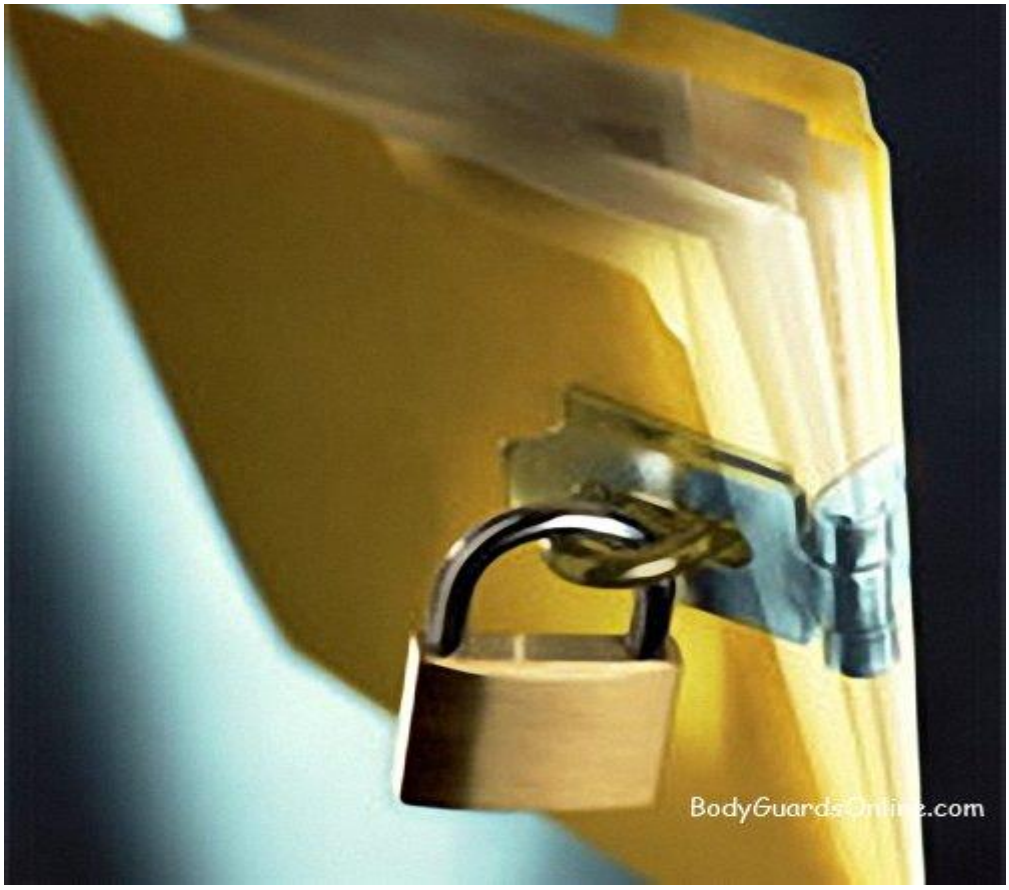
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ФІНАНСОВИХ РОЗСЛІДУВАНЬ

ОПОРНИЙ КОНСПЕКТ ЛЕКЦІЙ З ДИСЦИПЛІНИ «ОХОРОНА ДЕРЖАВНОЇ ТА КОМЕРЦІЙНОЇ ТАЄМНИЦІ»

для студентів освітньо-кваліфікаційного рівня «магістр» галузі знань – 07 Управління та адміністрування
Спеціальність – 073 Менеджмент



ТЕРНОПІЛЬ – 2018

Опорний конспект лекцій з дисципліни «Охорона державної та комерційної таємниці» розроблено для студентів денної та заочної форм навчання освітньо-кваліфікаційного рівня «магістр» галузі знань – 07 Управління та адміністрування, Спеціальність – 073 Менеджмент / І. В. Зайцева-Калаур, – Тернопіль: ТНЕУ, 2018. – 147 с.

Укладач:Зайцева-Калаур І.В – к.ю.н., доцент кафедри економічної безпеки та фінансових розслідувань Тернопільського національного економічного університету

Рецензенти:

– Н. В. Міловська– к.ю.н., доцент науковий співробітник відділу проблем приватного права Науково-дослідного інституту приватного права і підприємництва імені академіка Ф.Г. Бурчака НАПрН України

– Т. О. Подковенко – к.ю.н., доцент, доцент кафедри теорії та історії держави і права ТНЕУ

Відповідальний за випуск:

Москалюк Н.Б. – завідувача кафедри економічної безпеки та фінансових розслідувань Тернопільського національного економічного університету;

Розглянуто та рекомендовано до друку на засіданні кафедри економічної безпеки та фінансових розслідувань Тернопільського національного економічного університету;

Протокол № 2 від 06.09.2018 р.

Розглянуто та рекомендовано до друку Науково-методичною радою Юридичного факультету Тернопільського національного економічного університету

Протокол № 2 від 28.09. 2018 р.

ПЕРЕДМОВА

Із становленням України як суверенної, правової держави, розширенням її міжнародного співробітництва, реформуванням економіки та оборони постала необхідність створення принципово нової власної системи захисту інформації та законодавчого регулювання інформаційних правовідносин у сфері охорони таємниць. Конституція України, що стала гарантом побудови демократичної правової держави, не могла не врахувати загальносвітових тенденцій інформатизації суспільства. Тому багато її статей, зокрема, ст. 17, 32, 34, визначають забезпечення інформаційної безпеки як одну із найважливіших функцій держави і мають стати основою розвитку інформаційного законодавства. Ми живемо у світі конкурентної боротьби за сфери впливу на міжнародній арені, світових ринках, за пріоритети у науковій, військово-технічній, економічних галузях. Тому захист інформації, зокрема державної таємниці, є невід'ємною складовою національної безпеки України. А там, де переважають особливі інтереси держави, інтереси її безпеки, зовнішніх відносин та економіки, чинне законодавство повинно забезпечувати саме їх захист: утвердження інформаційного суверенітету України, її право на встановлення особливого порядку користування і розпорядження інформацією з обмеженим доступом, найважливішою складовою якої є державна таємниця.

Не менш актуальним є питання надійної охорони комерційної таємниці. Усвідомлюючи невпинний економічний розвиток, необхідність у досягненні переваги на ринку, потреб у знаннях про джерела загроз, порушників і потенційних збитків, господарюючі суб'єкти повинні приділяти увагу створенню системи охорони та захисту своїх інформаційних ресурсів. Питання забезпечення надійної охорони та захисту комерційної таємниці стає ще важливішим внаслідок загострення конкурентної боротьби на ринках, яке може призвести до використання конфіденційних відомостей з метою нанесення шкоди інтересам підприємства та завдання матеріальних і моральних збитків. Сьогодні рівень успішної та ефективної діяльності кожної організації залежить від уміння компанії захистити свою конфіденційну інформацію від її неправомірного використання. Таким чином, зараз існує актуальна потреба в захисті комерційної таємниці суб'єктів господарювання, який би був ефективним і відповідав сьогоднішнім та перспективним вимогам ринкового середовища.

Метою вивчення дисципліни є можливість опанувати систему правових знань щодо порядку захисту державної таємниці; закріплення підприємством права на комерційну таємницю, основні юридичні засади, що забезпечують функціонування та захист комерційної таємниці, а також основні принципи правового регулювання відносин у сфері захисту цього правового інституту, підстави, особливості відповідальності щодо порушень законодавства про державну та комерційну таємницю.

Завдання курсу: вивчення понятійного апарату навчальної дисципліни «Охорона державної та комерційної таємниці», пізнання її предмета і значення організації практичного захисту комерційних секретів у приватнопідприємницькій сфері економіки, а також концепції системного підходу до забезпечення захисту конфіденційної інформації.

Засвоївши програму навчальної дисципліни «Охорона державної та комерційної таємниці», фахівці за відповідним напрямом підготовки,

спеціальністю та спеціалізацією мають бути здатними вирішувати професійні завдання з урахуванням вимог захисту інформації та володіти:

- *На рівні знань знати:*

– поняття за загальну характеристика таємної інформації**;**

– законодавче забезпечення захисту державної таємниці;

– правове регулювання захисту комерційної таємниці;

– механізм визначення переліку інформації, що становить комерційну таємницю, та інформації, що не може бути визначена підприємством комерційною таємницею;

– механізм доступу до інформації що становить державну таємницю та комерційну таємницю;

– систему правового захисту комерційної таємниці підприємства, її елементи та складові;

– порядок забезпечення інформаційної безпеки та захист комерційної таємниці;

– порядок організації роботи з документами, що становлять державну таємницю; порядок організації колективної роботи з документами що становлять комерційну таємницю; обов'язкові умови, пов'язані із забезпеченням безпеки використання, збереження та захисту комерційної таємниці підприємства;

– види і процедури юридичної відповідальності за розголошення державної та комерційної таємниці;

– тощо.

- *На рівні практичних навичок вміти:*

– свідомо дотримуватися правил роботи з інформацією з обмеженим доступом та виконувати вимоги до захисту інформації, що діють у системі ОВС України;

– використовувати спеціальні технічні засоби захисту інформації;

– використовувати програмні та апаратні засоби розмежування доступу до інформації у автоматизованих системах та антивірусні засоби захисту інформації у персональних комп'ютерах;

– використовувати комп'ютерні криптографічні, стенографічні системи захисту інформації.

Тема 1. Інформація з обмеженим доступом: поняття та види

Поділ та загальна характеристика інформації за режимом доступу. Державна таємниця – особливий вид таємної інформації. Поняття, правова природа та ознаки комерційної таємниці. Об'єкти комерційної таємниці та суб'єкти права на комерційну таємницю.

1. За своєю значимістю інформація складає найважливіший потенціал держави та суспільства. В цьому зв'язку є важливим визначення поняття «інформація». У новому тлумачному словнику української мови інформація визначається як відомості про які-небудь події, чиюсь діяльність, повідомлення про щось .

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 .

Найчастіше поняття «інформація» розкривається через поняття «відомості». За визначенням, інформація і відомості – це синоніми. Але це не зовсім так. Відомості являють собою певні відносини між інформацією і відображуваним нею об'єктом. Ці відносини містять факт, інформацію про нього і суб'єкта, що одержує цю інформацію. Тобто, відомості – це копія реального факту. Інформація ж у неживій природі являє собою інформацію одного об'єкта щодо іншого об'єкта поза відносинами до суб'єкта. Тут відбувається лише сприйняття, збереження й обмін інформацією. Таким чином, поняття «інформація» ширше поняття «відомості».

У широкому розумінні поняття «інформація» містить у собі будь-які відомості, а також їх передання, поширення і використання.

Виділяють наступні 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 . Юридичне значення ознак інформації полягає в тому, що саме вони визначають її правовий режим і повинні бути основою концепції її правової охорони, що обирається законодавцем.

Чітке визначення поняття «інформація» подано законодавцем 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.

У цивільному законодавстві інформацію закріплено як об'єкт цивільних прав. Зокрема, 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».

Ті визначення, які сьогодні запропоновані законодавцем не містять вичерпного тлумачення поняття «інформація». Так, на думку провідного науковця

О.В. Кохановської, інформація є нематеріальним благом особливого роду, що відрізняє його від інших нематеріальних благ, але всі інші закріплені нематеріальні блага, зокрема результати інтелектуальної, творчої діяльності і особисті немайнові блага, можуть бути визначені, пояснені і охарактеризовані через феномен інформації; інформація, як благо, може поглинати зміст інших нематеріальних благ і має, таким чином, визначатися з урахуванням останніх.

«Інформація – це нематеріальне немайнове благо особливого роду, яке нерозривно пов'язане з життям, з його виникненням і закінченням, яке проявляється як особисте немайнове благо, як результат впливу на людину та інших суб'єктів та об'єктів права, як результат інтелектуальної творчої діяльності і як відомості про осіб, події та явища, предмети, об'єкти і процеси незалежно від форми їхнього представлення».

Інформація, як особлива субстанція має ряд властивостей та характеристик. Зокрема: фізична невідчужуваність, системність, селективність, субстанціональна несамостійність, послідовність, невичерпність, масовість, здатність інформації до обмеження і трансформації, універсальність, якість, актуальність.

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 на увазі два аспекти – якісний аспект, який розкриває масовість інформації як інформації суспільної, загальної для всіх; кількісний – як інформації, яка поширюється серед широкої мережі споживачів, користувачів інформації. Кількісний аспект вважається вторинним від якісного.

Актуальність інформації – ступінь відповідності інформації розвитку суспільства.

В юридичній літературі окремо виділяють властивості інформації, що визначають стан її безпеки: конфіденційність, цілісність, доступність.

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 [5, с.22].

Цінність інформації може бути різною (комерційною, економічною тощо) і залежить від таких її властивостей, як новизна, актуальність, корисність, цінність

предмета інформації тощо. Створення в Україні реального сектора економіки за рахунок розширення сфери діяльності суб'єктів малого підприємництва тягне за собою зростання попиту на комерційно цінну інформацію.

