТТЯ
ТЕМА 7
ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ. СПОСОБИ НЕСАНКЦІОНОВАНОГО ЗНЯТТЯ ІНФОРМАЦІЇ З ТЕХНІЧНИХ КАНАЛІВ ЇЇ ВИТОКУ

План семінарського заняття

1. Поняття технічного каналу витоку інформації.
2. Загальний підхід до технічного захисту інформації.
3. Фізичні основи утворення технічних каналів витоку інформації.
4. Організаційно-технічні заходи щодо ТЗІ на об’єкті.
5. Основи несанкціонованого зняття інформації способом та засобами високочастотного нав’язування.
6. Класифікація каналів витоку інформації.

Ключові поняття та терміни: технічний канал витоку інформації, технічний захист інформації (ТЗІ), електромагнітне випромінювання, акустичний канал, віброакустичний канал, оптичний канал, побічні електромагнітні випромінювання та наведення (ПЕМВН), високочастотне нав’язування, організаційно-технічні заходи захисту, контрольований доступ, технічні засоби зняття інформації, класифікація каналів витоку, інформаційна безпека об’єкта, криптографічний захист, інженерно-технічні методи.

Завдання для самостійної роботи над темою

Завдання 1. Опрацювати теоретичний матеріал теми 7 дистанційного курсу “Система охорони державної таємниці” у Віртуальному університеті ЛДУ БЖД.

Завдання 2. Користуючись рекомендованою літературою та теоретичним матеріалом лекції, самостійно опрацювати та розв’язати ситуаційні завдання.

Ситуаційне завдання 1. Під час перевірки об’єкта виявлено, що переговорна кімната розташована біля вікон із тонким склом. Які технічні та

організаційні заходи слід застосувати для запобігання витоку акустичної інформації?

Ситуаційне завдання 2. На підприємстві виявлено аномальне електромагнітне випромінювання від комп'ютерного обладнання. Які дії має виконати служба ТЗІ для локалізації можливого витоку інформації?

Ситуаційне завдання 3. Зовнішні спеціалісти змогли відтворити дані з комп'ютерної мережі шляхом високочастотного нав'язування. Які технічні рішення необхідно впровадити для запобігання подібним атакам у майбутньому?

Ситуаційне завдання 4. Під час аудиту з'ясувалося, що секретні переговори проводяться у приміщенні з відсутністю засобів віброакустичного захисту. Які ризики це створює і які технічні засоби потрібно додати?

Завдання 3. Користуючись рекомендованою літературою та теоретичним матеріалом лекції, підготувати аргументи для обговорення дискусійних тем.

Дискусійні теми:

– Чи можливо повністю усунути технічні канали витоку інформації, чи завжди існує залишковий ризик?

– Як знайти баланс між вартістю впровадження засобів ТЗІ та рівнем загроз для конкретного об'єкта?

– Наскільки ефективними є організаційні заходи безпеки без використання сучасних технічних засобів захисту?

ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ

1. Яке призначення технічного захисту інформації?
2. Надайте визначення поняття технічного каналу витоку інформації
3. Надайте визначення поняття небезпечного фізичного сигналу
4. Яка класифікація ТКВІ прийнята в Україні?
5. Що таке природні ТКВІ? Наведіть приклади таких каналів.
6. Що таке штучні ТКВІ? Наведіть приклади таких каналів. Яким шляхом утворюються штучні ТКВІ?
7. В чому полягає сутність та основні завдання ТЗІ?
8. Що є основними об’єктами захисту інформації?
9. Які технічні засоби і системи звуться додатковими технічними засобами і системами?
10. Яка фізична сутність акустичного сигналу?
11. Яка фізична сутність акустично-електричних перетворень?
12. Які частоти коливань відносяться до звукового діапазону частот?
13. Які частоти коливань відносяться до інфразвукового діапазону частот?
14. Які частоти коливань відносяться до ультразвукового діапазону частот?
15. Як утворюється мікрофонний ефект та яка його фізична сутність?
16. В чому полягає фізична сутність процесу модуляції?
17. Які види модуляції використовуються для передавання інформації по радіозв’язку?
18. Як і де утворюються паразитні випромінювання?
19. Який механізм утворення наводок? Де вони виникають?
20. В чому полягає небезпека паразитних випромінювань та наводок?
21. Дайте визначення організаційним заходам із захисту об’єкта.
22. Які основні організаційні та режимні заходи відносяться до основних?
23. Дайте визначення технічним заходам із захисту об’єкта.
24. Які основні складові технічних заходів?
25. Який порядок проведення робіт з ТЗІ?
26. В чому полягає особливість використання беззаходових способів зняття інформації?

27. Яке призначення технічного захисту інформації?
28. Надайте визначення поняття технічного каналу витоку інформації
29. Надайте визначення поняття небезпечного фізичного сигналу
30. Яка класифікація ТКВІ прийнята в Україні?
31. Що таке природні ТКВІ? Наведіть приклади таких каналів.
32. Що таке штучні ТКВІ? Наведіть приклади таких каналів. Яким шляхом утворюються штучні ТКВІ?
33. В чому полягає сутність та основні завдання ТЗІ?
34. Що є основними об’єктами захисту інформації?
35. Які технічні засоби і системи звуться додатковими технічними засобами і системами?
36. Яка фізична сутність акустичного сигналу?
37. Яка фізична сутність акустично-електричних перетворень?
38. Які частоти коливань відносяться до звукового діапазону частот?
39. Які частоти коливань відносяться до інфразвукового діапазону частот?
40. Які частоти коливань відносяться до ультразвукового діапазону частот?
41. Як утворюється мікрофонний ефект та яка його фізична сутність?
42. В чому полягає фізична сутність процесу модуляції?
43. Які види модуляції використовуються для передавання інформації по радіозв’язку?
44. Як і де утворюються паразитні випромінювання?
45. Який механізм утворення наводок? Де вони виникають?
46. В чому полягає небезпека паразитних випромінювань та наводок?
47. Дайте визначення організаційним заходам із захисту об’єкта.
48. Які основні організаційні та режимні заходи відносяться до основних?
49. Дайте визначення технічним заходам із захисту об’єкта.
50. Які основні складові технічних заходів?
51. Який порядок проведення робіт з ТЗІ?
52. В чому полягає особливість використання беззаходових способів зняття інформації?

Рекомендована література: [1-3, 5, 7, 14, 21, 24-25].

ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ

1. Що таке технічний канал витоку інформації?
   а) Сукупність небезпечних фізичних сигналів, середовищ їх розповсюдження та засобів технічної розвідки
   б) Система програмного захисту інформації
   в) Спосіб збереження даних на зовнішніх носіях
   г) Метод шифрування даних у комп’ютерних мережах

2. Яка основна мета технічного захисту інформації?
   а) Запобігання витоку конфіденційної інформації через технічні канали
   б) Збереження документів у друкованому вигляді
   в) Використання антивірусного програмного забезпечення
   г) Зменшення обсягу інформації в комп’ютерних системах

3. До яких типів належать технічні канали витоку інформації?
   а) Акустичні, радіотехнічні, оптичні, речові
   б) Програмні, апаратні, віртуальні
   в) Електромагнітні, біологічні, механічні
   г) Локальні, хмарні, мобільні

4. Що таке небезпечний фізичний сигнал?
   а) Сигнал, що містить інформацію, яку необхідно захищати
   б) Будь-яке електромагнітне випромінювання
   в) Аудіозапис розмов співробітників
   г) Відеозапис з камер спостереження

5. Як класифікуються технічні канали витоку інформації за способом виникнення?
   а) Природні та штучні
   б) Основні та додаткові
   в) Офіційні та неофіційні
   г) Мережеві та локальні

6. Що входить до акустичних каналів витоку інформації?
    а) Канали з акустично-електричними перетвореннями
    б) Високочастотні електромагнітні хвилі
    в) Програмні вразливості в комп’ютерах
    г) Механічні пристрої зчитування інформації

7. Яка особливість радіотехнічних каналів витоку інформації?
    а) Вони можуть містити паразитні випромінювання та наводки
    б) Використовують оптичні лазери для передавання даних
    в) Передають інформацію лише в закритих мережах
    г) Функціонують без використання електромагнітних хвиль

8. Що є обов’язковою частиною перевірки надійності функціонування системи ТЗІ?
    а) Постійний моніторинг та аудит безпеки
    б) Використання тільки сертифікованих пристроїв
    в) Зберігання інформації у паперовому вигляді
    г) Впровадження нових операційних систем

9. Як класифікуються технічні заходи щодо захисту інформації?
    а) Виявлення каналів витоку, перевірка техніки, екранування, перевірка працездатності
    б) Контроль доступу, фізична охорона, аудит безпеки
    в) Використання захисного ПЗ, резервне копіювання, обмеження доступу
    г) Встановлення антивірусів, контроль паролів, бекапи

10. Яка категорія приміщень потребує особливої уваги при організації технічного захисту інформації?
    а) Приміщення, де обробляється конфіденційна інформація
    б) Приміщення, де встановлено комп’ютери з доступом до інтернету
    в) Офіси, що використовують хмарні технології
    г) Будь-які приміщення з електронними пристроями

11. Що є ключовим елементом технічного захисту інформації?
    а) Виявлення та блокування всіх потенційних каналів витоку
    б) Використання антивірусного програмного забезпечення
    в) Обмеження фізичного доступу до комп’ютерів
    г) Використання лише сертифікованого програмного забезпечення

12. Чому технічні засоби зв’язку можуть становити загрозу безпеці інформації?
    а) Вони можуть мати паразитні електромагнітні випромінювання
    б) Їх легко пошкодити фізично
    в) Вони не підтримують сучасні стандарти безпеки
    г) Використовують застарілі технології

13. Яка характеристика інформаційної системи може бути використана для визначення її вразливості?
    а) Рівень паразитних випромінювань
    б) Частота оновлення програмного забезпечення
    в) Тип користувацького інтерфейсу
    г) Кількість одночасних підключень

14. Які заходи відносяться до технічного захисту інформації?
    а) Встановлення екранування приміщень та техніки
    б) Навчання персоналу правилам безпеки
    в) Шифрування електронної пошти
    г) Використання мобільного зв’язку

15. Що є основним способом високочастотного нав’язування?
    а) Використання зовнішнього радіосигналу для модулювання мовних сигналів
    б) Використання лазерних систем контролю
    в) Застосування криптографічних методів
    г) Обмеження доступу до приміщень

16. Які основні характеристики визначають рівень захищеності ІСБ?
    а) Комплексність, швидкодія, відмовостійкість, масштабованість
    б) Програмне забезпечення, розмір серверів, потужність батарей
    в) Кількість користувачів, підтримка мобільних пристроїв
    г) Операційна система, швидкість інтернет-з’єднання

17. Яка основна функція організаційно-технічних заходів щодо ТЗІ?
    а) Забезпечення надійності захисту інформації на об’єкті
    б) Зменшення витрат на кібербезпеку
    в) Оптимізація швидкодії інформаційних систем
    г) Захист тільки внутрішньої мережі установи

18. Які об’єкти відносять до основних об’єктів захисту інформації?
    а) Інформаційні ресурси, засоби обчислювальної техніки, системи зв’язку
    б) Веб-сайти, мобільні додатки, соціальні мережі
    в) Системи відеоспостереження, бази даних клієнтів, електронна пошта
    г) Будь-яке програмне забезпечення

19. Яка основна функція технічного аудиту системи безпеки?
    а) Виявлення та усунення потенційних загроз
    б) Підвищення швидкодії комп’ютерних мереж
    в) Контроль використання ресурсів співробітниками
    г) Оптимізація вартості інформаційної інфраструктури

20. Що є одним із ключових принципів організації технічного захисту інформації?
    а) Постійний моніторинг і оцінка рівня безпеки
    б) Обмеження доступу до інтернету
    в) Встановлення антивірусного програмного забезпечення
    г) Регулярне оновлення офісних додатків

ТЕМА 8
МЕТОДИ ТА ЗАСОБИ БЛОКУВАННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

ПЛАН

1. Основні загальні положення технічного захисту інформації.

2. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації.

3. Захист акустичної інформації від зняття радіозакладними пристроями. Методи пошуку радіозакладних пристроїв.

4. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами.

5. Захист інформації від несанкціонованого запису звукозаписувальними пристроями.

6. Захист електронної інформації.

7. Захист письмової інформації від оптичного зняття.

1. Основні загальні положення технічного захисту інформації

Об’єкт технічного захисту інформації – це будова, приміщення, окремий основний технічний засіб або їх група, об’єднана загальним призначенням, які підлягають захисту від технічних розвідок. Розглянемо окремо всі складові поняття об’єкта захисту. Як видно з визначення, об’єкт може бути однією зі складових, але він може поєднувати у собі і всі зазначені складові. Все залежить від того які, по-перше, види інформації необхідно захистити та, по-друге, у яких приміщеннях об’єкта циркулює ця інформація.

Якщо це лише один вид інформації, що може циркулювати в одному або групі приміщень будівлі, виконують лише заходи з захисту цього виду інформації та певних приміщень. Якщо треба захищати велику кількість приміщень (велику група, яка, *наприклад*, складається з підгруп); об’єктом захисту може бути вся будівля.

Якщо необхідно захистити декілька видів інформації, що циркулює у приміщеннях об’єкта, то використовується комплексний захист інформації. При цьому і сам об’єкт захисту може розміщуватися всередині іншого об’єкта, який не є в цілому об’єктом захисту інформації. *Наприклад*, виділені приміщення з обмеженим доступом, розміщені на території будівлі з більш широким доступом, передбачені для роботи з певними видами інформації.

Основні технічні засоби – це технічні засоби, призначені для обробки, зберігання та передавання закритої інформації. Існують і допоміжні технічні засоби та системи, призначені для обробки відкритої інформації. Але вони можуть утворювати технічні канали витоку закритої інформації.

Отже, приступаючи до захисту інформації на певному об’єкті, необхідно, в першу чергу, визначити, які види інформації підлягають захисту, а, по-друге, які приміщення у будівлі (або всю будівлю) необхідно захищати. Також необхідно знати ступінь таємності інформації, що підлягає захисту. Крім того обов’язково необхідно знати загрози для інформації, які можуть виходити від потенційного супротивника.

Загроза для інформації – це витік, можливість блокування або порушення цілісності інформації, що може здійснюватися під час використання технічних засобів, недосконалих з точки зору захисту інформації, або інші канали витоку інформації. В разі комплексного захисту необхідно розробляти підсистеми захисту для кожного окремого виду інформації, обов’язково пов’язавши їх у комплексну систему. При цьому необхідно виявити всі потенційні канали витоку інформації та забезпечити їх блокування з рівнем технічного захисту, відповідним ступеню таємності інформації та рівню потенційних загроз.

Рівень технічного захисту інформації – це сукупність вимог, в тому числі і тих, що нормуються, які визначаються режимом доступу до інформації та загрозами для її безпеки. Взагалі у технічному захисті інформації розрізняють два основні методи: пасивний та активний методи захисту інформації.

Активний захист побудовано на постановці перешкоди зняттю інформації шляхом випромінювання завад у канал витоку, рівень яких перевищує рівень небезпечних сигналів, які можна зняти з каналів витоку. До активного захисту

також відносяться методи протидії, що засновані на постійному контролі середовища розповсюдження небезпечних сигналів необхідними для цього приладами та комплексами, які дозволяють виявляти спроби зняття інформації та активного пошуку і знешкодження засобів зняття інформації.

Пасивний захист побудовано на зниженні спроможності певного технічного джерела витоку або середи розповсюдження небезпечних сигналів до передачі інформації шляхом технічних змін його властивостей, *наприклад*, шляхом екранування електромагнітного випромінювання.