«Комерційна цінність» інформації – це елементи її новизни, що не є загальновідомими, обумовлюють її значимість в цивільних відносинах і забезпечують суб'єктам права на комерційну таємницю певні конкурентні переваги та додатковий економічний ефект від здійснення підприємницької діяльності, а «комерційно цінна інформація» - це сукупність відомостей технічного, технологічного та ділового характеру, які складають при певних умовах комерційну таємницю.

У межах вивчення курсу становить інтерес зміст комерційно цінної інформації, яка складає комерційну таємницю. Така інформація є нематеріальним результатом інтелектуальної діяльності людини, доступ до якого може бути обмежений. Розглядаючи інформацію з обмеженим доступом як вид інформації, слід виходити з того, що вона має спільні ознаки, властиві інформації як об'єкту цивільних прав та специфічні ознаки, що істотно відрізняють її від інших видів інформації. Спільними ознаками є: відокремленість інформації, організаційна форма. Будь-яка інформація з обмеженим доступом має особливу цінність у силу її дійсної або потенційної невідомості третім особам, що відрізняє її від звичайної інформації і є її сутнісною ознакою.

У науковій літературі існують класифікації інформації, засновані на різних критеріях, у тому числі і за ступенем доступу. Так, наприклад, В.А. Копилов пропонує класифікувати інформацію на відкриту (документована, масова та інша інформація необмеженого доступу) та з обмеженим доступом (державна і службова таємниці, інформація, яка складає ноу-хау). Така ж класифікація визначена і в Законі України «Про інформацію». Так, стаття 20 Доступ до інформації за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

А.А. Шиверський виділяє три види інформації: відкриту інформацію, на поширення і використання якої немає жодних обмежень; запатентовану інформацію, що охороняється чинним законодавством або міжнародними угодами як об'єкт інтелектуальної власності; закриту інформацію, що охороняється законом та захищається за допомогою механізмів забезпечення державної, комерційної або іншої таємниці. При цьому, він розділяє інформацію яка захищається і не захищається. Підставою розподілу в даному випадку є той факт, що в суспільстві або в державі охороняється й захищається лише та інформація, що найбільш важлива для суб'єкта. Важливість цієї інформації визначається тим, що вона приносить якусь користь, прибуток і тому має потребу в охороні і захисті від третіх осіб. Критеріями віднесення інформації до того чи іншого виду є таємність і конфіденційність . С.І. Семілєтов класифікує інформацію на: загальнодоступну інформацію; закриту інформацію, що складає державну таємницю; конфіденційну інформацію, що складає і комерційну таємницю.

Завдяки кожній з розглянутих пропозицій щодо класифікації інформації відбувається більш поглиблене її вивчення. Таким чином найбільш ґрунтовно необхідно провести класифікацію інформації за такими критеріями:

– 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.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено 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.

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

1) про стан довкілля, якість харчових продуктів і предметів побуту;

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

3) 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;

4) про факти порушення прав і свобод людини і громадянина;

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

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

2. Важливим елементом забезпечення і інформаційної безпеки держави, і національної безпеки загалом, і реалізації функцій управління у органах державної влади є режим охорони державної таємниці в Україні.

Проблема врегулювання суспільних відносин у сфері охорони державної таємниці на сучасному етапі розвитку людства була вирішена в розвинутих країнах шляхом прийняття відповідних законів. Однак, у колишньому СРСР та донедавна в Україні не існувало закону не тільки про державну таємницю, але й про інформацію взагалі. Відносини, що виникали в сфері охорони державної таємниці регулювались на рівні урядових рішень, які в більшості випадків мали закритий характер і не давали змоги ознайомитися з ними як вченим-юристам, так і широкому загалу.

З прийняттям Закону України "Про державну таємницю" на законодавчому рівні було врегульовано суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, її засекречуванням та охороною з метою захисту життєво важливих інтересів України у сфері оборони, економіки, зовнішніх відносин, державної безпеки й охорони правопорядку.

Необхідно, перш за все, розкрити поняття "державна таємниця" та ознаки, які його характеризують. Чітке визначення поняття дозволить правильно визначати коло відомостей, котрі потрібно охороняти, розподіляти зусилля з організації охорони, вирішувати питання про відповідальність осіб за порушення

законодавства, уникати витрати сил та засобів на охорону несекретної інформації, правильно з'ясовувати та аналізувати можливі шляхи витоку інформації тощо.

Законодавство України дає чітке визначення поняття "державна таємниця". 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. Отже, слід виокремити та дослідити ознаки, які характеризують це поняття Перша ознака полягає у тому, що державна таємниця є видом таємної інформації правове регулювання якої здійснюється відповідним законом. Закон України "Про інформацію" вперше на законодавчому рівні закріпив необхідність врегулювання правових відносин у сфері охорони державної таємниці на рівні спеціального закону. Прийняття Закону України "Про державну таємницю" було першим кроком на шляху раціонального та демократичного підходу до регулювання вищезазначених суспільних відносин. До речі, законодавче врегулювання зазначених відносин притаманне й таким країнам як США, Сполучене Королівство Великобританії та Північної Ірландії, Польщі та інші.

Закон України "Про інформацію" визначив місце державної таємниці серед іншої інформації. За режимом доступу інформація поділяється на відкриту та інформацію з обмеженим доступом. Остання за своїм правовим режимом поділяється на конфіденційну і таємну. Саме одним з видів таємної і є державна таємниця.

Таким чином, перша ознака державної таємниці полягає в тому, що суспільні відносини, які виникають і складаються під час визначення такої інформації, її охорони та обігу врегульовано на рівні окремого закону.

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. На законодавчому рівні закріплено не всі сфери життєдіяльності держави, які може охоплювати державна таємниця, а лише найважливіші, які пов'язуються із забезпеченням національної безпеки. Слід зазначити, що не вся інформація у визначених сферах може становити державну таємницю, оскільки встановлюються відповідні її категорії. У зв'язку з цим, до державної таємниці можуть бути віднесені конкретні відомості лише за умови, що вони належать до визначених категорій.

Із усього інформаційного простору вирізняються державні інтереси та інтереси суспільства і громадян. Щодо останніх, законом установлено перелік відомостей, які забороняється відносити до державної таємниці:

– 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 і 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 і культури населення;

– про факти порушень прав і свобод людини і громадянина;

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

– інша інформація, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена.

Третя ознака полягає в тому, що розголошення державної таємниці може завдати шкоди національній безпеці України. Справді, немає сенсу приховувати інформацію, від розголошення якої не буде завдано шкоди. Як бачимо, шкода національній безпеці України є однією з матеріальних ознак цього поняття. Протиправний вихід державної таємниці з володіння правомочних суб'єктів, пов'язується з об'єктивним заподіянням або можливістю заподіяння шкоди. Під шкодою розуміються як економічні збитки так й інші тяжкі наслідки. Економічно, шкода визначається матеріальними збитками у кількісному (вартісному) виразі, які сталися чи можуть статися внаслідок розголошення конкретних відомостей, що становлять державну таємницю у сферах оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки і охорони правопорядку. Щодо інших тяжких наслідків, то вони пов'язуються з негативними змінами у зазначених сферах (головним чином, у сферах зовнішніх відносин, державної безпеки і охорони правопорядку), які відбулися чи можуть відбутися внаслідок розголошення конкретних відомостей, що становлять державну таємницю і які не піддаються економічному обрахунку у вартісному виразі. Обґрунтування шкоди національній безпеці, в разі розголошення державної таємниці України, здійснює державний експерт з питань державних таємниць під час віднесення інформації до державної таємниці. Він також бере участь у розробці критеріїв визначення шкоди, яку може бути завдано в разі розголошення такої інформації.

Наступна ознака полягає у тому, що на законодавчому рівні створено механізм віднесення інформації до державної таємниці та її засекречування. Як вже зазначалося, існують категорії інформації, яка становить державну таємницю. Відповідно до цих категорій інформації формується Звід відомостей, що становлять державну таємницю (ЗВДТ), який є єдиною формою реєстрації цих відомостей в Україні. З моменту опублікування Зводу держава забезпечує захист і правову охорону зареєстрованих у ньому відомостей. Служба безпеки України формує ЗВДТ на підставі рішень державних експертів з питань таємниць та публікує в офіційних виданнях. Інформація вважається державною таємницею з часу включення її до ЗВДТ. Реєстрація відомостей у Зводі є підставою для надання документу, виробу чи іншому матеріальному носію інформації, що містить ці відомості, грифу секретності, встановленому для них у ЗВДТ. На підставі та в межах ЗВДТ з метою конкретизації даних про інформацію, яка віднесена до державної таємниці, органи державної влади України можуть створювати відповідні розгорнуті переліки відомостей, що становлять державну таємницю. Такі переліки повинні бути затверджені державними експертами з питань таємниць та погоджені СБ України. Розгорнуті переліки, що становлять державну таємницю, не можуть суперечити ЗВДТ. Віднесення та засекречування інформації, котра становить державну таємницю є вольовим актом з боку держави і залежить від внутрішньо — та зовнішньополітичної обстановки, економічного розвитку, політичного режиму тощо.

Ознакою державної таємниці є те, що її охорона здійснюється державою. На відміну від інших видів інформації (банківської, комерційної) фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею в бюджетних установах і організаціях має здійснюватися за рахунок Державного бюджету

України, бюджету Автономної Республіки Крим та місцевих бюджетів. Кошти на зазначені витрати повинні передбачатися у відповідних бюджетах окремим рядком. Такі витрати інших установ і організацій, а також підприємств відносяться до валових витрат виробника продукції, виготовлення якої пов'язано з державною таємницею. Витрати, пов'язані з державною таємницею, на недержавних підприємствах, установах, організаціях відповідно до Закону України "Про державну таємницю" фінансуються на підставі договору з замовником робіт, пов'язаних з державною.

Підприємствам, установам і організаціям, які провадять діяльність, пов'язану з державною таємницею, можуть надаватися податкові та інші пільги в порядку, встановленому законом.

3. Важко переоцінити значення комерційної таємниці для суб’єкта господарської діяльності. Надійна охорона такої інформації, що носить конфіденційний характер є не лише способом захисту цінної інформації про об’єкти стратегічних змін, а і економічним інтересом та стратегічним ресурсом, який здатний забезпечити конкурентні переваги на ринку промисловості. Саме тому необхідність встановлення правового режиму комерційної таємниці є одним з першочергових питань забезпечення економічної безпеки підприємства.

Хоча комерційна таємниця є визнаним ефективним засобом, правового захисту економічних інтересів підприємців, однак до нині цей інститут позбавлений єдиного розуміння та уніфікованого правового регулювання. Наявна і термінологічна невизначеність: щодо комерційної таємниці застосовуються найрізноманітніші терміни – виробничий/технічний/комерційний секрет, конфіденційна/закрита інформація, комерційна/службова таємниця, ноу-хау і деякі інші Немає узгодженого трактування їхньої правової ролі та змісту. У правозастосовчій практиці немає одностайності і щодо того, чи є секрети виробництва об’єктом інтелектуальної власності. Тож на рівні деяких країн реалізовані різноманітні підходи, що часом істотно різняться.

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

Згідно 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 контролюючого цю інформацію [1, с. 67].

Термінологічні різночитання поняття комерційно цінної інформації спостерігаються в ФРН, Австрії, Італії. Німецька доктрина використовує для визначення конфіденційних відомостей два терміни: «торговий секрет» («Geschäftsgeheimnis») і «виробничий секрет» («Betriebsgeheimnis»). Аналогічну позицію займає австрійське право. Італійська доктрина використовує термін «промислові і торгові секрети» («segreto industriale e commerciale»), а датське право оперує поняттям «відомості про виробничі і торговельні відносини» («oplysninger om drifts-eller forretningsforhold»). Часто виробничі секрети (секрети

виробництва) ототожнюються з ноу-хау. При цьому, під комерційною таємницею розуміють не захищені законодавчим шляхом результати винахідництва, способи виготовлення, конструкції та інші збагачуючі техніку досягнення. Це можуть бути креслення, рецептура і інші подібні письмові відомості, вся сукупність виробничого досвіду у всіх його різновидах. При цьому неважливо, чи зафіксований досвід в письмовому вигляді або він проявляється в знаннях і досвіді фахівців. Комерційні знання і досвід також можуть охоронятися як виробничі секрети.

Збільшення термінів, які використовуються для позначення комерційно цінної інформації, призвело до того, що постала необхідність впровадження і використання більш загального терміна, що охоплює всю сукупність відомостей, пов'язаних із здійсненням господарської діяльності. Більшість науковців схилялися до використання поняття «господарська таємниця» («Wirtschaftsgeheimnis»).

На міжнародному рівні таким узагальнюючими поняттями, як було зазначено вище, є терміни «секретна інформація», «закрита інформація».

Аналогом даних універсальних термінів в нашому законодавстві виступає поняття «комерційна таємниця».

На сьогодні відсутній окремий спеціальний закон України про комерційну таємницю та її правову охорону, а правовідносини щодо комерційної таємниці регулюються окремими положеннями Цивільного кодексу України (ЦК), Господарського кодексу України (ГК), Закону України «Про захист від недобросовісної конкуренції» та іншими нормативними актами, в тому числі міжнародними. 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. Законодавцем 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. Склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону. 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 наступні.

1. Комерційною таємницею може визнаватися лише інформація. Слід підкреслити, що на відміну від відомих, традиційних для права об’єктів, інформація, зокрема що становить комерційну таємницю, характеризується специфічними особливостями та юридичними властивостями: інформація при включенні в обіг відокремлюється від автора або власника, опредметнюється у вигляді символів та знаків і внаслідок цього існує окремо та незалежно від автора або власника; після передачі інформації від одного суб’єкта до іншого інформація одночасно може належати двом учасникам інформаційних відносин; полягає в єдності інформації та матеріального носія, на якому закріплюється інформація. Така інформація повинна бути відображена в об’єктивній формі.

2. Інформація, яка становить комерційну таємницю, не потребує офіційного визнання її охороноспроможності, реєстрації чи дотримання інших формальних процедур для поширення на неї правової охорони. Для охорони комерційної таємниці необхідно мати відомості, достатні для її ідентифікації, тому вони мають бути зафіксовані на матеріальному носії (зразок, електронна форма, відео, звукозапис та ін.), доступному для сприйняття третіми особами (відповідно, усна форма є недостатньою). Така інформація повинна бути відображена в об’єктивній формі.

3. 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 норм вітчизняного законодавства є об'єктом права інтелектуальної власності суб'єкта підприємницької діяльності, використання якої не завдасть шкоди суспільству.

4. Така інформація має бути не відомою та не легкодоступною для інших осіб. Здатність інформації тиражуватись та розповсюджуватись без зміни її змісту в необмеженій кількості, якщо не встановлені обмеження доступу до неї втрачає свою економічну цінність.

Відсутність загальновідомості полягає в тому, що інформацією, яка складає комерційну таємницю, володіє обмежене коло осіб, хоча й не обов’язково одна особа. Однаковою або аналогічною інформацією можуть одночасно володіти декілька осіб – але визначальним є те, що коло цих осіб обмежене. Саме не загальновідомість є вихідною для встановлення охорони змісту об’єкту, яким є комерційна таємниця, за відсутності його спеціальної реєстрації.

Незагальнодоступність означає відсутність вільного доступу до інформації на законній підставі. Особи, які допущені до таємниці зобов’язані не розголошувати її.

З даною ознакою пов’язані дві наступні.

5. Внаслідок її невідомості вона має комерційну цінність. Розголошення комерційної таємниці згідно ст. 36 ГК України «може завдати шкоди інтересам суб’єкта господарювання».

Якщо інформація становить іншу цінність (особисту і т.п.), вона не може бути визнана комерційною таємницею.

Розрізняють «дійсну комерційну цінність» і «потенційну комерційну цінність» інформації. Дійсна – представляє цінність вже в момент її віднесення до комерційної таємниці, потенційна – виникає через певний проміжок часу після віднесення інформації до комерційної таємниці.

6. Зазначена інформація має бути предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Цей критерій є одним з найбільш важливих, оскільки об'єктивно відображає волю суб'єкта господарювання до збереження фактичної монополії над певним обсягом комерційно цінної інформації.

Зовнішнім проявом виражається у прийнятті відповідних правових, організаційних, технічних заходів щодо збереження конфіденційної інформації. Таким чином, при оцінці достатності заходів щодо охорони конфіденційності інформації, що становить комерційну таємницю, слід використовувати три критерії: правовий (закріплення режиму комерційної таємниці за певною інформацією в локальних актах), технічний (використання технічних способів захисту інформації) і організаційний (організація спеціального діловодства, створення спеціальних режимних підрозділів і т.п.).

7. Зміст та об’єм комерційної таємниці встановлюється володільцем інформації на власний розсуд. Йому належать всі права щодо розпорядження нею. Право особи на комерційну таємницю зберігається на весь час існування фактичної монополії цієї особи на інформацію, яка її складає.

Відповідно до ст. 506 ЦК України майновими правами інтелектуальної власності на комерційну таємницю є: право на використання комерційної таємниці; виняткове право дозволяти використання комерційної таємниці; виняткове право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці; інші майнові права інтелектуальної власності, встановлені законом

8. Ще однією особливою ознакою комерційної таємниці є необмеженість строку її захисту.

Сукупність усіх вище зазначених ознак дає підстави вважати інформацію комерційною таємницею.

Таким чином, інформація в режимі «комерційна таємниця» охоронятиметься доти, поки дотримуються усі умови, щодо порядку виникнення прав на неї, її охорони та захисту, або поки особа-розпорядник не прийме рішення про недоцільність зберігання її в секретності.

Спірним моментом при визначенні шляхів удосконалення чинного законодавства є проблема віднесення комерційної таємниці до об’єктів інтелектуальної власності. У книзі 4 ЦК України поряд з іншими об’єктами інтелектуальної власності законодавець виділяє комерційну таємницю, з чого слідує висновок, що до комерційної таємниці можуть бути віднесені лише результати інтелектуальної (творчої) діяльності людини. Така практика захисту комерційної таємниці сьогодні існує і в міжнародному праві. Як уже зазначалось вище, її захист передбачено Паризькою конвенцією про охорону промислової власності, Угодою з торгівельних аспектів прав інтелектуальної власності, де останню визнають об’єктом інтелектуальної власності.

Поряд з цим, не всі об’єкти і не будь-які відомості, що можуть бути віднесенні до комерційної таємниці, є результатом інтелектуальної (творчої) діяльності. Згідно ч. 2 ст. 505 ЦК 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. Існуюча практика підприємницької діяльності під грифом комерційно-цінної 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. Подібний поділ такої інформації запропоновано і в науковій літературі. Для прикладу, 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. У зв'язку з цим, 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 що до певних фактів, подій, явищ та продукти інтелектуальної діяльності. Зважаючи на це, потрібно забезпечити захист інформації, яка є результатом інтелектуальної діяльності, так і інформації, що не містить таких ознак.

Отже, щодо співвідношення інформації, яка захищається за допомогою законодавства про інтелектуальну власність та конфіденційної інформації, що є комерційно цінною, то воно виглядає наступним чином: комерційна таємниця не обов'язково є об'єктом інтелектуальної власності, однак інформація, що захищена законодавством про інтелектуальну власність, може бути визнана комерційною таємницею.

Ухвалюючи рішення, чи слід скористатися механізмом охорони комерційної таємниці як об'єкта інтелектуальної власності, необхідно насамперед проаналізувати переваги і недоліки такої охорони порівняно з іншими засобами охорони інтелектуальної власності. 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 потрібно її розкриття або реєстрація у державному органі. Водночас 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. Як наслідок, незапатентована комерційна таємниця може бути запатентована іншою особою, якщо вона буде розкрита нею самостійно. У цьому полягає відмінність комерційної таємниці від патентів на винаходи, які охороняють власників патентів навіть від тих, кому вдалося самостійно розробити аналогічне технічне рішення. Закон не передбачає покарання за добросовісне розкриття, що має бути здійснено у такі законні способи, як: 1) *самостійне створення*; комерційна таємниця не забезпечує виключності, 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 комерційна таємниця 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:

1) по природі: технологічні, виробничі, організаційні, маркетингові, інтелектуальні, рекламні;

2) по належності власнику: власність організації; власність групи організацій; власність однієї особи; власність групи осіб;

3) по призначенню: економічні; ноу-хау; нові технології; технічні вироби; зразки.

Законодавець обмежує право суб'єкта господарювання на комерційну таємницю шляхом встановлення переліку інформації, яка не може бути віднесена до комерційної таємниці. Даний перелік закріплений в підзаконному нормативно-правовому акті Постанові КМУ № 611 від 9 серпня 1993 року «Про перелік відомостей, що не становлять комерційну таємницю», а також в ряді спеціальних законів. Дані обмеження визначають межі використання комерційної таємниці у господарській діяльності.

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. Таким чином, права на комерційну таємницю можуть належати лише тій особі, яка визначила інформацію комерційною таємницею, тобто яка своїм волевиявленням засвідчила намір утримувати певні комерційно цінні відомості в режимі конфіденційності та вжила адекватних дій щодо збереження такого стану невідомості інформації.

Нині діюче законодавство України, що регулює питання охорони та захисту комерційної таємниці не дає однозначної відповіді, хто конкретно виступає суб'єктом права на комерційну таємницю. Так, Зі змісту ст.ст. 36 ГК України випливає, що дані норми спрямовані на охорону комерційної таємниці, володарем якої виступає суб'єкт господарювання. У ЦК України коло власників комерційної таємниці ширше. 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». Таке законодавче трактування щодо визначення суб'єкта права на комерційну таємницю не суперечить ст.162 ГК України, де зазначено: «Особа, самостійно і сумлінно отримала інформацію, яка є комерційною таємницею, має право використовувати цю інформацію на свій розсуд».

Таким чином, законодавством не обмежується коло суб'єктів права на комерційну таємницю, відсутні також будь-які спеціальні статусні вимоги до таких суб'єктів. Відповідно, суб'єктами права на комерційну таємницю в Україні можуть бути не лише громадяни та юридичні особи України, а й іноземці, особи без громадянства та іноземні юридичні особи на рівні з національними суб'єктами права на комерційну таємницю.

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.

Національний режим для іноземних суб'єктів господарської діяльності на території України запроваджено згідно з Законами України «Про зовнішньоекономічну діяльність» та «Про міжнародне приватне право», що надає їм по відношенню до комерційної таємниці не менший обсяг прав і обов’язків, ніж мають суб'єкти господарської діяльності України. Цим же законом проголошені принци рівності перед законом всіх суб'єктів зовнішньоекономічної діяльності, а також принцип рівного захисту їх інтересів.

Оскільки інформація, що визначена як комерційна таємниця, повинна мати комерційну цінність, то, суб'єктами права на комерційну таємницю виступають перш за все суб'єкти підприємницької діяльності (в тому числі і фізичні особи-суб'єкти підприємницької діяльності). Таке право виникає із моменту їх державної реєстрації, отримання у випадках, передбачених законодавством, відповідних ліцензій, а також по здійсненню певних дій для встановлення режиму комерційної таємниці (дії правового, організаційного та технічного характеру). Таким чином, право на комерційну таємницю виникає після здійснення новоствореним суб'єктом підприємницької діяльності юридичних фактів, які лежать в основі права на комерційну таємницю. В науковій літературі, такі юридичні факти поділяють на об'єктивні умови виникнення права на комерційну таємницю і суб'єктивні. Об'єктивні умови знаходять відображення в нормах законів та інших нормативно-правових актах. До суб'єктивних умов відносять самостійно застосовувані законним власником заходів з охорони комерційно-цінної інформації.

Суб’єктами права на комерційну таємницю можуть виступати і суб’єкти некомерційної господарської діяльності. Однак, їх право обмежене використанням комерційної таємниці тільки в цілях отримання прибутку, яке може бути спрямована на реалізацію поставлених перед організацією завдань.

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. Дана категорія суб’єктів виступають у якості користувачів інформації, що становить комерційну таємницю. Так, фізичні особи без статусу суб'єкта підприємницької діяльності перебувають у трудових відносинах із суб'єктом господарювання, та у зв'язку з виконанням ними службових обов’язків їм стала відома комерційна таємниця. Або ж фізичні особи отримали комерційну таємницю в силу цивільно-правового договору. Такі особи виступають користувачами комерційної таємниці. Вони мають право використовувати останню в обсягах, визначених у трудовому, цивільно-правовому договорах, і зобов'язані не розголошувати отриману інформацію третім особам, не використовувати її в протиправних цілях.

Правом на доступ до комерційної таємниці мають органи державної влади, місцевого самоврядування в рамках закріпленої за ними компетенції для реалізації поставлених перед ними завдань. Органи державної влади, органи місцевого самоврядування, їх посадові особи наділені організаційно-господарськими

повноваженнями щодо суб'єктів господарювання. Вони здійснюють прогнозування та планування економічної діяльності, ліцензування, патентування, квотування, стандартизацію та сертифікацію, на них накладається обов'язок справляння податків, обов'язкових платежів, обмеження монополізму та сприяння конкуренції у сфері господарювання, державного контролю та нагляду за господарською діяльністю. Для реалізації перерахованих завдань органи державної влади, місцевого самоврядування повинні мати право доступу до внутрішньої інформації суб'єкта господарювання, в тому числі і тієї, яка становить комерційну таємницю. Вони не можуть використовувати цю інформацію в особистих корисливих цілях, і отримують її лише в обсягах, встановлених законодавством. Останні не відносяться до суб'єктів права на комерційну таємницю, а наділені правом використовувати інформацію для досягнення певного результату передбаченого нормою закону.