Для ТЗІ використовуються обидва напрямки захисту. Але слід відзначити, що пасивні методи захисту не використовують фізичних процесів, які шкідливі для здоров'я оточуючих та заважають повсякденній діяльності людей. Однак у більшості випадків застосування активних методів захисту є необхідним, які разом з пасивними методами захисту забезпечують потрібний ступінь рівня технічного захисту інформації.

Таким чином, ми розглянули основні загальні положення технічного захисту інформації та можемо перейти до розгляду методів та засобів блокування технічних каналів витоку окремих видів інформації. Почнемо з каналів витоку акустичної інформації.

2. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації

Першочерговим завданням при розробці проекту та обладнанні об'єкта для його захисту від витоку інформації є встановлення технічних каналів витоку інформації для кожного конкретного приміщення.

Зокрема, серед акустичних каналів витоку можуть бути як такі, що зумовлені конструктивними особливостями приміщення, так і ті, що створені навмисно (*наприклад*, замасковані отвори у стінах, звуководні канали). Особливо це стосується старих споруд, та блочних бетонних споруд – в останніх звуководні канали утворюються на стиках блоків. Для проведення робіт із захисту акустичної інформації використовуються прилади для загальних

акустичних вимірювань та спеціалізована апаратура, яка побудована на тих самих принципах, що й апаратура для зняття інформації.

Крім того, органолептично перевіряються всі приміщення, які можуть бути пов'язані з об'єктом захисту створеними навмисно звуководними каналами. При цьому, за правило, користуються повними будівельними планами всієї будівлі, де розміщено об'єкт захисту. Одночасно перевіряють відсутність (чи наявність) засобів зняття інформації на виявлених каналах витоку. При проведенні цих робіт особливу увагу слід звертати на можливість несанкціонованого зняття акустичної інформації з металевих трубопроводів опалення, вентиляції та водопостачання.

Після проведення обстеження на базі отриманих результатів вимірювань та розрахунків складається паспорт об'єкта та проектується система його захисту (обираються типи та кількість необхідної апаратури, місця розміщення випромінювачів та інше). Захиститися від витоку акустичної інформації через зачинені вікна та через стіни, стелю й підлогу можна при застосуванні спеціальних генераторів випадкових або псевдовипадкових електричних коливань, які навантажено на перетворювачі електричного сигналу в механічні коливання. Такі генератори створюють маскувальний механічний сигнал, який заважає приймати мовні сигнали на перетворювачі, що використовуються при знятті акустичної інформації. Перетворювачі генераторів розміщують на склі та на стінах, підлогах та стелях. Зрозуміло, що спочатку з'ясовують можливість такого зняття інформації з суміжних приміщень (тобто можливість проникнення в суміжні приміщення сторонніх осіб). Захищати вікна в приміщеннях, де циркулює інформація з обмеженим доступом, необхідно в тих випадках, коли вони виходять на незахищений простір, якщо охоронна зона (відстань від вікна до периметра охорони) не перевищує 200 м. Такий захист ефективно діє також проти зняття акустичної інформації з вікон за допомогою лазерного випромінювання та спрямованого мікрофона.

Нині широко відомі та часто використовуються як зарубіжні, так і вітчизняні генератори випадкових вібрацій. Генератори вібрацій можна віднести

до активних методів захисту, бо ці вібрації є активною завадою для акустичних сигналів та діє на середовища, з поверхні яких їх намагаються знімати.

Також до активних методів захисту як від прослуховування через будівельні конструкції мембранного типу, так і від прослуховування за допомогою різних типів мікрофонів, можна віднести генератори акустичного шуму, який поширюється у приміщенні, яке захищається. Зрозуміло, що при роботі таких генераторів вести розмову дуже неприємно, бо шум від генераторів заважає розмовляти. Тому з'явилися комбіновані генератори, які побудовані на принципі: завада не повинна заважати тому, хто її застосовує.

Існує три загальні тенденції розробки таких генераторів. Перша тенденція – використання зворотного зв'язку для регулювання спектра шумового сигналу та його рівня залежно від рівня акустичного сигналу, який треба маскувати. Друга тенденція – створення закритого ланцюга зв'язку для розмов між учасниками переговорів. Вона реалізується або шляхом шифрування розмов, що передаються в ізольованому від навколишнього акустичного середовища колі, або шляхом використання поза цього кола спеціальної завади, що не дозволяє зняття розбірливої акустичної інформації за межами цього кола.

Третя тенденція – використання змішаної завади, яка складається з тихої музики, шуму та голосових сигналів декількох учасників розмови, які зсунуті у часі та інвертовані по спектра. Така суміш сигналів не дозволяє зняти розбірливі сигнали розмови. Навіть якщо записати розмову, що замасковано таким чином, та очистити її відомими нині методами, неможливо отримати розбірливих сигналів. При цьому методі маскування рівень завади, що випромінюється у повітря приміщення, значно нижчий від рівня шуму, який випромінюється при застосуванні звичайного генератору. Такий шум не заважає розмові та не є шкідливим для здоров'я оточуючих.

Захист від будь-яких (радіо- чи звичайних, з дротовим зв'язком) мікрофонів, що встановлені в приміщенні, може бути виконаний також методом "завантаження" його мембрани. При застосуванні цього методу у повітря випромінюється акустична завада у вигляді модульованих ультразвукових сигналів високого рівня, які діють на мембрану мікрофону з таким тиском, що

інші акустичні коливання меншого рівня мікрофонами не сприймаються. До недоліків такого методу захисту слід віднести шкідливий вплив на людину та зовнішнє середовище ультразвукових коливань високого рівня та дуже швидке затухання таких коливань у повітрі.

Використовується також ще один метод захисту акустичної інформації, пов'язаний з встановленням електромагнітної завади від генераторів радіочастотного випромінювання. Він також дозволяє нав'язати шумову або, навіть, будь-яку іншу акустичну інформацію на нелінійні елементи апаратури звукозапису та з'єднуючі дроти мікрофонів. Метод засновано на випромінюванні у навколишнє середовище широкосмугової модульованої радіохвилі з енергією, що достатня для наведення на елементи апаратури зняття інформації сигналів завади, що повністю блокують її функціонування. Апаратура, що використовується при реалізації всіх цих методів, буде наведена нижче.

Серед генераторів вібраційних та шумових коливань сьогодні набули широкого застосування генератори "Барон", які призначено для захисту інформації, яка обговорюється в службових приміщеннях, методом вібраційного та акустичного зашумлення. Генератор створює на поверхнях конструкцій, які огороджують приміщення, та у відкритому просторі завади з рівнями, що виключають можливість виділення конфіденційної інформації з суміші сигналу з завадою.

Генератор має 4 канали формування завад, до кожного з яких можуть підключатися до 30–40 вібраторів п'єзоелектричного типу, до 10 вібраторів електромагнітного типу або акустичних систем, що забезпечують перетворення електричного сигналу в механічні коливання в конструкціях, що огороджують приміщення, а також в акустичні коливання повітря.

Разом із створенням традиційної шумової завади для підвищення ступеня маскування мовної інформації генератор може формувати нестаціонарну заваду у вигляді суміші трьох сигналів від станцій радіомовлення, для чого є три вбудовані радіоприймачі. В ході роботи здійснюється автоматичне перелаштування робочої частоти кожного з приймачів. Перелаштування робочої

частоти здійснюється за випадковим законом як у часі, так і по радіостанціях за рядом встановлених заздалегідь частот.

Для корекції амплітудно-частотної характеристики (АЧХ) приміщення кожний з каналів має вбудований еквалайзер (коригувач частотної характеристики під акустичні особливості приміщення) на п’ять смуг.

Кількість каналів завади – 4; вихідна потужність кожного каналу – не менш ніж 20 Вт; діапазон частот від 175 до 5600 Гц; кількість вібраторів, що підключаються до одного каналу: п’єзоелектричних – до 40, електромагнітних – до 10. Ці прилади дозволяють ефективно захистити акустичну інформацію в приміщенні від витоку телефонними каналами при покладеній трубці.

Значно складніше захистити від зняття інформацію під час розмови по телефону. Існує декілька видів приладів, які спроможні визначати підключення до телефонної мережі приладів, що живляться від цієї мережі. Це найпростіші прилади виявлення підслуховуючих пристроїв та несанкціонованого підключення до телефонної мережі, таких приладів багато.

Однак треба враховувати, що всі вироби подібного класу можуть контролювати телефонну мережу лише від апарата до АТС. Підключення на АТС можливе лише у одному випадку – з відповідного дозволу суду технічними службами правоохоронних органів. Але у цьому випадку підключення не може бути виявлене жодним приладом.

Саме тому необхідні реально працюючі прилади, які б надійно виявляли “інтелігентні” способи зняття інформації з телефонних ліній, *наприклад*, способом індукційного зняття або пристроями з надвисокими вхідними опорами та відповідно малими ємностями. Але ніякі прилади, що використовуються з одного боку лінії, не можуть виявити наявність засобів зняття інформації на протилежному полюсі зв’язку, тобто у абонента, з яким ведеться розмова (якщо він, звичайно, сам не потурбувався про захист своєї частини лінії). Тому для надійного захисту телефонних розмов слід використовувати “закриті” телефонні канали, де застосовується криптографічний захист інформації (скремблери).

Існує декілька принципів криптографічного захисту акустичної інформації. Відповідно до цього є й різні прилади захисту, які відрізняються різною вартістю та надійністю.

Найбільш надійними є прилади та методи, що використовують вокодери та ліпідери з подальшим шифруванням. Принцип роботи таких пристроїв полягає у цифровій обробці аналогових сигналів, виявленні та розкладенні слів та звуків на окремі форманти та передачі мови у вигляді попередньо зашифрованому набору формант. При цьому ключове слово до шифру може сягати довжини до 512 знаків, а інколи і ще більше. Це системи надвисокої надійності, *наприклад*, урядовий зв'язок. На розшифрування такої перехопленої розмови за правило потрібно багато часу, інколи мільйони років.

Існують менш складні системи, які засновано на цифровій обробці спектра сигналів та передачі сигналів з іншим спектром. На приймальному кінці у відповідності з завданими правилами приймання відбувається зворотне перетворення сигналів.

Зрозуміло, що всі апарати криптографічного захисту інформації працюють у закритому режимі лише тоді, коли вони встановлені з обох кінців лінії зв'язку, тобто наявні у обох абонентів, що розмовляють між собою.

На останнє слід додати, що всі наведені вище методи та засоби захисту інформації як у провідних каналах, так і у каналах радіозв'язку застосовуються (або можуть бути застосовані) для захисту повідомлень у системах оперативного зв'язку ОВС.

3. Захист акустичної інформації від зняття радіозакладними пристроями. Методи пошуку радіозакладних пристроїв

Перший, найбільш ефективний – це постійний радіомоніторинг ефіру. Метод полягає у постійній перевірці радіовипромінювань та виявленні нових складових у рисунку спектра (тобто, нових частот випромінювання), шляхом порівняння з попереднім. При появі у контрольованій області спектра нових частотних складових проводять пошук передавача. Для цього використовують спеціальні прилади та методи пошуку, які складають сутність другого підвиду.

Але якщо перший підвид вимагає, в разі появи нових спектральних складових, застосувати інший, то останній може бути використаний автономно. Це метод періодичних оглядів, який застосовується на об'єктах, де відсутня апаратура для постійного контролю. Виконувати цю роботу повинні фахівці, що добре розуміються у радіотехнічних вимірюваннях та володіють методикою виявлення та знешкодження радіозакладок.

Такі приймачі мають вихід на персональний комп'ютер (другий елемент системи), з якого за допомогою спеціальної програми (третій елемент системи) провадиться керування режимами роботи сканера. Сканер може перенастроюватися із заданим шагом дискретності по частоті. Крім того, він може працювати з сигналами, які мають різний вид модуляції та в різній смузі частот прослуховування (широкій та вузькій), має зменшувач шуму, індикацію режиму. Взагалі, сканер може працювати автономно від ПЕОМ, що і використовується при пошуку радіозакладок. Є й більш досконала апаратура, яка використовується у професійній радіорозвідці.

Програма моніторінгу побудована таким чином, що запам'ятовує спектр просканованої ділянки ефіру та використовує його як еталон при порівнянні з наступними вимірюваннями. Результати пошуку виводяться на монітор. В разі виявлення нових частотних складових у контрольованій зоні ПЕОМ видає сигнал тривоги. Система може працювати і в автоматичному режимі.

Зараз багатьма фірмами розроблено декілька таких програм. Принцип їх побудови однаковий, хоча вони можуть бути різними за вартістю і точністю роботи. Зараз подібні програми розроблені й в Україні. Це програма "DigiScoun", яку слід відмітити серед багатьох програм, розроблених для автоматичного сканування ефіру.

Робота комплексу з цією програмою побудована за принципом порівняння параметрів акустичних сигналів та працює таким чином:

1. На першому етапі вимірюється та запам'ятовується спектр радіосигналів по всьому діапазону роботи сканера. Одночасно встановлюється вид модуляції для кожного сигналу, випромінювання якого зафіксовано.

2. На другому етапі на кожній з виявлених частот комплекс випромінює у повітря декілька складних акустичних сигналів, які сприймаються ним через ланцюг зворотного зв'язку, а саме – через радіоканал (приймач сканера) на тій частоті, що перевіряється. Якщо в приміщенні є радіозакладка, то параметри сигналу, який продетектовано з ефіру, співпадуть з параметрами сигналу, що випромінювався у повітря приміщення. Для забезпечення однозначності сигналів, що сприймаються радіозакладкою, в сигнал, що випромінюється комплексом, додається акустичний сигнал з приміщення (шум, розмови і т. інше) через другий ланцюг зворотного зв'язку (мікрофон, підсилювач та змішувач сигналів).

Розглянемо методику та засоби пошуку та знешкодження радіозакладних пристроїв. За наявності комплексу радіомоніторингу при проведенні таких робіт необхідно провести моніторинг ефіру. В разі відсутності такого комплексу можна проводити контроль за допомогою сканера. Такі роботи проводяться двома – трьома особами і завжди починаються з розпитувань хазяїв приміщення, що перевіряється: чи дарували їм якісь сувеніри, якщо так, то коли, й які з них знаходяться у приміщенні.

Далі завжди проводять візуальний огляд приміщення, звертаючи особливу увагу на зручні (для розміщення закладки) місця. У цих роботах слід користуватися ліхтариком. Крім меблів, слід оглянути електричні та телефонні розетки, вентиляційні отвори, ніші для батарей опалювання і т. п. Також особливу увагу слід звернути на рамки від різних картин, естампів, портретів, фотографій. При огляді цих предметів треба детально проаналізувати їх конструкцію та перевірити, чи не виконані вони так, що утворюють резонансний контур для ВЧ-нав'язування.

Далі сканером перевіряється ефір. При цьому для активації закладок, що спрацьовують від акустичного сигналу, застосовується спеціальні сигнали, записані на магнітофон. Така фонограма записується з суміші мовних та синусоїдальних сигналів з частотою 400 Гц та 1 кГц.

Одночасно можна починати перевірку у близькому полі. Для цього використовуються індикатори (або детектори) поля. Такі прилади фіксують наявність джерела випромінювання, що розміщено на відстані до 25 см від

антени апарата. Це портативний широкосмуговий радіоприймач, що реагує на електромагнітне поле (джерело радіовипромінювання).

Як правило, такі прилади забезпечені світовою та звуковою індикацією, яка сигналізує про наближення до джерела випромінювання. Часто вони мають вбудований частотомір з індикацією частоти випромінювання. Такі прилади є незамінними там, де неможливо провести візуальний контроль.