Визначивши питання щодо суб'єктів права на комерційну таємницю, слід з'ясувати, що являє собою саме «право на комерційну таємницю».

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. Зазначений перелік майнових прав інтелектуальної власності на комерційну таємницю не є вичерпним.

Право на комерційну таємницю надає суб'єктам такі основні можливості. По-перше, воно забезпечує суб'єкта права на таку інформацію можливістю її засекречування від широкої публіки. По-друге, воно надає відповідному суб'єкту можливість вимагати, щоб інші особи утримувалися від використання незаконних способів одержання інформації, яка складає його комерційну таємницю. Не потрібно ніякого додаткового права забороняти третім особам здійснювати належні такому суб'єкту права в кожному окремому випадку, така заборона в загальній формі первісно встановлена законодавством. По-третє, суб'єкт права на комерційну таємницю має можливість її розкрити. Вчетверте, відповідний суб'єкт може звертатися за захистом своїх порушених прав до суду.

Тема 2. Правовий захист державної таємниці

Законодавче забезпечення захисту державної таємниці. Законодавчо закріплені вимоги до інформації, що містить ознаки державної таємниці, впроваджені з метою охорони державної таємниці. Організаційно-правові заходи

охорони та захисту державної таємниці. Організаційно-правова структура системи охорони державної таємниці.

1. Особливістю формування законодавчого забезпечення системи охорони державної таємниці в Україні стало те, що цей процес відбувався не в рамках національних державних утворень (крім нетривалого періоду національно-визвольних змагань 1917 – 1920 рр.), а був складовою процесів, які проходили в державах, до складу яких на той час входили українські території. Незалежна Україна успадкувала радянську загальнодержавну систему захисту державної таємниці, де було збережено більшість елементів цієї структури. В подальшому при формуванні національної системи охорони державної таємниці враховувалися як випробувані на практиці традиційні засоби і методи, так і досвід розвинених демократичних країн.

Для з'ясування порядку формування сучасного законодавства у сфері охорони державної таємниці, варто коротко розглянути історичні витоки даного процесу. Початком такого формування наукові джерела визначають період кінця XIX початку XX століття.

Із кінця XIX століття охорона державної таємниці набуває системних ознак, попри істотні недоліки. Значною мірою це зумовлювалось неналежною нормативно-правовою базою. Передусім, відсутнє конкретне визначення самого терміна «державна таємниця». Іншою особливістю нормативно-правової бази того періоду була відсутність детального переліку відомостей, що становлять державну таємницю. Кожна із складових державного апарату на власний розсуд визначала, які саме відомості уважаються таємними, та проводила діяльність із захисту такого роду інформації.

Вдосконалення нормативно-правової бази у сфері захисту державної таємниці визначалось заходами, спрямованими на протидію державній зраді і шпигунству. Уложення про покарання розрізняло три види державної зради: загальну, військову і дипломатичну. Оскільки неодмінною кваліфікуючою ознакою державної зради було посягання на державну таємницю поділ такого роду інформації здійснювався та три види. ІЩо ж до конкретних відомостей, то можна лише виділити їх окремі групи, що мали гриф «ті, що повинні зберігатись у таємниці». Вони стосувались воєнної складової, «...планів російських фортець й інших укріплених споруд, гаваней, портів, арсеналів». Сюди ж відносили мобілізаційну документацію.

Хоча на той час сила і могутність держави оцінювались, виходячи з її можливості вести і вигравати війни, чимало таємних і інших важливих державних документів, зокрема накази по воєнному відомству, не вважалися таємними, тому їх передача не була караною. У той же час шпигунство ставало масовим, систематичним, удосконалювались способи збирання інформації. Справа доходила до курйозів. У 1910 році головний військовий суд навіть висловив думку, що «передача агентам іноземної держави взагалі всіх наказів по військовому відомству не підлягає покаранню», мотивуючи це тим, що у цих наказах містяться відомості, котрими керуються у своїй діяльності всі чини військової частини. Відповідно, такі документи пропонувалось уважати нетаємними.

Рішення військового суду було локалізоване роз'ясненням Сенату, котрий зазначив, що збір відомостей про кількість військ і назви військових частин у будь-якому пункті для передачі іноземній державі є кримінально караним діянням. Тож

постала нагальна потреба не лише чіткого визначення поняття «державна таємниця», а й конкретного переліку відомостей, що її становлять.

Уперше порохом у Європі запахло у 1908 році, що зумовило й перші кроки з посилення режиму таємності. У жовтні 1909 року було заборонено публікувати у періодичних виданнях будь-яку інформацію про пересування військ і їх бойову підготовку. Заборона діяла протягом 6 місяців, потім її періодично продовжували до 5 грудня 1911 року. Відомості про переміщення військових частин уважались цілком таємними до завершення реорганізації армії.

Доки не було уведено в дію нові закони, контррозвідники керувались у своїй діяльності підзаконним актами. Наказом військового міністра у червні 1911 р. було запроваджено Інструкцію начальникам контррозвідувальних відділень, яка досить детально регламентувала організацію боротьби зі шпигунством та іншими видами діяльності іноземних держав у Росії, що загрожували безпеці імперії. А головне, спільними зусиллями фахівців Військового міністерства та Департаменту поліції тут було вміщено тлумачення поняття військового шпигунства (військової розвідки), котре охоплювало й поняття державної таємниці, тобто інформації, що потребує захисту від шпигунів.

Тож у документі містився 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 (портову, 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 знаходження, властивості й прохідність місцевих природних перешкод та можливі місця висадки, так само як і про прилеглі до укріплених районів місцевості; 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; є) дані про ґрунтові шляхи сполучення в цих місцевостях, особливо про мережу шосейних доріг, природні перешкоди, що на них знаходяться та перевізні засоби; ж) 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; з) телеграфні та телефонні повідомлення; прибережні й острівні спостережні пункти морського відомства і прикордонної варти; голубино-поштові й радіотелеграфні станції; й) військове повітроплавання; к) характеризуючи дані командного складу військового і морського відомств.

З березня 1912 р. воєнний міністр та міністр юстиції підписали «Пояснюючу записку до проекту про зміни діючих законів про державну зраду

шляхом шпигунства», де наголосили на невідповідності правових норм вимогам часу. На підставі вказаної записки й почав формуватися перелік секретної інформації, а поняття державної таємниці фактично було зведено до військової. Записка була надзвичайно переконливою, тому всі етапи законодавчого процесу законопроект пройшов дуже швидко і 5 липня 1912 року, після схвалення Державною радою, затверджений царем. У Законі «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». Встановлено кримінально-правову заборону продажу чи заявки за кордон секретних винаходів або удосконалень, які стосувалися військової оборони країни; а також опублікування або повідомлення будь-якій іншій особі таких відомостей.

Право визначати, які саме відомості заборонені до друку, надавалось міністру внутрішніх справ у звичному порядку, без участі законодавчих органів. Зважаючи на зростання загрози воєнного зіткнення і той факт, що нарешті з'явився закон про відповідальність про державну зраду, у грудні 1912 року МВС скористалося своїм правом. Було складено перелік відомостей, заборонених до друку. Фактично, це і був перший у ХХ ст. Звід відомостей, що становлять державну таємницю. Діяв він протягом одного року з часу публікації. До цього переліку входила інформація: 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, виклик із 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.

В умовах загрози війни зведення поняття державної таємниці до військової складової було зрозумілим. Однак із військового погляду цей перелік був недосконалим і не охоплював низки вкрай важливих для безпеки держави аспектів. Значною мірою на це вплинула переконаність генштабів усіх ворогуючих держав у маневреності й короткотривалості майбутньої війни.

Зважаючи на недосконалість вказаного переліку і закінчення терміну його дії, у січні 1914 року було уведено в дію новий його варіант. Складався він із 10 пунктів і діяв протягом одного року. До нього входили відомості: 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.

Справжня нормотворча лихоманка з питань охорони державної таємниці припадає на переддень Першої світової війни. 12 липня 1914 року був опублікований один перелік, а 20-го, за шість днів до оголошення «Височайшого маніфесту про початок воєнних дій між Росією й Австро-Угорщиною», вже інший. Їх публікація мала на меті не допустити поширення відомостей, що стосуються оборонних питань, у період політичних ускладнень. У переліку було заборонено обговорення в пресі пропускної спроможності залізниць (п. 7), заходів із приводу воєнних дій армії і флоту (п. 15), інформації про роботу інтендантських відомств і військові припаси в Росії й за кордоном (п. 16) та низки інших доповнень.

Перші переліки стосувалися лише друку. Однак 20 липня було видано указ урядовому Сенату, в якому міністр внутрішніх справ зобов'язувався забороняти оголошення відповідної інформації після оголошення мобілізації й під час війни, також у промовах і доповідях на публічних зібраннях. Тоді ж було вирішено підготувати новий перелік, зробивши його обов'язковим не тільки для друку, але й для промов і 26 липня 1914 року був опублікований більш повний перелік із 25 пунктів. У ньому детальніше класифікувалась інформація, що стосувалась штатного розпису, дислокації та мобілізаційної готовності збройних сил, укріплення й інших військових споруд, шляхів сполучення, стратегічних планів. Окремим пунктом засекречувались відомості, що вказували на початок мобілізації.

Розголошення відомостей, що стосуються власне воєнних дій, цим переліком не передбачалось. Та саме з ним Росія вступила в Першу світову війну.

Таким чином, відсутність детального Переліку повідомлень, які становили державну таємницю, призвела до неможливості чіткої градації між таємною інформацією й відкритою. Саме тому досить важко було довести в суді факт того, що розголошена звинувачуваним інформація містила державну таємницю. Спроби змінити ситуацію були здійснені лише в переддень Першої світової війни. Попри те, що поняття таємниці було зведене до військової складової, це був перший звід відомостей, що становлять державну таємницю. У воєнні роки ця робота продовжилась.

На сьогоднішній день в Україні діє загальнодержавна система охорони державної таємниці, що успадкована від колишнього СРСР. Для того періоду характерним є процес тотального засекречування різних відомостей, що в результаті було причиною порушення ряду прав та свобод громадян. Незважаючи на тотальне засекречування інформації у радянські часи, правова основа в сфері охорони державної таємниці не досягла високого рівня, що характеризувалося відсутністю актів, які закріплювали основні інформаційні засади у СРСР. Характерним є те, що більшість відносини у сфері державної таємниці регулювалися на рівні урядових рішень, які у багатьох випадках мали закритий характер та не давали можливості для ознайомлення широкому загалу.

Згодом система охорони державної таємниці почала змінюватися та вдосконалюватися, що було зумовлено новим рівнем міждержавних та інформаційних відносин.

Початком створення сучасної системи охорони державної таємниці можна вважати момент 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».

Законодавчим актом, що заклав фундамент демократичного розвитку інформаційної сфери держави, став прийнятий 2 жовтня 1992 р. Закон України «Про інформацію», який проголошує інформаційний суверенітет України, закріплює право громадян на інформацію, встановлює обов'язок держави здійснювати контроль за інформацією з обмеженим доступом, визначає правові основи інформаційної діяльності в державі. На законодавчому рівні вперше було закріплено необхідність врегулювання відносин у сфері державної таємниці нарівні спеціального закону. Закон України «Про інформацію» визначив місце державної таємниці серед іншої інформації, встановив види відповідальності за порушення інформаційного законодавства, поділив інформацію за режимом доступу на відкриту інформацію та інформацію з обмеженим доступом. Остання за своїм правовим режимом поділяється на конфіденційну і таємну. Саме одним з видів таємної інформації і є державна таємниця.

Найбільш вагомим кроком на шляху побудови сучасної демократичної системи охорони державної таємниці стало прийняття Закону України «Про державну таємницю» 21 січня 1994 р., у якому було закладено правовий фундамент охорони державної таємниці, встановлена процедура віднесення інформації до державної таємниці, а також врегульовано порядок засекречування та розсекречування її матеріальних носіїв, охорона державної таємниці в інтересах національної безпеки України тощо.

Законом України «Про державну таємницю» здійснено розподіл інформації, що може належати до державної таємниці за ступенями секретності: «Особливої важливості», «Цілком таємно» і «Таємно». Визначено не всі, а лише найважливіші сфери життєдіяльності держави, які може охоплювати державна таємниця. Це є відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України. Закон встановив розмежування компетенції державних органів у сфері охорони та забезпечення державної таємниці. Створено механізм віднесення інформації до державної таємниці та її розсекречування. Відповідно до категорій інформації, яка становить державну таємницю, формується Звід відомостей, що становлять державну таємницю (ЗВДТ), який є єдиною формою реєстрації цих відомостей в Україні. Звід відомостей, що становлять державну таємницю України затверджений наказом СБУ від 12 серпня 2005 р. З моменту опублікування Зводу держава забезпечує захист і правову охорону зареєстрованих у ньому відомостей.