І, нарешті, для виявлення закладок, що керуються дистанційно і можуть бути відключені від джерела живлення на час перевірки, слід застосувати так званий нелінійний локатор, тобто апарат, який виявляє напівпровідникові прилади навіть якщо вони не працюють. За допомогою такого апарата слід перевірити всі предмети інтер'єру, стіни, стелю (особливо, якщо вона підвісна), підлогу (особливо паркетну). Апаратура цього типу побудована на властивій всім напівпровідникам нелінійності характеристик, отже на обов'язковому процесу нелінійного перетворення сигналів (модуляції), що на них подаються у будь-який спосіб. Тому такі апарати випромінюють імпульси (або змінне електромагнітне поле достатньої потужності) та приймають і аналізують сигнал відгуку на наявність у ньому нових частотних складових, що відповідають другій та третій гармонікам контрольного сигналу.

Крім виявлення радіозакладних пристроїв їх можна придушити шляхом встановлення активної радіотехнічної широкосмугової або прицільної (вузькосмугової) завади. Вузькосмугова завада ставиться в тому випадку, коли точно відома частота, на якій працює радіозакладка. Але цей спосіб захисту використовується рідко та лише в разі, коли передавач закладки має дуже велику потужність.

В таких приладах використовуються генератор випадкового сигналу, підсилювачі потужності та випромінювачі. Але прилад "Завада" має значну перевагу над зарубіжними аналогами. По-перше, він має високу потужність, що дозволяє перекрити велику площу захисту, і, по-друге, його генератор побудовано на генерації "білого" шуму у широкій смузі частот, значно ширше, ніж у всіх інших приладів такого типу.

Слід додати, що прилади постановки радіотехнічної завади мають ще одне важливе призначення. Їх застосовують для блокування радіовибухових пристроїв під час розмінування. І в цьому випадку пристрій “Завада” має незаперечну перевагу, оскільки його генератор побудований на принципі генерації шуму, а не псевдовипадкових послідовностей, що використовуються у більшості інших аналогічних приладів. Саме тому при його застосуванні виключається можливість випадкового співпадіння сигналу завади з кодом підриву вибухового пристрою.

4. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами

При розгляді методів та засобів зняття інформації ми побачили, скільки можливих каналів витоку виникає на різноманітних технічних засобах, які використовуються у робочих приміщеннях та побуті. Зрозуміло, що при проектуванні системи захисту інформації слід потурбуватися про блокування цих каналів. Найбільш імовірне їх використання – це зняття акустичної та електромагнітної інформації. Найчастіше використовуються механізми перетворень акустичних сигналів у електричні та паразитні випромінювання і наводки. Також ніколи не виключається можливість використання супротивником ВЧ-нав’язування.

Для блокування таких каналів витоку використовуються активні методи протидії. Блокувати такі канали витоку можна застосуванням активної завади у радіотехнічному та звуковому діапазоні частот. При цьому слід забезпечити можливість виконання технічними засобами, які треба захистити, своїх основних функцій без перешкод для їх роботи з боку засобів захисту інформації.

Для цього у різних країнах на різних етапах розвитку методів та засобів технічного захисту інформації розроблялися окремі прилади, використання яких вимагало узгодження їх різних характеристик та можливостей для отримання цілісного комплексу захисту інформації.

Для активного захисту інформації від ВЧ-нав’язування можна використати новий метод, запропонований О. В. Рибальським. Його застосування змінює

властивості сигналу ВЧ-нав’язування, що робить його непридатним для отримання акустичної інформації. Цей ефект виникає тому, що випромінюється спеціальний сигнал протидії з частотою, близькою до частоти сигналу зондування ВЧ-нав’язування. Це призводить до виникнення явища биття між цими сигналами, а при наближенні частоти випромінюваного сигналу протидії до частоти сигналу ВЧ-нав’язування відбувається навіть захоплення частоти сигналу протидії генератором сигналу зондування ВЧ-нав’язування.

В результаті взаємодії двох таких коливань виникає нове коливання з частотою:

$$\omega = \frac{\omega_1 + \omega_2}{2},$$

де ω_1 – частота сигналу протидії,

ω_2 – частота сигналу зондування, та змінною амплітудою, максимальні значення якої повторюються з частотою $\Omega = \omega_1 - \omega_2$.

При цьому, при переході амплітуди цих коливань через нуль відбувається змінювання їх фази.

При використанні ВЧ-нав’язування зняття інформації може відбуватися методами амплітудної, частотної та фазової модуляції. Сам факт виникнення нового коливання з іншою частотою вже перешкоджає зняттю інформації, оскільки не відбувається перевипромінювання модульованих інформацією сигналів, або їх рівень значно послаблюється.

Змінювання фази нового коливання перешкоджає зняттю інформації методом фазової модуляції. Але цей ефект підвищується для фазової та частотної модуляції завдяки змінюванню частоти генерації випромінюваного сигналу вліво та вправо від її середнього значення сигналом керування, складеним з випадковим сигналом. Крім того, виникає паразитна амплітудна модуляція перевипромінюваних сигналів.

А складання генерованого сигналу з іншим випадковим сигналом призводить до ще більшого рівня завади для амплітудної модуляції, що додатково перешкоджає зняттю інформації.

5. Захист інформації від несанкціонованого запису звукозаписувальними пристроями

Несанкціонований аудіозапис належить до категорії технічних каналів витоку інформації і є одним із найбільш поширених способів отримання конфіденційних відомостей. Сучасні цифрові диктофони та вбудовані модулі запису у мобільних пристроях дозволяють непомітно фіксувати розмови з високою якістю та тривалістю збереження. Тому захист від такого виду загрози є критично важливим у діяльності державних органів, підприємств оборонно-промислового комплексу та організацій, що працюють із закритими даними.

Основні напрями захисту

Виділяють два ключові напрями:

– *виявлення звукозаписувальних пристроїв* – ідентифікація апаратури, що потенційно може бути використана для аудіозапису.

– *придушення можливості запису* – створення умов, що унеможливлюють або суттєво погіршують якість аудіофіксації.

Виявлення звукозаписувальних пристроїв

Методи виявлення базуються на фізичних принципах роботи диктофонів і мобільних пристроїв:

– *традиційний підхід* – використання металодетекторів. Однак цей метод потребує безпосереднього контролю особи (огляду, перевірки ручної поклажі), що не завжди є прийнятним із правових та етичних міркувань;

– *спеціалізовані індикаторні прилади* – портативні детектори, які реагують на роботу диктофону. Вони можуть бути розміщені на одязі персоналу служби безпеки. При наближенні до діючого пристрою на відстань 0,5-1 м. прилад подає сигнал (вібрація, звуковий або світловий індикатор);

– *радіочастотні детектори* – дозволяють ідентифікувати диктофони та смартфони з активними бездротовими модулями (Wi-Fi, Bluetooth, GSM), що передають або періодично випромінюють сигнали;

– *акустико-електричні методи* – застосування генераторів спеціальних імпульсів для виявлення мікрофонних капсул, що резонують на визначених частотах.

Придушення можливості аудіозапису

Захист будується на принципах створення завад, що ускладнюють роботу записувальних пристроїв:

– *акустичні завади* – застосування генераторів шуму (білого, рожевого, структурованого). Такі системи формують у приміщенні фоновий рівень звукових коливань, що перекриває мовний діапазон, роблячи запис нерозбірливим. Рекомендується використання *маскувальних акустичних систем* локального (у зонах переговорів) або просторового (по всьому приміщенню) типу;

– *електромагнітні завади* – створення перешкод для електронних компонентів цифрових диктофонів, зокрема мікрофонних підсилювачів чи модулів обробки сигналу. Слід враховувати нормативні обмеження, адже потужні ЕМ-поля можуть впливати на іншу техніку;

– *інфразвукове та ультразвукове маскування* – застосування випромінювачів у діапазонах, нечутних для людини, але таких, що викликають спотворення у мікрофонах звукозаписувальних пристроїв;

– *захист архітектурного середовища* – звукоізоляція приміщень, використання звукопоглинальних матеріалів, подвійних дверей і акустичних екранів для мінімізації поширення мовного сигналу.

Організаційні заходи

Технічний захист слід підкріплювати організаційними методами:

– регламентація доступу до нарад та переговорів;

– заборона на використання мобільних пристроїв і диктофонів у захищених приміщеннях;

– облаштування *зон без техніки* («no gadget areas»);

– проведення інструктажу персоналу щодо ризиків аудіозапису;

– регулярний огляд приміщень і контроль технічних засобів.

Захист інформації від несанкціонованого аудіозапису є багатокомпонентною задачею, що передбачає виявлення пристроїв потенційного прослуховування, створення активних завад для їх роботи та дотримання організаційних заходів. Ефективність системи забезпечується лише за умови комплексного застосування технічних та адміністративних методів із урахуванням специфіки приміщення та рівня загрози.

6. Захист електронної інформації

Захист електронної інформації є багатогранною галуззю, що поєднує інженерно-технічні, програмно-апаратні та організаційні заходи. Існує велика кількість відкритих і спеціальних наукових праць, присвячених проблемам запобігання витоку інформації, проте ефективна реалізація більшості технічних рішень потребує використання спеціалізованого обладнання та високоточної і/ вимірювальної техніки, які доступні переважно на великих науково-виробничих і/ підприємствах радіоелектронного профілю та в акредитованих лабораторіях. Такі організації зазвичай мають відповідні ліцензії і виконують роботи на замовлення державних установ, підприємств критичної інфраструктури та комерційних організацій.

Теоретичні засади і загальні підходи

Захист електронної інформації спрямований на запобігання несанкціонованому зняттю, модифікації або відтворенню даних, котрі проходять обробку, зберігання чи передавання за допомогою електронної техніки. До типових джерел загроз належать паразитні електромагнітні випромінювання та наведення, акустичні прояви обладнання, небажане випромінювання оптичного характеру, а також уразливості програмного забезпечення й засоби прихованого доступу. Тому система захисту повинна забезпечувати як зниження емісії (подавлення витоку), так і детекцію та локалізацію можливих каналів витоку.

Основні технічні методи захисту

1. Екранування від паразитних випромінювань і наводок. Екранування передбачає формування електромагнітного бар'єра, що обмежує випромінювання і проникнення зовнішніх сигналів. Технічна реалізація може здійснюватися як на рівні окремих пристроїв (екранування корпусів комп'ютерів, моніторів, накопичувачів), так і на рівні приміщення (екрануючі покриття стін, вікон, дверей). Методи екранування включають використання тонких металевих покриттів, металевих сіток, фольгованих матеріалів та спеціальних композитів. Для досягнення необхідного рівня захисту застосовують контролювання параметрів екрана (коефіцієнт екранування, частотний діапазон, стійкість до механічних дефектів).

2. *Маскування сигналів (заглушення).* Маскування здійснюється шляхом створення контрольованого шумового фону у відповідних частотних діапазонах, що унеможливлює виділення корисного сигналу з-поміж завад. Для цього використовують генератори широкосмугового шуму з налаштованим спектром і рівнем потужності. Важливою особливістю є адаптація спектральної щільності шуму до конкретних характеристик обладнання та середовища яке захищається.

3. *Заземлення та спеціальні ланцюги заземлення.* Правильне проектування систем заземлення знижує рівень паразитних струмів і перешкод, мінімізує утворення контурних різниць потенціалів і зменшує можливість екранування обхідними шляхами. Використовуються багаторівневі схеми заземлення, ізольовані контури та фільтрувальні входи для критичних ділянок.

4. *Спеціальні джерела живлення та фільтри в мережах електроживлення.* Захищене джерело живлення із стабілізованим виходом і високою якістю електросигналу зменшує ризик виникнення паразитних випромінювань. У мережі встановлюються високоякісні фільтри (LC, пасивні та активні), мережеві герметизатори й пристрої для гальванічної розв’язки, що перешкоджають проникненню ВЧ-сигналів по лініях живлення.

5. *Програмне шифрування інформації при збереженні й передаванні.* Широко застосовується криптографічний захист даних: шифрування файлових систем, баз даних, каналів зв’язку (VPN, TLS/SSL), а також методи цілісності й автентифікації. Програмне шифрування знижує практичну корисність материнських або фон-сигналів у випадку їх перехоплення, але не усуває фізичних каналів витоку як таких.

Технологічні особливості виконання робіт

Ряд заходів потребує складного технологічного обладнання та і/ спеціалізованих технологічних процесів. Зокрема, екранування корпусних елементів комп’ютерної техніки іноді виконується методом вакуумного напилення тонких металевих шарів (PVD, CVD), що забезпечує рівномірне металеве покриття з контролем товщини і адгезії. Для екранів приміщень застосовують екранувальні панелі з інтегрованою вентиляцією та фільтрацією,

що дозволяє зберегти мікроклімат приміщення без погіршення ефективності екрана.

Маскування за допомогою генераторів шуму вимагає дослідження спектральних характеристик прийомних каналів і їх взаємодії з навколишнім середовищем. Часто застосовують адаптивні системи маскування, що коригують спектр і потужність шумових сигналів у режимі реального часу.

Діагностика і контроль ефективності заходів

Оцінка ефективності заходів технічного захисту здійснюється за допомогою вимірювань рівнів випромінювань, спектрального аналізу, тестування каналу передачі та польових випробувань. Ключові інструменти включають спектроаналізатори, високочутливі приймачі, вимірювачі електромагнітної сумісності, а також пристрої для оцінки якості екранування (S-параметри, коефіцієнт ослаблення). Регулярні атестаційні вимірювання й аудит дозволяють виявляти деградацію захисних властивостей і вчасно проводити ремонтні роботи.

Організаційні та нормативні аспекти

Технічні заходи повинні доповнюватися організаційними: регламентація доступу до службових приміщень, політики щодо використання зовнішніх носіїв, інструктаж персоналу, контроль обігу технічних засобів, плани реагування на інциденти. Дотримання державних стандартів і нормативів (у тих юрисдикціях, де вони є) та вимог замовника – обов'язкова умова для проведення робіт. Також важливим є сертифікаційний контроль організацій, що виконують роботи з технічного захисту, та ведення технічної документації.

Рекомендації для практичної реалізації

– проводити попередні аудити безпеки і спектральні дослідження до застосування технічних заходів;

– використовувати багаторівневий підхід: поєднання екранування, маскування, фільтрації, захищених джерел живлення і криптостандартів;

– застосовувати адаптивні системи маскування та активного захисту, що коригуються відповідно до змін навколишнього середовища;

– забезпечити регулярні випробування й метрологічну підтримку обладнання для збереження ефективності ТЗІ;

– впроваджувати заходи організаційного характеру: обмеження доступу, політики використання носіїв, навчання персоналу та реагування на інциденти.

Захист електронної інформації – складний міждисциплінарний процес, що потребує високотехнологічних рішень і кваліфікованих кадрів. Тільки поєднання інженерних заходів (екранування, маскування, фільтрація), програмних засобів (шифрування) та організаційних політик забезпечує належний рівень протидії технічним каналам витоку. Виконання таких робіт має здійснюватися з урахуванням метрологічної підтримки й у рамках нормативних вимог, з обов'язковою системою контролю якості та періодичних перевірок.

7. Захист письмової інформації від оптичного зняття

Оптичне зняття інформації (фотографування, відеоспостереження, спостереження через оптичні прилади) є однією з найбільш поширених і доступних форм несанкціонованого збору даних. Джерелом такої інформації можуть бути як паперові носії, так і екрани моніторів, мобільних пристроїв або інших електронних відображувачів. У контексті захищених приміщень та об'єктів критичної інфраструктури оптичне зняття становить серйозну загрозу конфіденційності, оскільки дозволяє зафіксувати значні обсяги інформації на відстані й без фізичного контакту з об'єктом.

Канали оптичного зняття та їх характеристика

Оптичне зняття може здійснюватися із зовнішньої точки (через вікна, крізь щілини будівельних конструкцій), із внутрішньої – за допомогою камер/телекамер, а також шляхом використання довгофокусних об'єктивів, біноклів або дронів. Для екранів додатковим уразливим каналом є фотосканування з відбиття екрана на сусідні блискучі поверхні або з корекцією положення камери під час переміщення користувача.