Крім спеціального Закону «Про державну таємницю» важливе значення для забезпечення охорони та захисту державної таємниці мають Закони України ««Про основи національної безпеки України», «Про оперативно-розшукову діяльність», «Про захист інформації в автоматизованих системах», «Про доступ до публічної інформації». Серед Постанов Верховної Ради України, що регулюють питання у

сфері охорони державної таємниці, варто виокремити: «Про затвердження положення про порядок оформлення та використання прав на винаходи, корисні моделі і промислові зразки, що становлять державну таємницю» та «Про правила поводження народних депутатів України з таємними документами та інформацією». Важливе значення і інші підзаконні нормативно-правові акти: укази Президента, постанови Кабінету Міністрів тощо, які видаються на виконання законів та з метою їх реалізації. Серед останніх: «Положення про порядок надання, переоформлення та скасування громадянам допуску до державної таємниці», затверджене постановою Кабінету Міністрів України від 29 листопада 2001 р., «Положенням 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»

Особливе значення має охорона державної таємниці на міжнародному рівні. На сьогодні Україна уклала майже 40 окремих Угод про взаємний захист секретних відомостей з іноземними державами, у вересні 2002 р. таку угоду ратифіковано з НАТО, проте визнання Урядом України існування міждержавних секретів (у межах відповідних Угод) не означає автоматичного набуття такими секретами статусу державної таємниці України.

Міждержавні секрети, що передаються у зв’язку із певними обставинами у розпорядження відповідних державних органів України, згідно із ст. 8 Закону України «Про державну таємницю» можуть бути віднесені до державної таємниці України лише за умови, якщо вони підпадають під категорії, зазначені у цій статі, і їх розголошення може завдати шкоди інтересам національної безпеки України [3].

Важливою складовою забезпечення хорони та захисту державної таємниці є встановлення відповідальності за протиправні дії у цій сфері. За порушення правил поводження з державною таємницею встановлюється: дисциплінарна, адміністративна та кримінальна відповідальність. Так, Дисциплінарний Статут органів внутрішніх справ передбачає накладення дисциплінарних стягнень на осіб рядового і начальницького складу за вчинення дисциплінарних проступків.

Відповідальність за злочини у сфері охорони державної таємниці передбачена Особливою частиною КК за такі діяння: ст. 111 «Державна зрада» (у формі шпигунства), 114 «Шпигунство», 328 «Розголошення державної таємниці», 329 «Втрата документів, що містять державну таємницю», 422 «Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості». Так, наприклад, відповідно до ст. 328 КК України розголошення відомостей, що становлять державну таємницю, особою, якій ці відомості були довірені або стали відомі у зв’язку з виконанням службових обов’язків, за відсутності ознак державної зради або шпигунства карається позбавленням волі на строк від двох до п’яти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. Те саме діяння, якщо воно спричинило тяжкі наслідки, – карається позбавленням волі на строк від п'яти до восьми років. За порушення правил поводження з державною таємницею ст. 212-2 КУпАП передбачає адміністративну відповідальність, у диспозиції якої визначено досить

багато складів порушення, серед яких: порушення встановленого законодавством порядку надання допуску та доступу до державної таємниці; безпідставне засекречування інформації та ін.

2. 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.

У визначенні державної таємниці мають місце 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. Під шкодою розуміються як економічні збитки так й інші тяжкі наслідки. Економічно, шкода визначається матеріальними збитками у кількісному (вартісному) виразі, які сталися чи можуть статися внаслідок розголошення конкретних відомостей, що становлять державну таємницю у сферах оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки і охорони правопорядку. Щодо інших тяжких наслідків, то вони пов'язуються з негативними змінами у зазначених сферах (головним чином, у сферах зовнішніх відносин, державної безпеки і охорони правопорядку), які відбулися чи можуть відбутися внаслідок розголошення конкретних відомостей, що становлять державну таємницю і які не піддаються економічному обрахунку у вартісному виразі.

– Чітке визначення сфер, у яких може існувати державна таємниця, а саме: оборона, економіка, наука і техніка, зовнішні відносини, державна безпека й охорона правопорядку.

– Фіксація відомостей, що становлять державну таємницю, законом, тобто встановлення переліку таких відомостей у спеціальному. правовому акті – Зводі, на підставі та в межах якого створюються розгорнуті переліки відомостей, що становлять державну таємницю (формальний критерій);

– Охорона здійснюється державою. На відміну від інших видів інформації (банківської, комерційної) фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею в бюджетних установах і організаціях має здійснюватися за рахунок Державного бюджету України.

До державної таємниці у порядку, встановленому Законом України «Про державну таємницю», відноситься інформаці:

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 напрями розвитку окремих видів озброєння, військової і спеціальної техніки, їх кількість, тактико-технічні характеристики, організацію і технологію виробництва, наукові, науково-дослідні та дослідно-конструкторські роботи, пов'язані з розробленням нових зразків озброєння, військової і спеціальної техніки або їх модернізацією, а також про інші роботи, що плануються або здійснюються в інтересах оборони країни;

– про сили і засоби Цивільної оборони України, можливості населених пунктів, регіонів і окремих об'єктів для захисту, евакуації і розосередження населення, забезпечення його життєдіяльності та виробничої діяльності об'єктів народного господарства у воєнний час або в умовах надзвичайних ситуацій;

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

2) у сфері економіки, науки і техніки:

– про мобілізаційні плани і мобілізаційні потужності господарства України, запаси та обсяги постачання стратегічних видів сировини і матеріалів, а також зведені відомості про номенклатуру та рівні накопичення, про загальні обсяги поставок, відпуску, закладення, освіження, розміщення і фактичні запаси державного резерву;

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

– про плани, зміст, обсяг, фінансування та виконання державного замовлення для забезпечення потреб оборони та 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 підроблення, обігом, обміном або вилученням з обігу, а також про інші особливі заходи фінансової діяльності держави;

– про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, на базі яких можуть бути створені прогресивні технології, нові види виробництва, продукції та технологічних процесів, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України;

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;

4) у сфері державної безпеки та охорони правопорядку:

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

– про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової 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 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 органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, державні програми, плани та інші заходи у сфері охорони державної таємниці;

– про організацію, зміст, стан і плани розвитку технічного захисту секретної інформації;

– про результати перевірок, здійснюваних згідно з законом прокурором у порядку відповідного нагляду за додержанням законів, та про зміст матеріалів дізнання, досудового слідства та судочинства з питань, зазначених сфер;

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

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

Не відноситься до державної таємниці інформація:

– 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 і 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 і культури населення;

– про факти порушень прав і свобод людини і громадянина;

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

– інша інформація, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена.

3. 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.

Органи державної влади, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов'язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею.

Надання дозволу здійснюється на підставі заявок органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій та результатів спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею. З метою визначення наявності умов для провадження діяльності, пов'язаної з державною таємницею, Служба безпеки України може створювати спеціальні експертні комісії, до складу яких включати фахівців органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій за погодженням з їх керівниками. Результати спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, оформляються відповідним актом.

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.

Керівники органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, що провадять діяльність, пов’язану з державною таємницею, мають бути обізнані з чинним законодавством про державну таємницю.

Термін дії дозволу на провадження діяльності, пов’язаної з державною таємницею, встановлюється Службою безпеки України і не може перевищувати 5 років. Його тривалість залежить від обсягу робіт (діяльності), що здійснюються органом державної влади, органом місцевого самоврядування, підприємством, установою, організацією, ступеня секретності та обсягу пов’язаних з цими роботами (діяльністю) відомостей, що становлять державну таємницю.

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, передбачених цією статтею.

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.

Органи державної влади, органи місцевого самоврядування, підприємства, установи і організації, яким надано зазначений у цій статті дозвіл, набувають права на доступ до конкретної секретної інформації згідно з рішенням органів державної влади, уповноважених державним експертом з питань таємниць приймати такі рішення. За погодженням з цими органами здійснюється передача секретної інформації або її матеріальних носіїв органам державної влади, органам місцевого самоврядування, підприємствам, установам і організаціям, які мають дозвіл на провадження діяльності, пов’язаної з державною таємницею.

Порядок надання, переоформлення, зупинення дії або скасування дозволу на провадження діяльності, пов’язаної з державною таємницею, форма акта спеціальної експертизи щодо наявності умов для провадження діяльності, пов’язаної з державною таємницею, форма дозволу на провадження діяльності, пов’язаної з державною таємницею, та категорії режиму секретності встановлюються Кабінетом Міністрів України.

4. 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.

Умовно структуру системи охорони державної таємниці поділяють на три рівні, які знаходяться у взаємозв'язках один з одним. 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.

Для більш детальної характеристики системи охорони державної таємниці, в науковій літературі пропонують поділяти останню на чотири підсистеми: 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 статей 102,106 Конституції України) є гарантом державного суверенітету, територіальної цілісності України; Верховним Головнокомандувачем Збройних Сил України;здійснює керівництво у сферах національної безпеки та оборони держави; забезпечує державну незалежність, національну безпеку і правонаступництво держави; очолює Раду національної безпеки та оборони, а також встановлює порядок технічного та криптографічного захисту секретної інформації; встановлює більш тривалі строки дії рішень про віднесення інформації до державної таємниці, ніж строки, передбачені частиною першою статті 13 Закону «Про держану таємницю».

– Рада національної безпеки та оборони при Президентові України відповідно до Закону України «Про Раду національної безпеки і оборони України» (від 05.03.1998 № 183/98-ВР)) розробляє та розглядає питання і подає пропозиції (щодо визначення стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення національної безпеки у воєнній, інформаційній та інших сферах; удосконалення системи забезпечення національної безпеки та організації оборони, заходи воєнного, інформаційного та іншого характеру відповідно до масштабу потенційних та реальних загроз національним інтересам України; тощо); координує і контролює діяльність центральних і місцевих органів виконавчої влади у сфері національної безпеки та оборони.

– Верховна Рада України (за статтею 4 Закону України «Про державну таємницю»), визначає державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики, а також, відповідно до статті 85 Конституції України, оголошує за поданням Президента України стан війни і укладення миру, схвалює рішення Президента України про використання Збройних сил України та інших військових формувань у разі збройної агресії проти України; призначає на посаду та звільняє з посади за поданням Президента України Голову Служби Безпеки України; затверджує загальну структуру, чисельність, визначає

функції Служби Безпеки України, Збройних сил України інших утворених відповідно до законів України військових формувань, а також Міністерства внутрішніх справ України; тощо.

– Кабінет Міністрів України (відповідно до Закону України «Про Кабінет Міністрів України» (від 27.02.2014 № 794- VII)), здійснює заходи щодо забезпечення обороноздатності та національної безпеки України, громадського порядку, боротьби із злочинністю, ліквідації наслідків надзвичайних ситуацій; спрямовує та координує роботу міністерств, інших ОВВ, здійснення контролю за їх діяльністю, у тому числі, щодо здійснення державної політики у сфері охорони державної таємниці. Відповідно до Закону України «Про державну таємницю», визначає порядок реєстрації рішень державних експертів з питань таємниць, встановлює: порядок та механізм формування ЗВДТ (звід відомостей); єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передачі та транспортування матеріальних носіїв секретної інформації; порядок надання, переоформлення, зупинення та поновлення дії або скасування дозволу на провадження діяльності, пов'язаної з державною таємницею, форму акта спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, форму дозволу на провадження діяльності, пов'язаної з державною таємницею, та категорії режиму секретності; порядок надання, переоформлення та скасування громадянам допуску до державної таємниці та форми необхідних документів; порядок проведення перевірки громадян у зв'язку з їх допуском до державної таємниці; порядок надання, види, розміри компенсації за роботу у режимних обмеженнях.

– 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 №987/2009) здійснювати, у межах компетенції визначеної Законом України «Про державну таємницю», віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування.

2) Міністерства і центральні ОВВ (здійснюють у межах своїх повноважень державну політику щодо сфери охорони державної таємниці):

– Міністерство оборони України є головним органом у системі центральних органів виконавчої влади у формуванні та реалізації державної політики з питань національної безпеки у воєнній сфері, сфері оборони і військового будівництва, а також у формуванні державної політики у сферах цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню; здійснює в межах повноважень державну політику щодо охорони державної таємниці; проводить розвідувальну та інформаційно-аналітичну діяльність в інтересах національної безпеки та оборони держави; провадить діяльність із технічного захисту інформації для власних потреб; здійснює постійний моніторинг інформаційного середовища, виявляє потенційні та реальні інформаційні загрози в оборонній сфері, проводить попереджувальні інформаційні заходи.