Критичні характеристики каналів оптичного зняття: відстань виявлення (залежить від роздільної здатності об'єктива та умов освітлення), кут огляду, здатність до відновлення дрібних символів (чутливість по просторовій

роздільності), та маскування джерел зйомки (прикриття камери, використання малопомітних корпусів).

Технічні засоби захисту

Захист через вікна та прозорі поверхні:

– *оптичні бар'єри* – використання матованого, тонованого або спеціально текстурованого скла/плівок, що розмивають контури та унеможливлюють читання дрібних символів з відстані;

– *багатошарове скло з дифузійними шарами* – інжекційні чи ламіновані конструкції, що знижують чіткість зображення при збільшеній відстані;

– *штори та жалюзі* – механічні засоби, що забезпечують оперативне блокування візуального доступу. Рекомендується використовувати матеріали з високим коефіцієнтом світлопоглинання;

– *активне затемнення* – електрохромні або електролюмінісцентні плівки, що керуються дистанційно для швидкого перекриття огляду.

Захист від внутрішніх прихованих камер:

– *пошук і локалізація камер* – застосування оптичних детекторів, інфрачервоних і лазерних сканерів для виявлення об'єктивів за допомогою відбитого світла; використання радіочастотних (RF) детекторів для пошуку бездротових передавачів камер.

– *електронні засоби придушення* – у випадках законного та безпечного застосування (наприклад, лабораторії) можливе використання пристроїв, що генерують цільові оптичні чи інфрачервоні маскуючі сигнали, слід враховувати правові й технічні обмеження щодо придушення.

– *фізичний огляд* – інспекційні огляди приміщень, мережевих інтерфейсів та кабелів для виявлення незареєстрованих пристроїв; періодичні ревізії інженерних отворів, вентиляційних решіток, люстр та побутових приладів.

Захист екранів та електронних відображувачів

– *антигляр-фільтри і приватні фільтри (privacy filters)* – оптичні екрани, що обмежують кут огляду, роблячи зображення чітким лише для користувача у фронтальній зоні;

– *регулювання яскравості й контрасту* – мінімізація яскравості та використання темних тем інтерфейсу, що ускладнює оптичне зчитування на відстані;

– *розміщення та орієнтація робочих місць* – організаційний захід: монтаж екранів до внутрішньої частини приміщення, щоб уникнути напрямку на вікна чи проходи;

– *автоматичне затемнення при відсутності користувача* – скринсейвери з паролем, швидке блокування сесії при бездіяльності.

Методи виявлення та інструментальні засоби контролю

Ефективний захист передбачає регулярний моніторинг. До інструментальних методів належать: оптичні сканери та детектори об'єктивів, інфрачервоні камери для виявлення теплових слідів техніки, спектральні прилади для аналізу відбитого люмінесцентного світла, RF-детектори для пошуку бездротових передавачів, а також періодичні оптичні інспекції з використанням біноклів або довгофокусних об'єктивів для імітації зовнішньої загрозливої точки. Важливо інтегрувати результати таких перевірок у процедури s аудиту безпеки.

Організаційні заходи та політики. Технічні заходи повинні доповнюватися чіткою організаційною політикою. Ключові елементи: регламентація розташування робочих місць, правила зберігання паперових матеріалів (обмеження залишення на відкритих столах), заборона використання особистих фото- та відеопристроїв у захищених зонах, правила проведення візитів і супроводу, інструктаж персоналу щодо поведінки за наявності сторонніх осіб. Необхідно запровадити процедури регулярного контролю приміщень, реєстрації техніки та обліку ремонтних робіт, що можуть створювати тимчасові вразливості.

Оцінка ризику та тестування стійкості. Перед впровадженням захисних заходів рекомендується виконати оцінку ризику оптичного зняття: ідентифікувати цінні об'єкти (які документи/екрани містять критичну інформацію), оцінити ймовірні точки спостереження (зовнішні підходи, сусідні будівлі, рівень освітлення) та провести експериментальні тестування –

моделювання зйомки з різних відстаней і кутів з використанням реальної оптики для визначення максимальної відстані безпечного читання. Результати тестування повинні стати підґрунтям для вибору технічних і організаційних контрзаходів.

Практичні рекомендації:

– використовувати приватні фільтри для екранів на робочих місцях з конфіденційною інформацією; орієнтувати екрани всередину приміщення;

– застосовувати матове або захисне скло, штори або електрохромні плівки на вікнах у робочих зонах;

– впровадити регламент обліку і інспекцій техніки;

– заборонити встановлення особистих відео/фото пристроїв у захищених зонах;

– проводити періодичні огляди приміщень з використанням оптичних та RF-детекторів;

– проводити навчання персоналу щодо виявлення підозрілих пристроїв;

– у випадках підвищеної загрози застосовувати активні засоби маскування або адаптивне затемнення екранів, з урахуванням правових обмежень.

Захист письмової інформації від оптичного зняття потребує поєднання *у* інженерно-технічних рішень, інструментальної діагностики та організаційних політик. Тільки комплексний підхід – що включає фізичні бар'єри для оптичного доступу, контроль приміщень, технічне виявлення прихованих камер і навчання персоналу – забезпечує належний рівень конфіденційності. Оцінка ризиків та періодичне тестування стійкості захисту дозволяють адаптувати заходи до конкретних умов експлуатації та еволюції загроз.

СЕМІНАРСЬКЕ ЗАНЯТТЯ
ТЕМА 8
МЕТОДИ ТА ЗАСОБИ БЛОКУВАННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

План семінарського заняття

1. Основні загальні положення технічного захисту інформації.
2. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації.
3. Захист акустичної інформації від зняття радіозакладними пристроями.
4. Методи пошуку радіозакладних пристроїв.
5. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами.
6. Захист інформації від несанкціонованого запису звукозаписувальними пристроями.
7. Захист електронної інформації.
8. Захист письмової інформації від оптичного зняття.

Ключові поняття та терміни: технічний захист інформації, блокування каналів витоку інформації, акустичний захист, радіозакладні пристрої, пошук закладних пристроїв, акустошумові генератори, екранування, віброізоляція, допоміжні технічні засоби, звукозаписувальні пристрої, криптографічний захист електронної інформації, оптичний канал витоку, антишпигунські засоби, контроль технічного стану, спеціальні перевірки приміщень, світломаскування, шифрування даних, поліграфічний захист.

Завдання для самостійної роботи над темою

Завдання 1. Опрацювати теоретичний матеріал теми 8 дистанційного курсу “Система охорони державної таємниці” у Віртуальному університеті ЛДУ БЖД.

Завдання 2. Користуючись рекомендованою літературою та теоретичним

матеріалом лекції самостійно опрацювати та розв’язати ситуаційні завдання.

Ситуаційне завдання 1. У переговорній кімнаті під час аудиту було виявлено сторонні акустичні шуми, які можуть свідчити про роботу закладного пристрою. Які методи пошуку та блокування слід застосувати?

Ситуаційне завдання 2. Під час ділової наради один із співробітників використовував диктофон. Які організаційні та технічні заходи варто впровадити для запобігання несанкціонованому звукозапису в майбутньому?

Ситуаційне завдання 3. На підприємстві під час перевірки встановлено, що комп’ютери випромінюють електромагнітні сигнали, які можуть бути перехоплені на відстані. Які технічні засоби потрібно використати для їхнього екранування та захисту інформації?

Ситуаційне завдання 4. Було зафіксовано спробу фотографування документів із грифом “Таємно”. Які методи оптичного захисту слід застосувати для недопущення подібних випадків?

Завдання 3. Користуючись рекомендованою літературою та теоретичним матеріалом лекції підготувати аргументи для обговорення дискусійних тем.

Дискусійні теми:

– Чи можна вважати організаційні заходи (наприклад, заборону використання мобільних пристроїв) достатньо ефективними без технічних засобів захисту?

– Які методи виявлення закладних пристроїв є більш ефективними – активні (сканування, пошук сигналів) чи пасивні (екранування, акустичні перешкоди)?

– Чи можливо забезпечити повний захист від технічних каналів витоку в умовах швидкого розвитку нових шпигунських технологій?

ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ

1. Дайте визначення об’єкта технічного захисту інформації.
2. Коли використовується комплексний захист інформації?
3. Дайте визначення основних технічних засобів.
4. Дайте визначення допоміжних технічних засобів.
5. Дайте визначення поняття “загрози для інформації”.
6. Дайте визначення поняття “рівень технічного захисту інформації”.
7. Дайте визначення поняття “активний захист інформації”.
8. Дайте визначення поняття “пасивний захист інформації”.
9. Чим відрізняється пасивний захист від активного захисту інформації?
10. Який порядок проведення робіт з технічного захисту інформації на об’єкті?
11. Які фізичні явища покладено в основу методів і засобів захисту акустичної інформації від витоку через вібраційні канали?
12. В чому полягає метод “завантаження мембрани”, що використовується для придушення мікрофонів?
13. Які прилади використовуються для захисту акустичної інформації, що циркулює у приміщенні, від зняття з телефону?
14. Які засоби захисту акустичної інформації використовуються при передаванні її по телефонних мережах у проміжку від телефона до АТС?
15. Які прилади використовуються для виявлення засобів зняття акустичної інформації з телефонних мереж у проміжку від телефона до АТС?
16. Які засоби захисту акустичної інформації використовують для її захисту по всьому ланцюгу передавання у телефонній мережі між двома телефонами?
17. Що потрібно брати до уваги при візуальному пошуку радіозакладних пристроїв?
18. Які методи використовують для виявлення радіозакладних пристроїв?
19. Які функції виконують програми моніторингу ефіру?

20. Який алгоритм виявлення радіозакладних пристроїв з використанням методу моніторингу ефіру?
21. Які функції виконують сканери пошуку радіозакладних пристроїв?
22. Які функції виконують індикатори електромагнітного поля?
23. Які функції виконують нелінійні локатори?
24. Які багатофункціональні прилади використовують для виявлення засобів зняття інформації?
25. Які методи пошуку радіозакладних пристроїв, побудованих на використанні способу ВЧ-нав'язування ви знаєте?
26. Як використовуються генератори шуму для захисту акустичної інформації?
27. На яких принципах будуються генератори шуму?
28. Які методи та засоби використовуються для виявлення та захисту акустичної інформації від несанкціонованого запису звукозаписувальними пристроями?
29. Які методи та засоби використовуються для захисту електронної та електромагнітної інформації?
30. Які технічні методи та засоби використовуються для захисту письмової інформації?
31. Яким чином принцип системності реалізується у побудові комплексної системи технічного захисту інформації (КС ТЗІ), і чому він є ключовим для забезпечення її ефективності?
32. Які основні етапи проходить об'єкт інформаційної діяльності під час атестації на відповідність вимогам ТЗІ, і які типові помилки допускають під час цього процесу?
33. Які основні технічні канали витоку акустичної інформації виникають у сучасних офісних приміщеннях і які засоби пасивного та активного захисту доцільно застосовувати для їх нейтралізації?
34. Як використання віброакустичних генераторів шуму впливає на ефективність блокування акустичних каналів витоку?
35. Які сучасні радіотехнічні методи (наприклад, нелінійна локація, широкосмугове сканування) використовуються для виявлення закладних пристроїв, і в чому полягають їхні переваги та обмеження?

Рекомендована література: [1-3, 5, 7, 14, 21, 24-25].

ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ

1. Яке визначення має об’єкт технічного захисту інформації?
    а) Будова, приміщення, основний технічний засіб або їх група, що підлягають захисту.
    б) Комп’ютерна мережа установи.
    в) Серверна кімната та всі її складові.
    г) Захищене сховище паперових документів.

2. Яка головна мета технічного захисту інформації?
    а) Запобігання витоку інформації через технічні канали.
    б) Обмеження доступу працівників до інформації.
    в) Видалення всіх даних після їх обробки.
    г) Зменшення обсягу переданої інформації.

3. Що є основним технічним засобом захисту інформації?
    а) Технічний засіб, що обробляє, зберігає або передає закриту інформацію.
    б) Будь-який пристрій для передачі сигналів.
    в) Лише апаратні засоби шифрування.
    г) Засоби електронного документообігу.

4. Яка основна класифікація методів технічного захисту інформації?
    а) Пасивні та активні методи.
    б) Апаратура та програмне забезпечення.
    в) Захист фізичного доступу та мережеві заходи.
    г) Електромагнітні та акустичні методи.

5. Який метод технічного захисту інформації передбачає випромінювання завад?
    а) Активний.
    б) Пасивний.
    в) Фізичний.
    г) Логічний.

6. Що є основним недоліком пасивного захисту інформації?
    а) Не використовує фізичних процесів захисту.
    б) Вимагає великих енергетичних витрат.
    в) Може спричиняти шкідливий вплив на оточення.
    г) Використовується лише у військових об’єктах.

7. Що відноситься до активного методу захисту акустичної інформації?
    а) Генерація маскуючих шумів.
    б) Використання звуконепроникних матеріалів.
    в) Встановлення товстих стін у приміщенні.
    г) Обмеження доступу персоналу.

8. Який спосіб використовується для виявлення технічних каналів витоку акустичної інформації?
    а) Акустичні вимірювання.
    б) Візуальний контроль.
    в) Перевірка рівня вологості повітря.
    г) Контроль температурного режиму.

9. Як можна зменшити можливість зняття інформації за допомогою лазерного випромінювання?
    а) Використання генераторів механічного шуму.
    б) Заклеювання вікон темною плівкою.
    в) Відключення інтернет-з’єднання.
    г) Введення додаткового шифрування.

10. Що є основним елементом будь-якої інтегрованої системи захисту інформації?
    а) Виявлення та блокування потенційних загроз.
    б) Доступ до всіх баз даних.
    в) Фізичний контроль персоналу.
    г) Видалення всіх даних після їх обробки.

11. Який прилад використовується для захисту від витоку інформації через вікна?
    а) Генератор випадкових електромагнітних коливань.
    б) Біометричний сканер.
    в) Система відеоспостереження.
    г) Детектор руху.

12. Як можна захистити вікна приміщення від витоку акустичної інформації?
    а) Встановлення генераторів випадкових електричних коливань.
    б) Відключення електромережі у робочий час.
    в) Покриття вікон світлонепроникною плівкою.
    г) Використання лише спеціального скла.

13. Що є головним принципом комплексного захисту інформації?
    а) Використання кількох взаємопов’язаних підсистем.
    б) Захист лише секретної документації.
    в) Блокування всіх каналів зв’язку.
    г) Приховування апаратних засобів.

14. Чому важливо здійснювати регулярний моніторинг технічного захисту інформації?
    а) Для виявлення та усунення потенційних загроз.
    б) Для економії ресурсів.
    в) Для приховування можливих витоків.
    г) Для ускладнення роботи працівників.

15. Яка основна функція радіочастотних генераторів у системах захисту інформації?
    а) Генерація шумових перешкод для запобігання прослуховуванню.
    б) Запис телефонних розмов.
    в) Аналіз активності співробітників.
    г) Підсилення сигналу мобільного зв’язку.

16. Що таке рівень технічного захисту інформації?

а) Сукупність вимог та норм, що визначають безпеку інформації.

б) Ступінь закритості приміщень установи.

в) Час, необхідний для проникнення до мережі.

г) Кількість шифрованих файлів.

17. Який із наведених методів є пасивним захистом інформації?

а) Екранування електромагнітного випромінювання.

б) Випромінювання завад.

в) Введення контрольованих збоїв.

г) Використання акустичних сигналів.

18. Що є основною метою технічного захисту електронної інформації?

а) Захист від несанкціонованого доступу та витоку даних.

б) Спрощення процесів обробки інформації.

в) Оптимізація програмного забезпечення.

г) Підвищення швидкості передачі даних.

19. Яке з наведених рішень є найбільш ефективним для захисту телефонного зв’язку?

а) Використання пристроїв шифрування голосу.

б) Вимкнення телефонів під час розмов.

в) Перевірка телефонів на наявність додаткових мікрофонів.

г) Використання пристроїв запису розмов.

20. Чому використання активних методів захисту є ефективним для захисту інформації?

а) Вони активно заважають витоку інформації через технічні канали.

б) Вони споживають менше електроенергії.

в) Вони дозволяють працювати без шифрування.

г) Вони не впливають на роботу комп’ютерів.

ТЕМА 9
ВИДИ І ПРОЦЕДУРИ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА РОЗГОЛОШЕННЯ ДЕРЖАВНОЇ ТАЄМНИЦІ

ПЛАН

1. Загальні підстави застосування юридичної відповідальності за розголошення державної таємниці.

2. Кримінальна відповідальність за розголошення державної таємниці. Втрата документів, що містять державну таємницю.

3. Адміністративна відповідальність за порушення режиму державної таємниці.

4. Відповідальність за розголошення державної таємниці у нормах законодавства зарубіжних країн.

1. Загальні підстави застосування юридичної відповідальності за розголошення державної таємниці

Посадові особи та громадяни, винні у:

– розголошенні державної таємниці; втраті документів та інших матеріальних носіїв секретної інформації;

– недодержанні встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

– засекречуванні інформації, зазначеної у Законі 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;

– нехтуванні заходами із забезпечення охорони державної таємниці та відсутності 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 "Про державну таємницю".

2. Кримінальна відповідальність за розголошення державної таємниці. Втрата документів, що містять державну таємницю

Розглядаючи питання кримінальної відповідальності за розголошення державної таємниці, необхідно зупинитися на чіткому визначенні усіх конститутивних ознак складу злочину, передбачених ст. 328 Кримінального

кодексу України. По-перше, суспільна небезпека будь-якого злочину полягає в суттєвій шкоді, яка завдається цим злочином об'єкта кримінально-правової охорони, або у небезпеці завдання такої шкоди. Суспільна небезпечність розголошення державної таємниці досить висока. Практично кожен факт порушення встановлених правил поводження з державною таємницею становить джерело небезпеки.

Як вказується в юридичній літературі, при розголошенні державної таємниці суспільна небезпечність полягає в створенні можливості потрапляння відомостей, що становлять державну таємницю, у розпорядження іноземної розвідки чи інших організацій і осіб, які можуть використати їх на шкоду державі, суспільству чи окремим громадянам. У результаті вчинення цього злочину порушується схоронність секретної інформації: вона стає надбанням сторонніх осіб, які можуть передати ці відомості ще більш широкому колу осіб, у тому числі й ворожим елементам. Таким чином, порушення схоронності державної таємниці створює загрозу заподіяння шкоди національній безпеці України. Розголошення державної таємниці може призвести до людських жертв та інших важких наслідків з великими матеріальними або моральними збитками: дипломатичних ускладнень, науково-технічних і технологічних втрат, загроз життю й волі осіб, які співпрацюють із правоохоронними органами тощо.

Однією з головних ознак складу злочину, передбаченого ст. 328 КК, є предмет цього злочину – інформація, що становить державну таємницю. *Таким чином, у визначенні державної таємниці наявні такі ознаки:*

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. Висновок щодо того, чи є розголошена конкретна інформація державною таємницею, надає згідно із законодавством державний експерт з питань таємниць. Він також визначає ступінь секретності такої інформації і формулює висновок щодо шкоди національній безпеці України в разі її розголошення.

Визначальне значення, таким чином, має не гриф секретності, а дійсний зміст відомостей завдає чи не завдає їх розголошення шкоди національній

безпеці України в тій чи іншій сфері. Тому в усіх випадках посягання на схоронність державної таємниці необхідно мати висновок Державного експерта з питань таємниць, який несе персональну відповідальність за законність і обґрунтованість свого рішення про віднесення інформації до державної таємниці. Цей висновок має бути чітко викладений, уникаючи двозначності, та містити вказівку щодо ступеня секретності оцінюваної інформації, наявності шкоди національній безпеці у разі розголошення такої інформації, а також посилання на конкретний пункт Зводу та відповідного розгорнутого переліку, щоб слідчий, прокурор або суд могли перевірити правильність віднесення інформації до державної таємниці.

Відповідальність за ст. 328 нового КК настає незалежно від характеру відомостей, що становлять державну таємницю, які були розголошені (окрім інформації у сфері оборони у деяких випадках, які ми розглянемо нижче). Це має значення лише для встановлення тяжкості завданої шкоди, тобто ступеня суспільної небезпечності вчиненого злочину й може бути враховано судом при вирішенні питання про призначення винній особі конкретної міри покарання.

Розголошення державної таємниці слід розглядати як таке діяння (дію або бездіяльність) особи, внаслідок якого секретна інформація, що була їй довірена або стала відома у зв’язку з виконанням службових обов’язків, була сприйнята хоча б однією сторонньою особою. Розголошення шляхом активних дій – це будь-яка форма передачі відомостей, які становлять державну таємницю, сторонній особі, що дозволило їй сприйняти такі відомості.

Так, розголошення державної таємниці може відбутися в усній формі (у відкритому публічному виступі лекції, доповіді; у довірчій бесіді; під час розмови чи суперечки в громадському транспорті, на вулиці, в іншому місці в присутності сторонніх осіб тощо), у писемній формі (при листуванні; у відкритих публікаціях; у записах на не облікованих аркушах відомостей, що становлять державну таємницю, і наступній їх втраті і т. ін.), у формі наочної демонстрації чи умисної передачі стороннім особам для передруку, ознайомлення або іншого використання матеріальних носіїв секретної інформації: предметів, об’єктів, документів чи матеріалів, відомості про які становлять державну таємницю.

Розголошення шляхом злочинної бездіяльності – це нехтування належними заходами щодо збереження секретної інформації, у результаті чого стороння особа сприйняла таку інформацію. При цьому "секретоносій", нехтуючи правилами поводження із секретними документами, виробами тощо (через неуважність, безпам'ятність, довірливість), створює умови, за яких стороння особа ознайомилась з державною таємницею, тобто не перешкоджає такому ознайомленню.

Отже, розголошення державної таємниці передбачає обов'язкову наявність у процесі діяння другої сторони сторонньої особи, яка сприймає зазначені відомості. Однак у тексті ст. 328 КК України поняття "стороння особа" відсутнє. Втім дана дефініція набуває значення конститутивної ознаки складу розголошення державної таємниці.

Кримінальна відповідальність настає незалежно від того, скільком стороннім особам стала відома інформація, що становить державну таємницю. Ця обставина може враховуватися судом при вирішенні питання про призначення винному конкретної міри покарання.

Іноді можливі ситуації, коли з причин, які не залежали від волі винного, умисно розголошені ним відомості взагалі не були сприйняті сторонніми особами (внаслідок незнання національної мови, глухоти, сильного сп'яніння тощо). Такі невдалі спроби розголошення державної таємниці слід кваліфікувати також як незакінчений злочин.

Якщо відомості, що становлять державну таємницю, стали відомі стороннім особам при повному дотриманні посадовою особою правил поводження з такими відомостями, відповідальність суб'єкта виключається. Не буде розглядуваного злочину й у тому випадку, якщо саме сприйняття відомостей не було безпосередньо обумовлене фактом порушення встановлених правил поводження з державною таємницею.

Отже, з об'єктивної сторони *розголошення державної таємниці складається з трьох моментів, які потребують обов'язкового встановлення*:

а) порушення певних вимог нормативних актів, які встановлюють порядок поводження з державною таємницею, що виявляється в дії або бездіяльності;

б) сприйняття відомостей, що становлять державну таємницю, сторонньою особою;

в) причинний зв’язок між порушенням винним установлених правил поводження з державною таємницею та їх сприйняттям сторонньою особою.

Суб’єктивна сторона розголошення державної таємниці характеризується як умисною, так і необережною формами вини. Новий кримінальний закон не робить різниці між умисним і необережним розголошенням державної таємниці. Тобто форма вини не впливає на кваліфікацію, а враховується лише при індивідуалізації покарання в межах санкції закону. Однак у порядку подальшого удосконалення кримінального законодавства варто диференціювати кримінальну відповідальність за розголошення державної таємниці залежно від форми вини.

Отже, кримінальній відповідальності за розголошення відомостей, що становлять державну таємницю, підлягає фізична осудна особа, яка досягла на момент скоєння злочину 16-річного віку і має або мала допуск до державної таємниці, а так само взяла на себе письмове зобов’язання щодо збереження (нерозголошення) секретної інформації, довіреної чи такої, що стала відомою у зв’язку з виконанням службових обов’язків.

Крім того, військовослужбовці й прирівняні до них особи за розголошення відомостей не військового характеру, що становлять державну таємницю, які були їм довірені або стали відомі у зв’язку з проходженням служби й виконанням покладених на них обов’язків, також несуть відповідальність за ст. 328 КК України. Хоча відносно цієї категорії осіб у тексті закону пряма вказівка відсутня, однак їх службове становище свідчить про те, що вони також є спеціальними суб’єктами. Однак, якщо військовослужбовець розголошує державну таємницю військового характеру, його діяння за відсутності ознак державної зради слід кваліфікувати за ст. 422 КК. Звільнені в запас чи демобілізовані військовослужбовці за розголошення будь-якої інформації, що становить державну таємницю, підлягають відповідальності за ст. 328 КК України.

3. Адміністративна відповідальність за порушення режиму державної таємниці

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.

Те саме діяння, якщо воно спричинило важкі наслідки, карається позбавленням волі строком від двох до п'яти років.

Об'єкт цього злочину аналогічний об'єктові злочину, передбаченого ст. 328. Предметом злочину є:

а) документи, що містять державну таємницю;

б) інші матеріальні носії секретної інформації, що містять державну таємницю;

в) предмети, відомості про які становлять державну таємницю.

Документ – це передбачена законом матеріальна форма одержання, зберігання, використання і поширення інформації шляхом фіксації її на папері, магнітній, кіно-, відео-, фотоплівці або на іншому носієві. Це можуть бути книги, брошури, рукописи (*наприклад*, дисертації та автореферати дисертацій, дипломні роботи), окремі листи паперу (скажімо, видані для нотаток під час проведення нарад чи іспитів), карти, схеми, плани, фотонегативи та фотознімки кіно та відеострічки, магнітні диски тощо.

До інших матеріальних носіїв секретної інформації можуть бути віднесені не передбачені законом форми зберігання таємної інформації (незареєстровані у встановленому порядку блокноти "чернетки" тощо, в яких зроблено виписки із відповідних документів).

Предмети, відомості про які становлять державну таємницю, – це комплекси, системи, засоби окремі агрегати блоки, вузли, прилади, матеріали,

хімічні продукти, апаратура, устаткування, макети, зразки та інші матеріальні носії інформації, що становить державну таємницю, які не є документами (зразки зброї, військової та спеціальної техніки, обладнання, пальне, сировина тощо).

З об'єктивної сторони цей злочин сформульований як злочин з матеріальним складом і полягає у двох взаємопов'язаних фактах, перший із яких є причиною, а другий – наслідком:

1) порушення особою, якій було довірено матеріальні носії секретної інформації, що містить державну таємницю, або предмети, відомості про які становлять державну таємницю, встановленого законом порядку поводження із ними;

2) втрата зазначених матеріальних носіїв інформації або предметів. Між цими фактами обов'язково має бути безпосередній причинний зв'язок.

Порушення порядку поводження із вказаними матеріальними носіями інформації або предметами містить склад злочину, передбаченого ст. 329, лише у випадку, якщо воно стосувалось порядку, встановленого законом, а не будь-яким іншим нормативним правовим актом, і може полягати в недотриманні:

а) режиму секретності при роботі з відповідними документами чи предметами, неправильна організація обліку таємних предметів (скажімо, передавання їх іншим працівникам без оформлення у відповідних облікових документах), відсутність належної охорони приміщень де зосереджені таємні документи, недотримання належних умов транспортування таких документів (предметів) (*наприклад*, пересилання звичайними засобами поштового зв'язку замість фельд'єгерського чи інших спеціальних засобів зв'язку), робота з таємними документами в умовах, що не гарантують їх збереження (скажімо, у місцях, які не обмежують вільний доступ до них сторонніх осіб);

б) правил таємного діловодства передавання таємних документів на доповідь, ознайомлення чи виконання без належного оформлення, несанкціоноване виготовлення копій таємних документів і т. ін.

4. Відповідальність за розголошення державної таємниці у нормах законодавства зарубіжних країн

Порушення законодавства про державну таємницю, а саме:

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

– *засекречування інформації:*

• про стан довкілля, про 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 і громадянина; про незаконні дії органів державної влади, органів місцевого самоврядування та їх посадових осіб;

• іншої інформації, яка, відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена;

• безпідставне засекречування інформації;

• 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;

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

• невжиття заходів щодо забезпечення охорони державної таємниці та незабезпечення контролю за охороною державної таємниці;

• 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;

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

• невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності, – тягне за собою накладення штрафу на громадян від десяти до тридцяти неоподатковуваних мінімумів доходів громадян і на посадових осіб – від тридцяти до ста неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення з числа передбачених частиною першою цієї статті, за яке особу вже було піддано адміністративному стягненню, – тягне за собою накладення штрафу на громадян від тридцяти до вісімдесяти неоподатковуваних мінімумів доходів громадян і на посадових осіб – від п'ятдесяти до ста п'ятдесяти неоподатковуваних мінімумів доходів громадян. Об'єктом цього правопорушення є суспільні відносини у сфері охорони державної таємниці.

З моменту опублікування Зводу (змін до нього) відомості підлягають охороні з боку держави як такі, що становлять державну таємницю, хоча на цей час вони ще не були матеріалізовані.

Зовнішньою (матеріальною) ознакою віднесення документа, виробу або іншого матеріального носія інформації до предметів, що містять відомості, які становлять державну таємницю, є наданий йому гриф секретності – реквізит матеріального носія таємної інформації, який засвідчує ступінь її секретності ("особливої важливості", "цілком таємно", "таємно"). Строк, протягом якого діє

рішення про віднесення інформації до державної таємниці, встановлюється Державним експертом з питань таємниць, але не може перевищувати для зазначених видів інформації відповідно 5, 10, 30 і років. Проте після закінчення зазначеного строку його може бути подовжено.

Конкретні види інформації, яка належить до державної таємниці, перелічені у Законі України "Про державну таємницю". Ними є інформація у сфері:

а) оборони;

б) економіки, науки і техніки;

в) зовнішніх відносин;

г) у сфері державної безпеки та охорони правопорядку.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності "особливої важливості", "цілком таємно" та "таємно" лише за умови, що вони належать до зазначених чотирьох категорій і їх розголошення завдаватиме шкоди інтересам національної безпеки України.

Забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим звужуватимуться зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

Для кожної держави світу правова охорона державної таємниці є складовим елементом гарантування національної безпеки. Тому доцільно розглянути правове регулювання питань охорони та захисту державної таємниці та відповідальність за розголошення інформації в законодавстві зарубіжних країн, адже пізнаючи право інших країн, ми краще розуміємо своє національне.

Для розгляду цікавими є законодавчі заходи щодо охорони державної таємниці в Великобританії, Франції, Королівстві Іспанія, США, Королівстві Нідерландів (Голландія), Республіці Болгарія. А також, сучасний стан щодо забезпечення охорони державної таємниці в законодавстві пострадянських держав – Азербайджанської Республіки, Республіки Білорусь, Грузії, Латвійської Республіки.