– Міністерство закордонних справ України є головним органом у системі центральних органів виконавчої влади у формуванні та забезпеченні реалізації

державної політики у сфері зовнішніх зносин України забезпечує дипломатичними засобами захисту та зміцнює незалежність, державний суверенітет, безпеку, територіальну цілісність та непорушності кордонів України, її національні інтереси; забезпечує розроблення та реалізацію заходів з охорони державної таємниці в системі органів дипломатичної служби при здійсненні зовнішніх зносин та інше.

– Міністерства внутрішніх справ України за «Положення про Міністерство внутрішніх справ України» від 06.04.2011 №383/2011 є головним органом у системі центральних органів виконавчої влади у формуванні та реалізації державної політики у сфері захисту прав і свобод людини та громадянина, власності, інтересів суспільства і держави від злочинних посягань, боротьби зі злочинністю, розкриття та розслідування злочинів, охорони громадського порядку, забезпечення громадської безпеки, безпеки дорожнього руху, а також з питань формування державної політики у сферах міграції (імміграції та еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів у межах компетенції, визначеної законодавством, організовує та здійснює оперативно-розшукову діяльність; забезпечує криптографічний захист інформації, яка є власністю держави; забезпечує реалізацію державної політики стосовно державної таємниці, а також технічний захист інформації, контроль за їх збереженням в апараті Міністерства Внутрішніх Справ.

– 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, які здійснюють на відповідних територіях державний контроль за додержанням законодавства про державну таємницю та інформацію, а також забезпечують у межах своїх повноважень реалізацію державної політики стосовно захисту інформації з обмеженим доступом та захист персональних даних.

Органи місцевого самоврядування, підприємства, установи і організації, що провадять діяльність, пов'язану з державною таємницею повинні мати дозвіл на провадження такої діяльності, брати участь у діяльності, пов'язаній з державною таємницею, відповідно до компетенції, державних завдань, програм, замовлень, договорів (контрактів); мати приміщення для проведення робіт, пов'язаних з державною таємницею, сховища для зберігання засекречених документів, додержуватись передбачених законодавством вимог режиму секретності робіт та інших заходів, пов'язаних з використанням секретної інформації, порядку допуску осіб до державної таємниці, прийому іноземних громадян, а також порядку здійснення технічного та криптографічного захисту секретної інформації; мати режимно-секретний орган.

– Режимно-секретні органи – це окремі структурні підрозділи, які розробляють та здійснюють заходи щодо забезпечення режиму секретності, постійно контролюють за їх додержанням і підпорядковуються безпосередньо керівнику державного органу, органу місцевого самоврядування, підприємства,

установи, організації, що провадить діяльність, пов'язану з державною таємницею.

До підсистеми забезпечення та контролю належать:

– Суди загальної юрисдикції забезпечують охорону державної таємниці під час здійснення правосуддя при розгляді справ; здійснюють судовий захист прав і свобод громадян, інтересів органів державної влади, підприємств, установ, організацій у зв'язку з їх діяльністю щодо охорони державної таємниці України.

– Прокуратура України забезпечує представництво державних інтересів щодо охорони державної таємниці у судах; здійснює нагляд за дотриманням Конституції і Законів України.

– Служба Безпеки України – спеціально уповноважений державний орган у сфері забезпечення охорони державної таємниці бере участь у розробці і здійсненні заходів щодо забезпечення охорони державної таємниці та здійснювати контроль за додержанням порядку обліку, зберігання і використання документів та інших матеріальних носіїв, що містять службову інформацію, зібрану у процесі охорони державної таємниці, контррозвідувальної діяльності, у сфері оборони країни, сприяти у порядку, передбаченому законодавством, підприємствам, установам, організаціям та підприємцям у збереженні комерційної таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України; формує Звід Відомостей і вносить зміни нього; погоджують розгорнуті переліки відомостей, що становлять державну таємницю; встановлюють критерії визначення ступеня секретності інформації; проводять спеціальні експертизи щодо наявності умов для провадження діяльності, пов'язаної з держтаємницею; погоджують створення, реорганізацію та ліквідацію режимно-секретних органів; проводять перевірку громадян у зв'язку із допуском до державної таємниці; вносить Президенту України пропозиції про видання актів з питань збереження державної таємниці, обов'язкових для виконання органами державного управління, підприємствами, установами, організаціями і громадянами.

– Служба зовнішньої розвідки України здійснює спеціальні заходи впливу, спрямованих на підтримку національних інтересів і державної політики України в інформаційній та інших сферах; приймає участь у забезпеченні безпечного функціонування установ України за кордоном, безпеки співробітників цих установ та членів їх сімей у країні перебування, а також відряджених за кордон громадян України, які обізнані з відомостями, що становлять державну таємницю тощо.

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..

Тема 3. Процедура віднесення інформації до державної таємниці

Доекспертна стадія віднесення інформації до державної таємниці. Стадія експертного розгляду інформації для прийняття рішення про віднесення її до державної таємниці. Стадія формалізації рішення. Основні засади віднесення відомостей що містять ознаки державної таємниці до різних ступенів секретності.

1. Віднесення інформації до державної таємниці є ключовим моментом реалізації практичних аспектів охорони державної таємниці. Визначення поняття “віднесення інформації до державної таємниці” відповідно до ст. 1 Закону України “Про державну таємницю ” виокремлює три основні складові процесу віднесення: 1) 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; 2) включення цієї інформації до Зводу відомостей, що становлять державну таємницю; 3) опублікування змін до Зводу відомостей, що становлять державну таємницю (ЗВДТ). Процедура віднесення інформації до державної таємниці – це складне багато аспектне явище, яке не можна зводити лише до трьох перерахованих вище формалізованих дій. Відносячи інформацію до державної таємниці суб’єкти системи охорони державної таємниці (СОДТ) виконують певні послідовні дії. Звідси, віднесенню характерна тривалість у часі та алгоритмічність, при якій після певної виконаної дії повинна наступати чітко визначена наступна. А, отже, віднесення інформації до державної таємниці – це процес, а не одномоментна дія. Будь-який процес із метою кращої ясності та чіткішого його дотримання варто розбивати на послідовні ланки – етапи (стадії). 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. Проте у чинному законодавстві та підзаконних актах немає чітко виділеної етапної структури віднесення, що, є явним недоліком, подолання якого дозволить зрозуміти, зокрема, хто і в яких межах є відповідальний за кожну із ланок віднесення.

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

Державний експерт з питань таємниць здійснює відповідно віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування.

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. Втручання в діяльність державного експерта з питань таємниць особи, якій за посадою його підпорядковано, не допускається.

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

1) визначає:

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

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

– 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;

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

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

4) 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;

5) затверджує за погодженням із Службою безпеки України розгорнуті переліки відомостей, що становлять державну таємницю, зміни до них, контролює відповідність змісту цих переліків Зводу відомостей, що становлять державну таємницю;

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

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

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

9) бере участь:

– у 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:

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

2) подавати Службі безпеки України не 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;

3) 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;

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

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

Державний експерт з питань таємниць має право:

1) 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;

2) 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;

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

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

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

Державним експертам з питань таємниць, а також фахівцям, які залучаються до підготовки рішень та висновків державних експертів з питань таємниць, встановлюються додаткові виплати у порядку і розмірах, що визначаються законодавством.

Державний експерт з питань таємниць несе персональну відповідальність за законність і обгрунтованість 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.

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

Державний експерт з питань таємниць відносить інформацію до державної таємниці з питань, прийняття рішень з яких належить до його компетенції згідно з посадою. У разі, якщо прийняття рішення про віднесення інформації до державної таємниці належить до компетенції кількох державних експертів з питань таємниць,

воно за ініціативою державних експертів або за пропозицією Служби безпеки України приймається колегіально та ухвалюється простою більшістю голосів. При цьому кожен експерт має право викласти свою думку.

Відповідно до вимог законодавства, 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.

У зв'язку з цим віднесення відомостей до державної таємниці та їх засекречування повинно здійснюватися у відповідності з принципами законності, обґрунтованості і своєчасності.

Принцип законності віднесення відомостей до державної таємниці та їх засекречування полягає у відповідності відомостей, які мають бути віднесені до державної таємниці та засекречені, положенням законодавства про державну таємницю.

Принцип обґрунтованості віднесення відомостей до державної таємниці та їх засекречування полягає у встановленні шляхом експертної оцінки доцільності віднесення до державної таємниці і засекречування конкретних відомостей, імовірних економічних та інших наслідків цього акту, виходячи із балансу життєво важливих інтересів держави, суспільства, громадян.

Принцип своєчасності віднесення відомостей до державної таємниці та їх засекречування полягає у встановленні обмежень та поширення цих відомостей з моменту їх отримання (розробки) або завчасно.

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

•забезпечити баланс інтересів особи, суспільства, держави;

•всебічно врахувати доцільність віднесення відомостей до державної таємниці, виходячи із можливих позитивних і негативних наслідків цього акту;

•забезпечити обіг відомостей віднесених до державної таємниці в умовах своєчасно обмежених режимними заходами;

•здійснювати витрати коштів на захист тільки тих відомостей, розголошення яких завдаватиме шкоди життєво важливим національним інтересам.

Проте розгляд державним експертом інформації на предмет її належності до державної таємниці є хоча й основним, але не єдиним етапом віднесення інформації до державної таємниці. До того, як певна інформація потрапляє до державного експерта, вона, як правило, повинна пройти, умовно кажучи, доекспертний відбір. Передусім об'єктивно виникає потреба у віднесенні або, інакше кажучи, відбувається актуалізація певної інформації у процесі здійснення захисту національної безпеки як об'єктивний наслідок безперервного розвитку суспільства та держави. Конкретна потреба у віднесенні – це певна визначена інформація чи категорія інформації, яка потребує захисту у статусі державної таємниці. Поряд із потребою завжди виникає потенційна загроза завдання шкоди національній безпеці у разі витоку такої інформації. Але до того часу поки зазначена потреба не буде ідентифікована та стосовно неї не почнуться конкретні дії не можемо говорити про початок процесу віднесення, оскільки сама по собі потреба (проблема) може існувати невизначено довго в часі і не завжди її наявність породжує початок процесу віднесення.

Наявність потреби у віднесенні є обов'язковою передумовою процесу

віднесення, проте його початок – не обов'язковий наслідок її виникнення. Потреба у віднесенні повинна відповідати таким ознакам: перебувати в належній сфері; бути актуальною на момент її виявлення; відповідати належному рівню потенційного завдання шкоди. Вимога належної сфери полягає у тому, що потреба у віднесенні повинна локалізуватися у сфері оборони; економіки; науки і техніки; зовнішніх відносин; державної безпеки та охорони правопорядку. Актуальність на момент виявлення – така потреба 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).

З моменту виявлення потреби у віднесенні можемо говорити про початок першого етапу віднесення, який назвемо *етапом ініціювання віднесення*. Далеко не завжди потреба виявляється експертами. Суб'єктами виявлення можуть бути і режимно-секретні органи підприємств, установ чи організацій, і міністерства, і державні агентства, і комітети Верховної Ради України, і окремі громадяни тощо. Виявлення потреби може відбуватися по-різному: шляхом постійного моніторингу певної галузі, унаслідок планового перегляду актуальності та важливості інформаційних масивів галузі, під час виробничої, наукової чи управлінської діяльності тощо. Виявлення потреби у віднесенні є єдиним поштовхом та відповідно обов'язковим елементом процесу віднесення інформації до державної таємниці. На цьому етапі 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. Потреби у віднесенні інформації до державної таємниці виникають постійно і часто не прогнозовано, що є наслідком динамічності системи охорони державної таємниці. У разі, якщо виникає об'єктивна потреба у віднесенні інформації, але її вчасно не буде помічено, може завдатися уже реальна шкода національній безпеці.

Отже, дуже важливим є вчасне виявлення потреб у віднесенні інформації до державної таємниці. Проте зазначений етап не буде повним, коли поряд із самою ідентифікацією потреби не буде вжито заходів для захисту такої інформації та передачі питання про її розгляд на предмет її належності до державної таємниці державним експертам з питань таємниць або іншим компетентним органам (СБ України, вищі інстанції підприємства тощо). Вони можуть полягати, наприклад, у написанні офіційного звернення, зборі відомостей, що підтверджують важливість цієї інформації чи готуванні відповідних документів, в яких би надавалася попередня оцінка інформації. Тобто для початку першого етапу недостатньо лише виявити потребу у віднесенні, а потрібно також здійснити усі належні заходи реагування на неї, зовнішнім виразником яких повинні бути документальні акти (інформування належних відомств, звернення до державних експертів з питань таємниць тощо). Не можна говорити про зняття зазначеної 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, що не виключає можливості помилки, а, по-друге, не

кожен розгляд потреби у віднесенні повинен закінчуватися власне віднесенням до державної таємниці, оскільки вона має характер необхідності в розгляді питання саме про можливість чи неможливість її віднесення і може існувати якщо її хоча б розділяє один суб'єкт СОДТ.