Так, система охорони та захисту таємниць Великобританії базується на законі про державну таємницю, прийнятому ще в 1911 р. До нього було прийнято

ряд поправок в 1920, 1939 і 1988 рр. Переважно їх мета – подальше посилення відповідальності за розголошення державних таємниць. Поправки, прийняті в 1988 р, передбачають переслідування в кримінальному порядку за розголошення відомостей, що стосуються безпеки, розвідки, оборони або міжнародних відносин. Однак обвинувач (держава) повинен довести наявність реальних збитків. Так, при розгляді справи про розголошення інформації про національну безпеку, обвинувач зобов'язаний навести конкретні дані про ослаблення бойової могутності збройних сил. Згідно з доповненнями 1988 р., передбачається також кримінальне переслідування державних службовців, розголосили секретну інформацію, що не забезпечили належного зберігання секретних документів або повідомили кому-небудь відомості про спроби допуску до інформації, яка містить державну таємницю.

Кримінальна відповідальність передбачається і щодо осіб, які не перебувають на державній службі, якщо вони незаконним шляхом отримали офіційний секретний документ, відмовляються повернути його на вимогу владних структур. За розголошення відомостей, що містять державну таємницю, передбачається покарання у вигляді тюремного ув'язнення строком до 2-х років, штрафу або обох покарань одночасно. Уряд Великобританії серйозну увагу приділяє захисту секретних відомостей безпосередньо в кабінеті міністрів. Для цього в 1986 р. були розроблені так звані "Рекомендації членам кабінету міністрів про правила поведінки і дотримання таємниці при виконанні службових обов'язків". Ці особи, вказується в інструкції, повинні підтримувати репутацію англійського уряду і зберігати в таємниці все, що стосується його діяльності. При першому призначенні на посаду (а в деяких випадках – і при повторному) міністри зобов'язані пройти інструктаж з питань забезпечення державної безпеки. Проводять його представники Служби безпеки і контррозвідки. Уряд Великобританії вживає активних заходів щодо запобігання витоку секретних відомостей через засоби масової інформації. При цьому враховуються не тільки вимоги закону про державну таємницю, а й установки іншого документа – цивільного (не кримінального) закону про конфіденційність. Він, зокрема, передбачає наступну процедуру: уряд може домогтися через суд

першої інстанції рішення про заборону публікації шляхом окремої постанови судді без громадських слухань, часто навіть без оповіщення іншого боку і запрошення осіб, проти яких направлено рішення. При цьому може бути заборонена публікація матеріалів або книги не тільки в Великобританії, а в будь-якій країні світу.

Правові основи діяльності щодо охорони державних таємниць у Франції були закладені в 1960 р., коли держава увійшла до "ядерного клубу" – групи ядерних держав. 4 липня 1960 року був прийнятий указ про таємниці, в якому давалося досить широке трактування поняття, що визначає секретність відомостей.

Згодом, уже в 1972 р., був прийнятий закон про обмеження доступу сторонніх осіб на об'єкти, що охороняються. Причому дія цього закону поширювалася на будь-яку галузь. У 1978 р. парламент Франції прийняв закон, який проголошував право доступу громадян до адміністративних документів. Незважаючи на демократичний в цілому характер цього законодавчого акту, він має ряд положень, що обмежують допуск приватних осіб до службової інформації. Так, ст. 6 містить перелік категорій адміністративних документів, ознайомлення з якими заборонено для осіб, які не мають спеціального допуску.

Серед таких документів, зокрема, "секретні відомості про наради уряду, секретні відомості про національну оборону і зовнішню політику" та інші категорії документів, що містять промислові, комерційні і приватні таємниці. Закон передбачає, що всі міністерства повинні визначити категорії відомостей, що не підлягають розсекреченню і розголошенню на будь-яку галузь.

У США питання, пов'язані з охороною державної таємниці, розроблені й закріплені в ряді нормативно-правових актів (закони, президентські виконавчі накази, інструкції). У 1966 р. був прийнятий закон про свободу інформації. У ньому окреслено досить широке коло питань, що становлять державну таємницю і не підлягають розголошенню.

Серед них – *відомості, що стосуються національної оборони і зовнішньої політики США*:

– інформація, що стосується кадрової політики того чи іншого державного

відомства, торгових, комерційних і фінансових таємниць;

– слідчі документи, розголошення яких може перешкодити здійсненню правоохоронних заходів чи справедливому судовому розгляду;

– особисті справи, медичні карти та інші досьє, розкриття яких було б порушенням постулату недоторканості особи;

– відомості, що розкривають особистість секретного джерела інформації. Федеральні закони (“Про національну безпеку від 1947 р.”, “Про атомну енергію 1954 р.”, “Про спостереження за іноземною розвідкою 1978 р.”, “Про внутрішню безпеку 2002 р.”) безпосередньо стосуються захисту державної таємниці.

Особливу увагу адміністрація США надає обмеження порядку доступу до державних таємниць. Для цього послідовно втілюються рекомендації комітету конгресу з розвідки про значне скорочення кола співробітників урядових установ, що мають доступ до секретної інформації. Особливою віхою на цьому шляху можна вважати прийнятий в 1985 р закон США про покарання за розголошення секретної інформації, що передбачає штраф у 15 тисяч доларів або 3 роки тюремного ув’язнення, або і те й інше одночасно. Продовжує діяти директива міністерства оборони 1984 р. “Про нерозголошення важливої технічної інформації”, згідно з якою винуватцю загрожує тюремне ув’язнення або штраф в 1 мільйон доларів США або на суму, яка в п’ять разів перевищує вартість збитку, завданого розголошенням інформації. Проводячи аналогію з українським законодавством, слід зазначити, що ч. 1 ст. 328 КК України передбачає за розголошення державної таємниці можливість покарання у вигляді позбавлення волі на строк від двох до п’яти років. Можна зробити висновок, що в США активно ведеться боротьба з витоком таємної державної інформації.

В США все більше уваги приділяється так званій контррозвідувальній освіті населення: вихованню відповідальності за збереження секретів, підвищенню пильності і вмінню давати оцінку діям, які становлять загрозу національній безпеці, оволодіння навичками роботи з документами, що мають гриф “секретно”, “цілком секретно”. У країні організовано спеціальні телефонні лінії, за якими можна безкоштовно повідомити в спецслужби про факти

порушення режиму безпеки або про свої підозри щодо товаришів по службі.

У Голландії відповідальність за незбереження державної таємниці встановлена на рівні кримінального закону. Зокрема, КК містить 4 статті, в яких передбачена кримінальна відповідальність за злочини в сфері охорони державної таємниці. Ці злочини містяться в розділі I КК "Злочини проти безпеки держави". Кримінальна відповідальність встановлена за надання або створення доступу до секретної інформації:

а) необережне надання або створення доступу до секретної інформації;

б) кримінальній відповідальності підлягає також особа, що навмисне розпорядилася секретною інформацією або здійснює будь-яку діяльність з метою незаконного отримання такої інформації (ст. 98).

У КК Королівства Іспанія в розділі III "Злочини проти національної оборони" розділу XXIII книги II передбачені злочини, пов'язані з державною таємницею. Серед них дії, невідомі вітчизняному законодавству: наприклад, ст. 598 встановлює відповідальність за надання, видачу, перекручення чи знищення закритої або конфіденційної інформації в сфері національної безпеки чи оборони. Ст. 600 – за відтворення без належних повноважень планів або військової документації, ст. 601 – за необережне поширення секретної або закритої інформації, ст. 602 – за поширення секретної або закритої інформації, пов'язаної з ядерною енергією, ст. 603 – за знищення, псування, підробку або розкриття без повноважень закритої або секретної кореспонденції чи документації в сфері національної оборони. Можна зробити висновок, що кримінальний закон Іспанії диференційовано підходить до питання про покарання різних категорій злочинних посягань алежно від виду секретної інформації.

Глава XII КК Республіки Болгарія, присвячена злочинам проти основ обороноздатності держави, складається з двох розділів, перший називається. "Злочини проти державної таємниці", а другий – "Злочини проти несення військової служби". До злочинів проти державної таємниці болгарський законодавець відносить не тільки злочини, що посягають на відносини у сфері охорони державної таємниці (ст. 351 – поширення відомостей, що становлять державну таємницю, ст. 358 – втрата документів, видань або матеріалів, що

містять державну таємницю, ст. 359 – розголошення державної таємниці через необережність), але і злочини, які посягають на відносини, пов'язані з охороною відомостей військового, господарського чи іншого характеру, що не містять державної таємниці (ст. 360), а також відомості про діяльність служб безпеки, поліції щодо притягнення до відповідальності штатних і позаштатних таємних співробітників (ч. 1 ст. 357 КК).

Таким чином, кримінальне законодавство Республіки Болгарія найбільш повно і широко підходить до охорони державної таємниці.

На пострадянському просторі склалася інша ситуація з охороною державної таємниці.

Відповідні законодавчі акти про злочини, пов'язані з державною таємницею є і в КК Азербайджанської Республіки. Глава 31 "Злочини проти основ конституційного ладу державної влади" включено більшість злочинів, відповідальність за які передбачена і в КК АР.

У Республіці Білорусь норми, що передбачають порядок використання і захисту державної таємниці, встановлюються Законом "Про державні секрети", а відповідальність за злочини в сфері охорони державної таємниці передбачена в главі 32 КК "Злочини проти держави". До таких злочинів білоруський законодавець відносить умисне розголошення державної інформації, розголошення державної таємниці з необережності.

Схожа ситуація справ і в КК Латвійській Республіці. Закон "Про державну таємницю" регулює загальні питання її збереження, а в главі X "Злочини проти держави" Особливої частини кримінального закону включені норми, що передбачають відповідальність за умисне розголошення державної таємниці (ст. 94) та розголошення державної таємниці з необережності (ст. 95). Крім цих злочинів, кримінальний закон Латвійської Республіки складають і такі злочини, як,

– "Розголошення відомостей, що не підлягають поширенню" (ст. 329);

– "Розголошення відомостей, що не підлягають розголошенню, після звільнення з посади" (ст. 330).

У КК України, подібні діяння також передбачені, хоча віднесення їх латвійським законодавцем до злочинів у сфері охорони державної таємниці не

зовсім доцільно.

Якщо узагальнити положення кримінального закону країн пострадянського простору у питаннях кримінальної відповідальності за розголошення державної таємниці можна прослідкувати таке.

Таблиця 1

Перелік кримінально-правових норм, що передбачають відповідальність за розголошення державної таємниці в країнах пострадянського простору

№	*Країна*	*Норма кримінального закону*
1.	Республіка Білорусь	Глава 33. Злочини проти порядку управління, ст. 373.Умисне розголошення державної таємниці
3.	Республіка Молдова	Глава XVII. Злочини проти публічної влади та безпеки держави, ст. 344. Розголошення державної таємниці
4.	Естонська Республіка	Глава друга. Злочини проти держави, ст. 73. Розголошення державної таємниці
5.	Литовська Республіка	XVI Розділ. Злочини проти незалежності держави, цілісності території та конституційного ладу, ст. 125. Розголошення державної таємниці
6.	Латвійська Республіка	Глава X. Злочини проти держави, ст. 94.Умисне розголошення державної таємниці
7.	Грузія	Розділ 11. Злочини проти держави, Глава XXXVII. Злочини проти основ конституційного ладу та безпеки Грузії, ст. 320. Розголошення державної таємниці
8.	Азербайджанська Республіка	Розділ 3. Злочини проти державної влади, Розділ тридцять перший. Злочин проти основ конституційного ладу та безпеки держави, ст. 284. Розголошення державної таємниці
9.	Республіка Вірменія	Розділ 11. Злочини проти державної влади, Глава 28. Злочини проти основ конституційного ладу і безпеки держави, ст. 306. Розголошення державної таємниці
10.	Республіка Казахстан	Глава 5. Злочини проти основ конституційного ладу та безпеки держави, ст. 172. Незаконне отримання, розголошення державних секретів
11.	Узбекістан	Глава IX. Злочини проти республіки Узбекистан, ст. 162. Розголошення державних секретів

12.	Республіка Таджикистан	Розділ XIII. Злочини проти державної влади, Глава 29. Злочини проти основ конституційного ладу та безпеки держави, ст. 311. Розголошення державної таємниці
13.	Киргизька Республіка	Розділ X. Злочини проти державної влади, Глава 29. Злочини проти основ конституційного ладу та безпеки держави, ст. 300. Розголошення державної таємниці
14.	Туркменістан	Розділ IX. Злочини проти держави, Глава 22. Злочини проти держави, ст. 179. Розголошення державної таємниці

Кримінальні кодекси Республіки Білорусь (ст. 373), Республіки Молдова (ст. 344), Азербайджанської Республіки (ст. 284), Республіки Казахстан (ст. 172), Республіки Узбекистан (ст. 162), Республіки Таджикистан (ст. 311), Республіки Вірменія (ст. 306), Киргизької Республіки (ст. 300), Туркменістану (ст. 179) конкретно вказують на те, що відповідальність за розголошення державної таємниці лежить на особі, якій ці відомості були довірені або стали відомі по службі або роботі. Іншими словами, мова йде про наявність у цих складах злочинів спеціального суб'єкта, ознаки якого безпосередньо прописані в диспозиції тієї чи іншої норми. До речі, такий підхід щодо встановлення особи, яка нестиме кримінальну відповідальність за розголошення державної таємниці, дістався як спадщина всім цим кримінальним законодавствам від кримінального законодавства Радянського Союзу. При цьому законодавець зберіг цей підхід і в чинному кримінальному законі України. Не так одностайно розглядають проблему розголошення державної таємниці кримінальні закони країн, що також входили до складу Радянського Союзу, але на сучасному етапі є членами Європейського Союзу, а саме – Естонська Республіка, Литовська Республіка та Латвійська Республіка. Так, якщо дві останні зберегли традиційний підхід до передбачення кримінальної відповідальності за розголошення державної таємниці, що існував у радянському кримінальному законодавстві (кримінальний кодекс Литовської Республіки – ст. 125, кримінальний кодекс Латвійської Республіки – ст. 94), то кримінальний закон Естонської Республіки передбачає зовсім інші ознаки складу злочину розголошення державної таємниці.

По-перше, мова в ньому йдеться про відомості, що піддаються розголошенню, різних ступенів секретності (в ч. 1 ст. 73 “Конфіденційно”, в ч. 2 ст. 73 – “Таємно” та в ч.3 ст. 73 – “Цілком таємно”).

По-друге, ця кримінально-правова норма не передбачає у своїй структурі наявності будь-яких спеціальних ознак суб’єкта злочину, тобто мова йде про вчинення суспільно небезпечного діяння загальним суб’єктом – будь-ким.

По-третє, суспільно небезпечне діяння передбачено не тільки у формі розголошення певних відомостей, а й передбачається у формі видання незаконного дозволу на доступ до відомостей, що становлять державну таємницю.

Дещо по-іншому розглядає проблему розголошення державної таємниці Кримінальний кодекс Грузії. У Грузії правовідносини щодо захисту державної таємниці регулюються Законом Грузії “Про державну таємницю”. У КК Грузії норми, що передбачають відповідальність за злочини в сфері охорони державної таємниці, передбачені розділом XXXII “Злочини проти основ конституційного ладу і безпеки Грузії” розділу 11 “Злочини проти держави”. Грузинський законодавець до таких злочинів відносить розголошення державної таємниці (ст. 320 КК) і порушення порядку дотримання державної таємниці (ст. 321 КК).

На відміну від переважної більшості кримінальних законів, що розглянуті, розголошення державної таємниці відповідно до положень ст. 320 КК Грузії здійснюється особою, якій ця таємниця була відома або довірена на підставі свого службового становища. Тобто, не просто довірені або стали відомі у зв’язку з виконанням службових обов’язків, як це передбачено ст. 328 КК України, а як зазначено раніше – державна таємниця відома цій особі. Це певною мірою відрізняється одне від одного. Якщо, у випадку з кримінальним законодавством України, закон наголошує на певній ситуації, внаслідок якої особа володіє державною таємницею – довірена або стала відома у зв’язку з виконанням службових обов’язків, то грузинського законодавця не цікавить джерело отримання особою відомостей, що утворюють державну таємницю. Вони наголошують на тому, що особі відома ця інформація. При цьому як вона стала їй відомою, ніхто не наголошує.

Іншими словами, особа може будь-яким способом отримати таку інформацію (почути з розмови інших осіб, довідатись із друкованих або електронних джерел тощо) і усвідомлюючи, що вона, тобто інформація, є державною таємницею, розголосити її. Це, з позиції кримінального законодавства Грузії, є розголошенням державної таємниці. Формулювання таким чином кримінально-правової норми є певною мірою некоректним. Річ полягає в тім, що узагальненість ситуації, на відміну від інших кримінально-правових норм розглянутих раніше кримінальних кодексів, може призводити до ускладнень правозастосування, а саме – як на практиці встановити факт усвідомлення особою віднесення відомостей до державної таємниці, якщо вона не зобов'язана знати, яка інформація, відповідно до чинного законодавства, має статус таємної.

Інша річ, коли грузинський законодавець передбачає альтернативну ситуацію володіння особою державною таємницею – вона довірена особі на підставі її службового становища. У цій ситуації, логіки притягнення особи до кримінальної відповідальності, а також побудови кримінально-правової норми не порушено.

Кожна держава з метою захисту інформації, що містить державну таємницю, формує систему її охорони та спеціального захисту. Державна таємниця як вид таємниці, що включає встановлену законом і захищається державою інформацію в області військової, економічної, зовнішньополітичної, розвідувальної, контррозвідувальної діяльності, доступ до якої обмежується в інтересах безпеки держави, присутній на рівні закону в кожній з розглянутих держав. Закони держав чітко встановлюють види і містять перелік відомостей, які відносяться до державної таємниці.

Одночасно слід зазначити, що в кримінальному законодавстві розглянутих держав відсутній єдиний підхід щодо визначення злочинних діянь у сфері охорони державної таємниці. Але при цьому її охорона передбачена в різних розділах Особливої частини кримінальних кодексів держав.

СЕМІНАРСЬКЕ ЗАНЯТТЯ
ТЕМА 9
ВИДИ І ПРОЦЕДУРИ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА РОЗГОЛОШЕННЯ ДЕРЖАВНОЇ ТАЄМНИЦІ

План семінарського заняття

1. Загальні підстави застосування юридичної відповідальності за розголошення державної таємниці.
2. Кримінальна відповідальність за розголошення державної таємниці.
3. Втрата документів, що містять державну таємницю.
4. Адміністративна відповідальність за порушення режиму державної таємниці.
5. Відповідальність за розголошення державної таємниці у нормах законодавства зарубіжних країн.

Ключові поняття та терміни: державна таємниця, розголошення державної таємниці, кримінальна відповідальність, адміністративна відповідальність, дисциплінарна відповідальність, втрата секретних документів, умисне розголошення, необережне розголошення, режим державної таємниці, посадова особа, обмежений доступ, таємна інформація, зарубіжне законодавство у сфері державної таємниці, захист секретної інформації, правопорушення, санкції, покарання.

Завдання для самостійної роботи над темою

Завдання 1. Опрацювати теоретичний матеріал теми 9 дистанційного курсу “Система охорони державної таємниці” у Віртуальному університеті ЛДУ БЖД.

Завдання 2. Користуючись рекомендованою літературою та теоретичним матеріалом лекції, самостійно опрацювати та розв’язати ситуаційні завдання.

Ситуаційне завдання 1. Співробітник підприємства залишив секретний документ у громадському місці, у результаті чого він був знайдений сторонніми

особами. Яка форма юридичної відповідальності настає і які фактори вплинуть на її суворість?

Ситуаційне завдання 2. Посадова особа під час інтерв'ю журналісту розповіла деталі про секретний проект, не усвідомлюючи, що ця інформація має гриф "Таємно". Як класифікувати таке порушення та які наслідки воно тягне?

Ситуаційне завдання 3. У процесі перевірки виявлено, що керівник підрозділу систематично допускає порушення правил зберігання документів із державною таємницею. Який вид відповідальності може бути застосований і чи можливе одночасне притягнення до кількох видів?

Ситуаційне завдання 4. Громадянин України, маючи допуск до державної таємниці, виїхав за кордон та передав відомості іноземній компанії. Які норми кримінального законодавства передбачають відповідальність у цій ситуації?

Завдання 3. Користуючись рекомендованою літературою та теоретичним матеріалом лекції, підготувати аргументи для обговорення дискусійних тем.

Дискусійні теми:

– Чи повинна відповідальність за необережне розголошення державної таємниці бути такою ж суворою, як за умисне?

– Які відмінності у підходах до покарання за розголошення державної таємниці між Україною та провідними зарубіжними країнами (США, Німеччина, Франція)?

– Як забезпечити баланс між свободою слова та необхідністю захисту державної таємниці?

ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ТА ПЕРЕВІРКИ ЗНАНЬ

1. Назвіть загальні підстави застосування юридичної відповідальності за розголошення державної таємниці.
2. Перерахуйте конституційні ознаки складу злочину, передбаченого ст. 328 Кримінального кодексу України.
3. Наведіть ознаки, наявні у визначенні державної таємниці.
4. Назвіть умови та наслідки розголошення державної таємниці.
5. Окресліть відповідальність при втраті документів, що містять державну таємницю.
6. Адміністративна відповідальність за порушення режиму державної таємниці.
7. Які дії або бездіяльність відносяться до порушення законодавства про державну таємницю?
8. Відповідальність за розголошення державної таємниці у нормах законодавства Великобританії.
9. Відповідальність за розголошення державної таємниці у нормах законодавства Франції.
10. Відповідальність за розголошення державної таємниці у нормах законодавства США.
11. Відповідальність за розголошення державної таємниці у нормах законодавства Голландії.
12. Відповідальність за розголошення державної таємниці у нормах законодавства Королівства Іспанія.
14. Відповідальність за розголошення державної таємниці у нормах законодавства Республіки Болгарія.
15. Відповідальність за розголошення державної таємниці у нормах законодавства Азербайджанської Республіки.
16. Відповідальність за розголошення державної таємниці у нормах законодавства Латвійській Республіці.
17. Наведіть перелік кримінально-правових норм, що передбачають відповідальність за розголошення державної таємниці в країнах пострадянського простору.

Рекомендована література: [1-3, 5, 7, 21, 24-25].

ТЕСТОВІ ПИТАННЯ ЗА ТЕМОЮ ЛЕКЦІЇ

1. Що враховується при визначенні ступеня суспільної небезпечності злочину?
   а) Важкість завданої шкоди.
   б) Місце скоєння злочину.
   в) Політична ситуація в країні.
   г) Кількість свідків злочину.

2. Яка роль державного експерта з питань таємниць при кваліфікації злочину?
   а) Формує висновок про шкоду розголошення.
   б) Здійснює досудове розслідування.
   в) Контролює доступ до архівів.
   г) Розробляє державні стратегії.

3. В якому випадку слід вважати розголошення завершеним злочином?
   а) При сприйнятті інформації сторонньою особою.
   б) При створенні загрози витоку інформації.
   в) Після втрати документів.
   г) Після публікації матеріалів у ЗМІ.

4. Хто несе відповідальність за порушення вимог до збереження державної таємниці під час міжнародного співробітництва?
   а) Посадові особи та громадяни.
   б) Іноземні делегації та групи.
   в) Представники громадських організацій.
   г) Журналісти зі спецдопуском.

5. Хто може бути спеціальним суб’єктом злочину за статтею 328 КК України?
   а) Особа з допуском до державної таємниці.
   б) Будь-який громадянин України.
   в) Представник дипломатичної служби.
   г) Іноземний громадянин без реєстрації.

6. Яке порушення передбачає відповідальність за статтею 328 Кримінального кодексу України?
    а) Розголошення державної таємниці.
    б) Пошкодження державного майна.
    в) Розголошення комерційної таємниці.
    г) Умисне знищення архівів.

7. Яка форма вини враховується при індивідуалізації покарання за розголошення державної таємниці?
    а) Умисна або необережна форма вини.
    б) Суто умисна форма вини.
    в) Суто необережна форма вини.
    г) Відсутність вини.

8. Яка з форм вчинення розголошення державної таємниці є прикладом активної дії?
    а) Озвучення відомостей у громадському місці.
    б) Невжиття заходів безпеки.
    в) Забуття пароля до секретного носія.
    г) Перевищення службових повноважень.

9. Яке покарання передбачене за вчинення злочину без вини?
    а) Відповідальність не настає.
    б) Арешт до одного року.
    в) Адміністративний штраф.
    г) Суспільно корисні роботи.

10. Яким є основний критерій сторонньої особи?
    а) Відсутність доступу до секретної інформації.
    б) Незнання української мови.
    в) Психологічний стан підозрюваного.
    г) Проживання за кордоном.

11. Кого вважають сторонньою особою згідно з поняттям “розголошення державної таємниці”?
    а) Осіб без права доступу до відомостей.
    б) Військовослужбовців.
    в) Посадових осіб з допуском.
    г) Суддів та прокурорів.

12. Що є обов’язковою ознакою складу злочину розголошення державної таємниці?
    а) Сприйняття інформації сторонньою особою.
    б) Встановлення авторства документа.
    в) Порушення закону про вибори.
    г) Наявність секретного сховища.

13. У якому випадку не настає кримінальна відповідальність за розголошення державної таємниці?
    а) Якщо відомості не були сприйняті сторонньою особою.
    б) Якщо відомості були передані усно.
    в) Якщо інформація містила гриф таємності.
    г) Якщо було відсутнє письмове зобов’язання.

14. Що має бути вказано у висновку державного експерта?
    а) Пункт Зводу відомостей.
    б) Кількість сторінок у документі.
    в) Назва установи-розробника.
    г) Дата створення інформації.

15. Як визначають ступінь секретності розголошеної інформації?
    а) За висновком державного експерта.
    б) За рішенням працівника служби безпеки.
    в) За змістом документа.
    г) За грифом на матеріальному носії.

16. До якого віку настає кримінальна відповідальність за розголошення держтаємниці?
    а) З шістнадцяти років.
    б) З вісімнадцяти років.
    в) З двадцяти одного року.
    г) З сімнадцяти років.

17. Яка форма вини визначає кримінальну відповідальність?
    а) Як умисна, так і необережна.
    б) Лише умисна.
    в) Лише необережна.
    г) Наявність обставин, що пом’якшують вину.

18. Який зв’язок є обов’язковим для складу злочину?
    а) Причинний зв’язок між порушенням правил і сприйняттям.
    б) Тимчасовий зв’язок між особами.
    в) Територіальний зв’язок із місцем зберігання інформації.
    г) Культурний зв’язок між фігурантами справи.

19. Коли особа визнається винною у розголошенні таємниці?
    а) Якщо передала інформацію сторонній особі.
    б) Якщо спілкувалася з іноземцями.
    в) Якщо зберігала інформацію вдома.
    г) Якщо не мала при собі документа.

20. У якій формі може бути реалізоване розголошення державної таємниці?
    а) У письмовій, усній або наочній формі.
    б) Лише у письмовій формі.
    в) Через технічні засоби зв’язку.
    г) Через втрату документа у транспорті.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Конституція України від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. 1996 р. № 30.
2. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 8073-X.
3. Кримінальний кодекс України: Закон України від 05.04.200 р. 1 № 2341-III.
4. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651-VI.
5. Про внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах": Закон України від 31.05.2005 р. № 2594-IV.
6. Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави: Закон України від 19.06.2003 р. № 975-IV.
7. Про державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV // Відомості Верховної Ради України. – 2006. – № 30.
8. Про державну таємницю: Закон України (із змінами і доповненнями, внесеними Законом України від 21.09.1999 р. № 1079-XIV). *Відомості Верховної Ради України*. 1999. № 49.
9. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI.
10. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.1992 р. № 2782-XII.
11. Про захист інформації в автоматизованих системах "*Закон* України" від 05.07.1994 р.
12. Про захист інформації в інформаційно-телекомунікаційних системах"*Закон* України".
13. Про захист персональних даних: Закон України від 1.06.2010 р. № 2297-IV.
14. Про інформацію. Закон України від 2.10.1992 р. № 2657-XII.

15. Про контррозвідувальну діяльність: Закон України від 26.12.2002 р. № 374-IV.
16. Про науково-технічну інформацію: Закон України від 25.06.1993 р. № 3322-XII.
17. Про Національний архівний фонд та архівні установи: Закон України від 24.12.1993 р. № 3814-XII.
18. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII.
19. Про Національну поліцію: Закон України від 2.07.2015 р. № 580-VIII.
20. Про Національну систему конфіденційного зв'язку: Закон України від 10.012002 р. № 2919-111.
21. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII.
22. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 р. № 183/98-ВР.
23. Про розвідувальні органи України: Закон України від 22.03.2001 р. № 2331-III.
24. Про Службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII. Відомості Верховної Ради України. 1992. № 27.
25. Граничні тарифи на послуги конфіденційного зв'язку, які надаються споживачам у Національній системі конфіденційного зв'язку. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 07.08.2013 р. № 420.
26. *Державний* стандарт України ДСТУ 33 96.0-96. Захист інформації. Технічний захист інформації. Основні положення.
27. *Державний* стандарт України ДСТУ 33 96.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
28. *Державний* стандарт України ДСТУ 33 96.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
29. *Державний* стандарт України ДСТУ 3859–99. Засоби інженерно-технічного укріплення та захисту об'єктів. Терміни та визначення.

30. Звід відомостей, що становлять державну таємницю затверджено наказом Служби безпеки України 12.08.2005 р. № 440, зареєстровано в Міністерстві юстиції України 17.08.2005 р. за № 902/11182
31. *Звід* відомостей, що становлять державну таємницю України (ЗВДТ-2000): Затв. наказом голови СБУ від 01.03.2001 р. № 52, зареєстровано в Міністерстві юстиції України 22.03.2001 р. № 264/545511.
32. Інструкцію про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні. Затверджено наказом Генеральної прокуратури, МВС, СБУ, Адміністрації ДПСУ, Міністерства фінансів та Міністерства юстиції України від 16.11.2012 р. № 114/1042/516/1199/936/1687/5.
33. Інструкція про порядок відбору та передачі секретних документів на архівне зберігання. Затверджено наказом Державного комітету України з питань державних секретів та технічного захисту інформації та Головного архівного управління при Кабінетові Міністрів України від 03.03.1997 р. № 25/7.
34. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави. Затверджено постановою Кабінету Міністрів України від 27.11.1998 р. № 1893.
35. Інструкція про порядок погодження органами Служби безпеки України призначення особи на посаду заступника керівника підприємства з питань режиму, начальника режимносекретного органу, його заступника, працівника, на якого покладаються обов’язки щодо забезпечення режиму секретності, а також керівника секретного архівного підрозділу підприємства. Затверджено наказом голови СБУ від 08.05.2015 р. № 306.
36. *Інструкція* щодо умов і правил здійснення діяльності у галузі технічного захисту інформації та контролю за їх дотриманням: Наказ Державної служби України з питань технічного захисту інформації від 23.05.1994 р. № 46.
37. *Наказ* Державного комітету України з питань державних секретів та технічного захисту інформації від 9.02.1998 р. № 23 “Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності”.