Наступним етапом віднесення після ідентифікації потреби та первинної реакції на неї є її направлення 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. Варто зазначити, що не завжди суб'єкти звернень є ті самі, що виявили потребу у віднесенні інформації до державної таємниці України. Наприклад, потреба була виявлена режимно-секретним органом підприємства, що, у свою чергу, звернулося до СБ України, яка вже офіційно надіслала звернення до належного державного експерта. Тобто цей етап, є *етапом передачі питання про віднесення певної інформації до державної таємниці на розгляд державному експерту з питань таємниць*, містить увесь шлях проходження інформації про потребу у віднесенні від суб'єкта, що її виявив, до суб'єкта, що приймає із цього питання кінцеве рішення – державного експерта з питань таємниць. У цьому етапі може брати участь будь-який суб'єкт СОДТ. До експерта крім факту наявності потреби у віднесенні направляється усе зібране її обґрунтування. У разі, якщо ініціатором розгляду є державний експерт самостійно, тоді закономірно відсутній етап передачі, але не виключений той факт, що необхідність розгляду питання про віднесення була донесена до нього, наприклад, підлеглими особами.

Отже, доходимо висновку, що цей етап не є обов'язковим у випадку власної ініціативи експерта, але його наявність є обов'язковою підставою розгляду експертом питання про віднесення інформації до державної таємниці. Зазначені перші два етапи утворюють *доекспертну стадію* віднесення.

2. Після доекспертної стадії слідує *стадія експертного розгляду*. Її законодавче розуміння міститься у ст. 1 Закону України "Про державну таємницю", а саме – "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". На цій стадії оцінюється інформація державним експертом з питань таємниць, на основі якої ним приймається рішення про її віднесення до державної таємниці або про відмову від нього, а також у разі позитивного рішення про присвоєння такій інформації чи певній її категорії відповідного ступеня секретності.

Для проведення належної оцінки інформація аналізується, доповнюється додатковими даними, надається на розгляд фахівцям відповідної галузі (експертна комісія). Документальним закріпленням цієї стадії є рішення державного експерта з питань таємниць про віднесення інформації до державної таємниці або обґрунтована відмова у прийнятті такого рішення.

Належність інформації до державної таємниці з огляду на її законодавче визначення необхідно визначати через рівень потенційного завдання шкоди національній безпеці. Етапи часткової та повної селекції в стадії експертного розгляду виокремленні досить умовно, оскільки описані ними дії виконуються ще під час попередньої оцінки інформації на етапі ідентифікації та реакції на потребу

у віднесенні. Суб'єктами на стадії експертного розгляду є державні експерти та створені ними експертні комісії. Після надходження офіційного звернення на ім'я експерта про розгляд питання на предмет віднесення певної інформації до державної таємниці чи у випадку власної ініціативи державного експерта, як правило, попередній висновок – рекомендацію надає експертна комісія, як дорадчий орган державного експерта з питань таємниць, вона також готує проект рішення державного експерта. На самому початку комісія, як правило, проводить часткову та повну селекцію інформації та визначається з необхідністю та обсягом отримання додаткових матеріалів. Проте бувають випадки, коли кількість матеріалу достатньою для прийняття належного рішення і збирання додаткових відомостей є непотрібним. У зв'язку із цим *збирання додаткових матеріалів,* що необхідні для прийняття рішення, виокремлюємо в окремий факультативний етап. Після їхнього надходження 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.

Останній четвертий етап стадії експертного розгляду завершує рішення державного експерта. Він абсолютно не пов'язаний із рекомендаціями експертної комісії, але при цьому вся відповідальність за рішення покладається лише на нього. 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. Зазначені вище етапи, на нашу думку, є найоптимальнішим поділом стадії експертного розгляду. Для успішного проходження інформацією стадії експертного розгляду слід дотримуватися низки вимог, а саме: питання про віднесення повинно розглядатися належним 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 повинен бути наділений достатніми повноваженнями для збирання додаткової інформації, що потрібна для збирання рішення; часові строки стадії, які встановлюються законом, повинні бути не меншими тим затратам часу, що реально необхідні для прийняття обґрунтованого рішення.

Найбільше питань виникає до методики обрахування шкоди. На сьогодні вона визначається Методичними рекомендаціями державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей додержавної таємниці та ступеня їх секретності, які є застарілими і фактично не використовуються, а державні експерти та члени експертних комісій приймають рішення зважаючи на власний досвід, що надає рішенню суб'єктивності. Після прийняття остаточного рішення експертом про віднесення інформації до державної таємниці воно надсилається в СБ України. З цього моменту настає *стадія формалізації рішення*.

3. На першому етапі стадії формалізації рішення орган СБ України здійснює перевірку рішення державного експерта на предмет відповідності встановленим законодавством вимогам (передусім Конституції України, Закону України "Про державну таємницю" тощо). У разі наявності недоліків (недостатня мотивувальна

частина, відсутність обов'язкових реквізитів тощо) рішення повертається державному експерту на доопрацювання. Лише після відсутності зауважень до формально-юридичної частини рішення воно згодом включається до ЗВДТ, про що видається відповідний наказ. Спецслужба у цьому випадку є контролюючим органом, проте вона не може впливати на зміст самого рішення, а лише здійснює його перевірку на відповідність законодавству. Даний етап є *етапом узгодження рішення державного експерта із СБ України.* Його мета – не допустити набуття законної сили рішеннями, що прийнятті всупереч закону чи не відповідають його вимогам.

Наступним етапом є *етап внесення змін у ЗВДТ та їх юридичне оформлення.* Він полягає у тому, що на основі нових рішень державних експертів СБ України, як відповідальний за укладання ЗВДТ орган, вносить до цього документа зміни протягом не більше як трьох місяців та надсилає його нову редакцію до Міністерства юстиції України на реєстрацію. Після належної реєстрації в Міністерстві юстиції наступає останній 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. Наступним етапом, який обов'язково слідує за опублікуванням нового ЗВДТ чи змін до нього, є приведення матеріальних носіїв інформації у відповідність із новим ЗВДТ чи змінами до нього. Але цей етап уже виходить за межі процесу віднесення і виникає як наслідок останнього.

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. Цей висновок набирає чинності з моменту внесення Службою безпеки України змін до 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.

Рішення (висновок) державного експерта (експертів) з питань таємниць, видане в межах його (їх) повноважень і зареєстроване Службою безпеки України у Зводі відомостей, що становлять державну таємницю, є обов'язковим для виконання на території України.

У рішенні державного експерта з питань таємниць зазначаються:

– інформація, яка має становити державну таємницю;

– підстави для віднесення інформації до державної таємниці та обгрунтування 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.

Звід відомостей, що становлять державну таємницю, формує та публікує в офіційних виданнях Служба безпеки України на підставі рішень державних експертів з питань таємниць.

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.

На підставі та в межах Зводу відомостей, що становлять державну таємницю, з метою конкретизації та систематизації даних про секретну інформацію 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 незалежно від форм власності, що провадять діяльність, пов'язану із державною таємницею, за ініціативою та погодженням із замовником робіт, пов'язаних з державною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю. Такі переліки погоджуються із Службою безпеки України, затверджуються державними експертами з питань таємниць та реєструються у Службі безпеки України.

Розгорнуті переліки відомостей, що становлять державну таємницю, не можуть суперечити Зводу відомостей, що становлять державну таємницю.

У разі включення до Зводу відомостей, що становлять державну таємницю, або до розгорнутих переліків цих відомостей інформації, яка не відповідає категоріям і вимогам або порушення встановленого порядку віднесення інформації до державної таємниці заінтересовані громадяни та юридичні особи мають право оскаржити відповідні рішення до суду. З метою недопущення розголошення державної таємниці судовий розгляд скарг може проводитися в закритих засіданнях відповідно до закону.

Процедура віднесення складається із низки послідовних та нормативно регламентованих дій суб'єктів СОДТ. Це, у свою чергу, означає, що йому властиві ознаки правового процесу, що має зовнішні юридичні наслідки. Для його дотримання та можливістю ведення за ним контролю з боку громадськості він вимагає максимальної чіткості та ясності для усіх належних суб'єктів.

Таким чином, можна виділити три стадії та десять етапів, а саме: 1) *доекспертна стадія:* а) етап ініціювання процесу віднесення; б) етап передачі питання про віднесення певної інформації до державної таємниці на розгляд державному експерту з питань таємниць; 2) *стадія експертного розгляду*: а) етап попередньої селекції інформації, що може належати до державної таємниці; б) етап остаточної селекції інформації, що може належати до державної таємниці; в) етап збору додаткових матеріалів; г) визначення рівня можливої шкоди національній безпеці України; ґ) етап прийняття рішення щодо віднесення інформації до державної таємниці та визначення ступеня її секретності; 3) *стадія формалізації рішення*: а) етап узгодження рішення державного експерта із СБ України; б) етап внесення змін у ЗВДТ та їх юридичне оформлення; в) етап оприлюднення змін до Зводу відомостей, що становлять державну таємницю.

4. *Строк, протягом якого діє рішення про віднесення інформації до державної таємниці,* встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, та інших обставин. Він не може

перевищувати для інформації із ступенем секретності *«особливої важливості» – 30 років*, для інформації *«цілком таємно» – 10 років*, для інформації *«таємно» – 5 років.*

Після закінчення передбаченого строку дії рішення про віднесення інформації до державної таємниці державний експерт з питань таємниць робить висновок про скасування рішення про віднесення її до державної таємниці або приймає рішення про продовження строку дії зазначеного рішення в межах строків.

Президент України з власної ініціативи або на підставі пропозицій державних експертів з питань таємниць чи за зверненням органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій чи громадян 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.

Якщо реквізити, неможливо нанести безпосередньо на матеріальний носій секретної інформації, вони мають бути зазначені у супровідних документах.

Забороняється надавати грифи секретності, матеріальним носіям іншої таємної інформації, яка не становить державної таємниці, або конфіденційної інформації.

Перелік посад, які дають право посадовим особам, що їх займають, надавати матеріальним носіям секретної інформації грифи секретності, затверджується керівником органу державної влади, органу місцевого самоврядування, підприємства, установи, організації, що провадить діяльність, пов’язану з державною таємницею.

Ступені секретності науково-дослідних, дослідно-конструкторських і проектних робіт, які виконуються в інтересах забезпечення національної безпеки та оборони держави, встановлюються державним експертом з питань таємниць, який виконує свої функції у сфері діяльності замовника, разом з підрядником.

Після закінчення встановлених строків засекречування матеріальних носіїв інформації та у разі підвищення чи зниження визначеного державним експертом з

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

Строк засекречування матеріальних носіїв інформації має відповідати строку дії рішення про віднесення інформації до державної таємниці, встановленого рішенням державного експерта з питань таємниць.

Перебіг строку засекречування матеріальних носіїв інформації починається з часу надання їм грифа секретності.

Громадяни та юридичні особи мають право внести посадовим особам, які надали гриф секретності матеріальному носію секретної інформації, обов'язкову для розгляду мотивовану пропозицію про розсекречування цього носія інформації. Зазначені посадові особи повинні протягом одного місяця дати громадянину чи юридичній особі письмову відповідь з цього приводу.

Рішення про засекречування матеріального носія інформації може бути оскаржено громадянином чи юридичною особою в порядку підлеглості вищому органу або посадовій особі чи до суду. У разі незадоволення скарги, поданої в порядку підлеглості, громадянин або юридична особа мають право оскаржити рішення вищого органу або посадової особи до суду.

Тема 4. Правовий захист комерційної таємниці.

Правове регулювання захисту комерційної таємниці в Україні. Правова характеристика уніфікованих основ захисту комерційної таємниці в міжнародному праві. Механізм визначення переліку інформації, що становить комерційну таємницю. Інформація, що не може бути визначена підприємством комерційною таємницею. Юридичне закріплення права підприємства на комерційну таємницю. Дії організаційного, технічного та психологічного характеру по управлінню комерційною таємницею на підприємстві.

1. Термін « комерційна таємниця» був вперше введений у правовий обіг Законом України «Про підприємства в Україні» (втратив чинність з 01.01.2004 р.). Згідно зі статтею 30 цього Закону під комерційною таємницею підприємства розуміють відомості, пов'язані з виробництвом , технологічною інформацією, управлінням , фінансами та іншою діяльністю підприємства , що не є державною таємницею , розголошення (передача, витік) яких може завдати шкоди його інтересам.

У подальшому положення цього Закону щодо комерційної таємниці знайшли свій розвиток і законодавче закріплення в Цивільному і Господарському кодексах України , які були введені в дію в 2004 році.

У розумінні статті 505 Цивільного кодексу України комерційною таємницею

є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Подібне тлумачення знаходимо також у статті 36 Господарського кодексу України, відповідно до положень якої 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. Склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання самостійно, відповідно до законодавства.