38. Наказ МВС України № 059 від 14.06.1998 р. “Про організацію та виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України”.
39. НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”.
40. Положення про організацію роботи архівів. Затверджено наказом Міністерства юстиції України 27.05.2015 р. № 797/5.
41. Положення про порядок здійснення криптографічного захисту інформації в Україні. Затверджено Указом Президента України від 22.05.1998 р. № 505//98.
42. Положення про порядок підготовки документів щодо передачі державної таємниці іноземній державі чи міжнародній організації. Затверджено Указом Президента України від 14.12.2004 р. № 1483/2004.
43. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб: Наказ ДСТСЗІ СБУ від 23.02.2002 р.№ 9.
44. Порядок здійснення заходів з охорони державної таємниці під час проведення секретних науково-дослідних та дослідно-конструкторських робіт. Затверджено постановою КМУ від 17.07.2003 р. № 1082.
45. Порядок організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях. Затверджено постановою Кабінету Міністрів України від 18.12.2013 р. № 939.
46. Постанова Кабінету Міністрів України “Концепція технічного захисту інформації в Україні” від 8.10.1997 р. № 1126.
47. Постанова Кабінету Міністрів України “Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах” від 16.02.1998 р. № 180.
48. Постанова Кабінету Міністрів України “Про затвердження “Порядку організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях” від 02.10.2003 р. № 1561-12.

49. Постанова Кабінету Міністрів України “Про Положення про порядок видачі суб’єктам підприємницької діяльності спеціальних дозволів /ліцензій на здійснення окремих видів діяльності” від 17.05.1994 р. № 316.
50. Правила поводження та забезпечення охорони інформації НАТО з обмеженим доступом в Україні. Затверджено наказом СБУ від 09.06.2002 р. № 177/ДСК.
51. Про види, розміри і порядок надання компенсації громадянам у зв’язку з роботою, яка передбачає доступ до державної таємниці: постанова КМУ від 15.06.1994 р. № 414.
52. Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ Служби Безпеки України від 12.08.2005 р. № 440.
53. Про затвердження зобов’язання громадянина України у зв’язку з допуском до державної таємниці та анкети для оформлення допуску до державної таємниці: наказ голови Служби безпеки України від 18.07.2001 р. № 190.
54. Про затвердження Концепції технічного захисту інформації в Україні: постанова КМУ від 8.10.1997 р. № 1126.
55. Про затвердження Переліку психічних захворювань (розладів), які можуть завдати шкоди охороні державної таємниці і за наявності яких допуск до державної таємниці громадянинові не надається. Затверджено наказом Міністерства охорони здоров’я та Служби безпеки України від 13.05.2002 р. № 174/136.
56. Про затвердження Положення про державну експертизу в сфері технічного захисту інформації: Наказ ДСТСЗІ СБУ від 29.12.1999 р. № 62.
57. Про затвердження Положення про експертні комісії з питань державної таємниці: наказ Служби безпеки України від 14.12.2004 р. № 696.
58. Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою Кабінету Міністрів України від 16.02.1998 р. № 180.

59. Про затвердження Положення про умови зберігання документів Національного архівного фонду. Затверджено наказом Міністерства юстиції України від 02.03.2015 р. № 296/5.
60. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою КМУ від 29.03.2006 р. № 373.
61. Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях. Затверджено наказом Міністерства юстиції України від 18.06.2015 р. № 1000/5.
62. Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць. Затверджено Указом Президента України від 01.12.2009 р. № 987/2009.
63. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.1999 р. № 1229/99.
64. Про Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства. Затверджено Указом Президента України від 17.07.2006 р. № 621/2006.
65. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229.
66. Про порядок виїзду з України і в'їзду в Україну громадян України: Закон України від 21.01.1994 р. № 3857-XII.
67. Про проведення експертизи цінності документів: постанова КМУ від 8.08.2007 р. № 1004.
68. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію. Затверджено постановою КМУ від 19.10.2016 р. № 736.
69. Типове положення про експертну комісію державного органу, органу місцевого самоврядування, державного і комунального підприємства, установи та організації. Затверджено наказом Міністерства юстиції України 19.06.2013 р. № 1227/5.

70. Типове положення про секретний архівний підрозділ державного органу, органу місцевого самоврядування, підприємства, установи, організації. Затверджено наказом Міністерства юстиції України 12.02.2015 р. № 167/5/104.
71. Указ Президента України “Положення про технічний захист інформації в Україні” від 27.09.1999 р. № 1229/99.
72. Yara O. (2022). Features of criminal liability for disclosure of information constituting a state secret in Ukraine and foreign countries: comparative legal analysis. Law. Human. Environment, (№ 2), DOI 10.31548/law2022.02.009
73. Адабаш О. В. Становлення системи охорони державної таємниці в незалежній Україні (законодавче забезпечення). Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція. 2014. № 11, т. 1. С. 174–177.
74. Архипов О. Є., Ворожко В. П. Щодо методики реалізації процедури віднесення інформації до секретної. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2008. № 2 (17). С. 11–16.
75. Архипов О. Є., Муратов О. Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою: монографія. К.: Наук.-вид. відділ НА СБ України, 2011. – 195 с.
76. Архипов О. Є., Бородавко І. Т., Ворожко В. П. Оцінювання ефективності системи охорони державної таємниці [Монографія]. Київ: Науково-видавничий відділ Національної академії Служби безпеки України. Київ : Наук.-вид. від. НА СБ України, 2007, 63 с.
77. Болдир С. В. Реформування системи охорони державної таємниці: правові аспекти. Інформація і право. 2018. № 1 (24). С. 112–120.
78. Нормативне забезпечення інформаційної безпеки. Головань С. М. Петров О. С., Хорошко В. О., Чирков Д. В., Щербак Л. М. За ред. проф. В. О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.
79. Грищенко І. В. Досвід країн Східної Європи у сфері охорони державної таємниці. Порівняльно-аналітичне право. 2015. № 4. С. 19–22.

80. Грищенко І.В. Механізм міжнародного співробітництва у сфері охорони державної таємниці між Україною та Єврепейським Союзом. Visegrad Journal on Human Rights. 2016. № 2/1. С. 34–38.
81. Державна та комерційна таємниця. Нормативна-правове регулювання / Роїна О. М. – К.: КНТ, 2006. – 424 с. ISBN 966-373-111-7
82. Державна таємниця // Енциклопедія сучасної України: у 30 т/ ред. кол. І. М. Дзюба [та ін.]; НАН України, НТШ, Координаційне бюро енциклопедії сучасної України НАН України. – К., 2003–2019. – ISBN 944-02-3354-X.
83. Державна таємниця // Митна енциклопедія: у2т./ І. Г. Бережнюк (відп. ред.) та ін. – Хм.: ПП Мельник А. А., 2013. – Т.1: А – Л. – 47 с. – ISBN 978-617-7094-09-7.
84. Державна таємниця як складова національної безпеки України: охорона та доступ до державної таємниці. Джус О. А., Золотарьова М. К., Копотун І. М., Макарова Т. П. (2023). Київ: Професіонал ВД. ISBN 978-611-01-2935-0.
85. Довженко Л. М. Поняття системи забезпечення державної таємниці України. Вісник ХНУВС. 2013. № 1 (60). С. 159–165.
86. Єфімов В. В. Забезпечення державної таємниці в оперативно-розшуковій діяльності. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2011. № 4. С. 41–418.
87. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом С. М. Головань, В. Б. Дудикевич, В. С. Зачепило, Л. Т. Пархуць, В. О. Хорошко, Л. М. Щербак. Львів: Видавництво Львівської політехніки, 2005. 288 с.
88. Дрейс Ю. О. (2014). Функціонування системи охорони державної таємниці в Україні: організаційно-правова структура, принципи та завдання. Безпека інформації, 20(2). DOI: https://doi.org/10.18372/2225-5036.20.7305
89. Історія охорони державної таємниці в Україні: монографія / О. В. Ботвінкін, В. М. Шлапаченко, В. П. Ворожко, А. С. Пашков. К.: Науково-видавничий відділ Національної академії СБ України, 2008. 155 с.

90. Климчук С. Проведення порівняльного аналізу законодавства у сфері інформації з обмеженим доступом України та країн-членів НАТО. Юридичний радник. 2006. № 11. С. 9–16.
91. Ковальчук С. О., Крет Г. Р. Матеріальні носії секретної інформації: поняття, види і порядок зберігання під час кримінального провадження. Наукові праці НУ ОЮА. 2013. С. 410–419.
92. Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник/ Борис Кормич. – К. : Кондор, 2005. 382 с.
93. Костенко І. В. Організаційне забезпечення безпеки транспортування таємної кореспонденції. Матеріали міжнародної науково-практичної конференції. Донецьк, 2010. 350 с.
94. Костенко І. В. Режим таємності в органах внутрішніх справ при здійсненні оперативно-розшукової діяльності. Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2011. № 4. С. 294–299.
95. Кулініч О. О. Теоретико-методологічні підходи до визначення структури інформації з обмеженим доступом. Актуальні проблеми держави і права. 2008. С. 24–32.
96. Костенко О. Профессиональная тайна и режим секретности в органах прокуратуры Украины. LegeasiViata. 2015. Decemberie. С. 52–56.
97. Кравченко О. О. (2022). Охорона конфіденційної інформації та комерційної таємниці в умовах воєнного стану. Науковий вісник Дніпропетровського державного університету внутрішніх справ, спеціальний випуск № 2 (121). С. 476–480.
98. Корченко О. Г., Казмірчук С. В., Дрейс Ю. О. Метод аналізу і оцінки величини можливої шкоди національній безпеці держави у сфері охорони державної таємниці / Захист інформації. 2012. Том 14, № 3 (56). С. 5–18. URL: http://www.nbuv.gov.ua/ old_jrn/natural/Zi/2012_3/1.pdf
99. Михайлуца М. Державна таємниця за кримінальним законодавством України та зарубіжних країн світу: порівняльноправовий аналіз. Національний юридичний журнал: теорія і практика. 2016. С. 167–171.

100. Нарис історії охорони державної таємниці в Україні: монографія / В. П. Ворожко, Б. В. Бернадський, О. В. Ботвінкін. К.: Наукове видання, 2012. 188 с.
101. Олійник В. Понятійні проблеми інституту державної таємниці. Науковий часопис Національної академії прокуратури України. 2015. № 4. С. 129–135.
102. Олійник В. І. (2020). Досвід кримінально-правового забезпечення охорони державної таємниці країн близького зарубіжжя. Юридична наука, (12(114)), С. 144–152.
103. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посібник / [А. Б. Стоцький, О. І. Тимошенко, А. М. Гуз та ін.], за заг. ред. В. С. Сідака. – К. : Вид-во Європ. ун-ту, 2006. – 232 с.
104. Організація охорони державної таємниці в Україні : навч. посіб. [Електронний документ] / А. М. Супруненко, І. І. Башта, А. М. Лисеюк, К. С. Свіріна, Ун-т держ. фіск. служби України. – Ірпінь : Ун-т ДФС України, 2020. – 370 с. – (Серія “На допомогу студенту УДФСУ”, т. 68). URI https://ir.dpu.edu.ua/handle/123456789/558
105. Охорона державної таємниці: навчальний посібник. Зачепило В. С., Шандра З. А., Опірський І. Р., Тишик І. Я., Мороз Л. В. Міністерство освіти і науки України, Національний університет “Львівська політехніка” Видавництво Львівської політехніки, 2015, 168 с.
106. Правове забезпечення інформаційної діяльності в Україні. Горобцов В., Колодюк А., Кормич Б. та ін., ред. І. С. Чиж; Ін-т держави і права ім. В. М. Корецького, Нац. Академія Наук України, Держ. комітет телебачення і радіомовлення України. – К.: Юридична думка, 2006. – 384 с.
107. Рогатинська Н. З. Кримінальне провадження, яке містить відомості, що становлять державну та банківську таємницю. Актуальні проблеми правознавства. 2016. Випуск 1. С. 180–186.
108. Розвадовський О. Забезпечення охорони державної таємниці та службової інформації : теоретичний, правовий та організаційний аспекти : монографія : у 2-х ч. – К. : Центр нав.-наук. та наук.-практ. видань НА СБ України, 2014. – (Ч. 1. – 228 с.; Ч. 2. – 284 с.).

109. Розголошення державної таємниці. Велика українська юридична енциклопедія. У 20 т. Т. 17. Кримінальне право / В. Я. Тацій (відп. ред.) та ін. – 2017. – С. 860.
110. Розголошення державної таємниці. Українська енциклопедія ім. М. П. Бажана, 2003. – Т. 5 : П – С. – 736 с.
111. Семенюк О. Г. Еволюція наукових поглядів на забезпечення діяльності з охорони державної таємниці. Інформація і право. 2017. № 1 (20). С. 123–131.
112. Семенюк О. Порядок віднесення інформації до державної таємниці: порівняльний аналіз вітчизняного та зарубіжного законодавства, шляхи удосконалення цієї процедури. Юридична Україна. 2016. № 3–4. С. 58–63.
113. Система забезпечення інформаційної безпеки України // Національна безпека і оборона. – 2001. – № 1. – С. 16–28.
114. Системи охорони державної таємниці: електронний навчально-методичний комплекс / Опірський І. Р., Гарасимчук О. І. та ін., 2021. – Львів: Національний університет “Львівська політехніка”.
115. Служба безпеки України Порядок отримання спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею. [Електронний ресурс] – Режим доступу до ресурсу: https://ssu.gov.ua
116. Таємна інформація // Юридична енциклопедія: [у 6 т.]/ ред. кол. Ю. С. Шемшученко (відп. ред.) [та ін.].– К.: Українська енциклопедія ім. М. П. Бажана, 2004. – Т.6: Т – Я. – 768 с.– ISBN 966-7492-06-0.
117. Термінологічний довідник з питань технічного захисту інформації. Коженевський С. Р., Кузнецов Г. В., Хорошко В. О., Чирков Д. В. / За ред. проф. В. О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.
118. Трембач І. І. Поняття державної таємниці як об’єкта кримінально-правової охорони. Актуальні проблеми вітчизняної юриспруденції. 2017. Спецвипуск, Ч.1. С. 227–230.
119. Чердинцев Ю. Г. Правові засади режиму секретності в Україні. Актуальні проблеми вітчизняної юриспруденції. 2018. № 6, т. 1. С. 48–52.
120. Шлапаченко В. М. Шляхи удосконалення нормативноправового визначення державної таємниці. Інформаційна безпека людини, суспільства, держави. 2013. № 3 (13). С. 41–44.

121. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ // Актуальні проблеми економіки. – 2006. – № 10. – С. 220–225.
122. Ящук В. Проблеми оцінювання впливу штучного інтелекту на систему захисту державної таємниці в органах сектору безпеки і оборони України / Ящук В. // Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України: матеріали Науково-практичної конференції (Львів, 20 грудня 2024) / упорядник: Т. В. Магеровська. – Львів : ЛьвДУВС, 2025. – 137 с. (С. 129–133).
123. Ящук В. І. Організація багаторівневої системи охорони державної таємниці в умовах воєнного стану. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : тези ІІІ Міжнародної науково-практичної конференції (Хмельницький, 21 листопада 2024 року). Хмельницький : Видавництво НАДПСУ, 2025. 1804 с. (С. 1226–1229).
124. Ящук В. І., Ошурко Б. Сучасні виклики захисту державної таємниці в умовах війни. Інформаційна безпека та інформаційні технології: збірник доповідей V Міжнародної науково-практичної конференції, ІБІТ 2024, м. Львів, 27 листопада 2024 року. Львів, ЛДУ БЖД, 2024, 661 с. (С. 17–20).

НАВЧАЛЬНЕ ВИДАННЯ

Ящук Валентина Ігорівна
Івануса Андрій Іванович
Ткачук Ростислав Львович
Балацька Валерія Сергіївна

СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

Навчальний посібник

Літературний редактор **Галина Падик**

Технічний редактор
та ком'ютерна верстка **Маріанна Климус**
Ростислав Ткачук

Друк **Назарій Петролюк**

Підписано до друку 19.12.2025 р.
Формат 60x84/16. Гарнітура Times New Roman.
Друк цифровий. Папір офсетний.
Ум. друк. арк. 16,9

Друк ЛДУБЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
Тел. /факс: (032)233-24-79
E-mail: vnrd@ldubgd.edu.ua
Свідоцтво суб'єкта видавничої справи ДК №7249 від 09.02.2021 р.