Також необхідно зазначити, що статтею 231 Кримінального кодексу України встановлено відповідальність за умисні дії, спрямовані на отримання відомостей, які становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності. Статтею 232 Кримінального кодексу України встановлена кримінальна відповідальність за умисне розголошення комерційної таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо такі дії вчинені з корисливих чи інших особистих мотивів і завдали істотної шкоди суб'єкту господарської діяльності. У разі відсутності істотної шкоди за такі дії передбачена адміністративна відповідальність відповідно до ч. 3 ст. 164-3 Кодексу України про адміністративні правопорушення.

Аналіз нормативно-правових актів, які визначають правовий режим комерційної таємниці, а також специфіка комерційної таємниці як об'єкта правового регулювання дозволяє зробити класифікацію гарантій збереження комерційної таємниці на гарантії, що забезпечують: реалізацію права на комерційну таємницю; охорону комерційної таємниці; захист права на комерційну таємницю; гарантії, залучення до юридичної відповідальності за порушення права на комерційну таємницю.

До гарантій, що забезпечує реалізацію права на комерційну таємницю, відносяться:

а) конституційні гарантії. Ст.ст. 41, 42, 54 Конституції України, які закріплюють право кожного володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності, на підприємницьку діяльність, яка не заборонена законом; свободу літературної, художньої, наукової і технічної творчості;

б) гарантії, закріплені в Законі України «Про інформацію», що носять міжгалузевий характер: що визначають право на інформацію, забезпечене наявністю відповідних режимів, в тому числі режиму конфіденційності щодо інформації комерційного характеру;

в) гарантії, закріплені в ГК України. Ст. 47 ГК України встановлює загальні гарантії прав підприємців, незалежно від обраних ними організаційних форм підприємницької діяльності. Держава надає рівні права і можливості для залучення і використання матеріально-технічних, фінансових, трудових, інформаційних, природних та інших ресурсів;

г) гарантії, закріплені в ЦК України (ст. 506 ЦК України закріплює майнові права інтелектуальної власності на комерційну таємницю).

До гарантій, що забезпечують охорону комерційної таємниці суб'єкта господарювання, відносяться:

а) гарантії, закріплені в ГК України. Держава гарантує недоторканність майна і забезпечує захист майнових прав підприємця. Вилучення основних і оборотних фондів, іншого майна допускається відповідно до ст.41 Конституції України на підставах і в порядку, передбачених законом. Згідно ч.3 ст.162 ГК України особа, протиправно використовує комерційну таємницю, зобов'язана відшкодувати завдані суб'єкту господарювання збитки;

б) гарантії, закріплені в ЦК України. Згідно ст. 507 ГК України органи державної влади зобов'язані охороняти від недобросовісного комерційного використання інформацію, яка є комерційною таємницею;

в) процесуальні гарантії, закріплені в ГПК.

г) організаційно-правові гарантії, що встановлюються власником комерційної таємниці.

До гарантій, що забезпечує захист права на комерційну таємницю, відносяться:

а) конституційні гарантії, що закріплюють захист інтелектуальної власності, моральних та інтелектуальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності; Конституція гарантує захист державою конкуренції у підприємницькій діяльності, недопущення неправомірного обмеження конкуренції та недобросовісної конкуренції;

б) гарантії, закріплені в ГК України та ЦК України, що передбачають способи захисту, а також умови їх застосування.

До гарантій, що забезпечує можливість притягнення до юридичної відповідальності за порушення права на комерційну таємницю, відносяться:

а) гарантії, закріплені в КК України (ст.231 Кримінального Кодексу України «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю», ст.232 КК України «Розголошення комерційної таємниці»);

б) гарантії, закріплені в Кодексі України про адміністративні правопорушення (ч.3 ст.1643 КпАП України, яка встановлює відповідальність за отримання, використання, розголошення комерційної таємниці з метою заподіяння шкоди діловій репутації або майну іншого підприємця);

в) гарантії, закріплені в ГК України, Законі України «Про захист від недобросовісної конкуренції» (ст.ст.16-19 Закону України «Про захист від недобросовісної конкуренції», ст. 36 ГК України, яка визначає недобросовісною конкуренцією неправомірне збирання, розголошення, схилення до розголошення та неправомірне використання комерційної таємниці, а також ст.ст.20-26 Закону України «Про захист від недобросовісної конкуренції», що передбачають відповідальність за недобросовісну конкуренцію).

Можна констатувати, що за порушення права на комерційну таємницю, передбачені наступні види відповідальності: господарсько-правова (ст.36 ГК України, ст.ст.20-26 Закону України «Про захист від недобросовісної конкуренції»), цивільно-правова (ст. 24 Закону України «Про захист від недобросовісної конкуренції», що передбачає відшкодування збитків), адміністративна (ч.3 ст.1643 КпАП), кримінальна (ст.ст.231, 232 КК). При цьому,

норми КК і КпАП спрямовані на захист добросовісної конкуренції та дублюють ознаки протиправності діянь, закріплені в Законі України «Про захист від недобросовісної конкуренції».

2. Для комерційної таємниці відсутній єдиний міжнародний договір, що надає загальне визначення та встановлює уніфіковані основи правового захисту.

Захист комерційної таємниці здійснюється, переважно, в межах регіональних угод. Основою такого захисту є стаття 10 bis Паризької конвенції про охорону промислової власності 1883 року в редакції 1967 р. (набула чинності для України 25 грудня 1991 р.) щодо недобросовісної конкуренції:

“(1) Країни Союзу зобов’язані забезпечити громадянам країн, що беруть участь у Союзі, ефективний захист від недобросовісної конкуренції.

(2) Актом недобросовісної конкуренції вважається будь-який акт конкуренції, що суперечить чесним звичаям у промислових і торговельних справах”,

а також стаття 10 ter Паризької конвенції:

“(1) Країни Союзу зобов’язуються забезпечити громадянам інших країн Союзу законні засоби для ефективного припинення всіх дій, зазначених у статтях 9, 10, 10 bis.

(2) Крім того, вони зобов’язуються передбачити заходи, що дозволяють союзам та об’єднанням, існування яких не суперечить законам їх країн і які представляють зацікавлених промисловців, виробників чи торговців, діяти через суд чи адміністративні органи з метою припинення дій, передбачених у статтях 9, 10, 10 bis, тією мірою, якою це дозволяє закон країни, де витребовується охорона, для союзів і об'єднань даної країни”.

Хоча загалом зазначені положення Конвенції є недосконалими й недостатніми для створення системи охорони конфіденційної інформації, їх нерідко використовують для первинного обґрунтування іншими міжнародними актами (наприклад, TRIPS).

Іншим важливим для характеристики комерційної таємниці міжнародним актом є Стокгольмська конвенція про заснування Всесвітньої організації інтелектуальної власності 1967 року.

Відповідно до ст. 2, “інтелектуальна власність” включає права, що відносяться, зокрема, до “захисту проти недобросовісної конкуренції”.

Система СОТ. Саме на статтю 10 bis Паризької конвенції посилається Угода з торгових аспектів прав інтелектуальної власності, укладена в межах Світової організації торгівлі (далі – Угода ТРІПС). Ця Угода була схвалена в результаті Уругвайського раунду міжнародних переговорів (1986–1994 рр.) разом з Угодою про формування СОТ та стала першою комплексною багатосторонньою домовленістю, що забезпечує охорону комерційної таємниці.

Стаття 1 Угоди ТРІПС визнає комерційну таємницю (вживає термін “закрита інформація”) інтелектуальною власністю разом з іншими об’єктами. Угода містить Розділ 7 “Охорона закритої інформації” [Protection of Undisclosed Information], який складається зі ст. 39:

“1. У процесі забезпечення ефективного захисту від недобросовісної конкуренції, як це передбачено статтею 10bis Паризької конвенції (1967), країни-учасниці повинні охороняти закриту інформацію відповідно до частини другої цієї статті та дані, надані урядам або урядовим органам відповідно до частини третьої

цієї статті.

2. Фізичні та юридичні особи повинні мати можливість перешкоджати тому, щоб інформація, яка правомірно перебуває під їхнім контролем, була без їхньої згоди розкрита, отримана або використана іншими особами в спосіб, що суперечить чесній комерційній практиці, якщо ця інформація:

(a) є секретною у тому розумінні, що вона в цілому або в конкретному поєднанні та розташуванні її складових не є відомою або легко доступною для осіб, які належать до певного кола, що звичайно має справу з подібною інформацією;

(b) має комерційну цінність з огляду на її секретність; та (c) у конкретних обставинах стала предметом розумних дій для збереження її секретності з боку особи, яка правомірно контролює цю інформацію.

3. Країни-учасниці, у випадках, коли умовою погодження торгового обігу фармацевтичних або сільськогосподарських хімічних продуктів, у яких використовуються нові хімічні речовини, є подання попередньо нерозкритих даних про випробування або інших даних, отримання яких було пов'язано зі значними зусиллями, повинні охороняти такі дані від недобросовісного комерційного використання. Також країни-учасниці повинні охороняти такі дані від розкриття (крім випадків, коли це необхідно для захисту населення або не вживаються заходи для забезпечення охорони цих даних від недобросовісного комерційного використання)".

Під способом, що суперечить чесній комерційній практиці, розуміють, зокрема, такі дії, як порушення договору, порушення довіри та спонукання до такого порушення, що включають отримання закритої інформації третіми особами, які знали або повинні знати, що подібні дії супроводжували це отримання.

Отже, в Угоді ТРІПС закріплено три відомі критерії режиму комерційної таємниці: секретність, комерційна цінність і вжиття адекватних заходів для забезпечення секретності, запозичені з американського законодавства.

Значущість підходу до тлумачення закритої інформації Угодою ТРІПС випливає з того, що ст. 41–47 Угоди на країни-учасниці покладено обов'язок створення національних систем для впровадження визнаних Угодою прав інтелектуальної власності. При цьому країни повинні забезпечити справедливі й рівні процедури для володільців інтелектуальних прав і такі засоби захисту, як судові заборони та компенсація шкоди.

Важливим також є поширення на відносини щодо охорони закритої інформації або комерційної таємниці міжнародної системи СОТ вирішення спорів.

Таким чином, ст. 39 Угоди ТРІПС встановила мінімальні правила, яким має відповідати законодавство країн членів СОТ. Формулювання статті залишають місце для визначення конкретних схем, що відповідатимуть правовим системам країн, але обов'язковим є включення згаданих трьох необхідних елементів та системи законного примусу для реалізації відповідних положень. Треба зазначити, що визначення комерційної таємниці, яке міститься в ст. 505 Цивільного кодексу України, є дуже близьким до ст. 39 Угоди ТРІПС.

NAFTA (Північноамериканська угода про вільну торгівлю). Стаття 1711 Північноамериканської угоди про вільну торгівлю (укладена в 1994 р. Канадою, США та Мексикою) фактично відтворює положення ст. 39 Угоди ТРІПС з окремими відмінностями. По-перше, вживається термін "комерційна таємниця" (trade secrets), що відповідає традиції США. По-друге, однією з ознак комерційної таємниці визнано дійсну або потенційну комерційну цінність (Угода ТРІПС не

містить такого поділу). По-третє, країнам-учасницям Угоди дозволяється вимагати матеріальні докази для доведення вживання заходів з охорони комерційної таємниці. По-четверте, забороняється обмежувати тривалість дії режиму комерційної таємниці.

Європейський Союз. Правова система ЄС (acquis communautaire) не містить окремого акту для охорони комерційної таємниці. Це пов'язано, зокрема, зі заставленням, що відрізняється від американської ідеології, до охорони об'єктів інтелектуальної власності, що виходить з пріоритетності вільної конкуренції та вільного руху товарів (робіт, послуг). Ще Римським Договором 1957 року встановлено, що будь-яка заборона або обмеження вільного обігу товарів унаслідок використання права на промислову власність може мати місце, лише якщо це право не є засобом свавільної дискримінації або прихованого обмеження торгівлі товарами між країнами-членами. Таким чином, особливості правового режиму охорони комерційної таємниці, як і інших об'єктів інтелектуальної власності, зумовлені, насамперед, політикою забезпечення вільної конкуренції. Це, зокрема, означає сумнівність можливості визнання необмеженої в часі охорони комерційної таємниці, оскільки це може тлумачитись як право промислової власності, що порушує вільний обіг товарів.

Правова система ЄС надає охорону інформації, що становить комерційну таємницю, у вигляді охорони "ноу-хау", яка міститься в Європейській патентній конвенції. Під "ноу-хау" розуміють цілісну технічну інформацію, що є секретною, зафіксованою в матеріальному об'єкті та може бути встановленою у будь-який можливий спосіб. "Секретний" означає "такий, що не є загальновідомим або легкодоступним".

Охорона комерційної таємниці не є справою виключно національного законодавства. Міжнародна торгівля та інвестиції створили передумови для розвитку правових інструментів комерційної конфіденційної інформації. Основною рушійною силою цих змін стали глобальні інвестиції розвинутих країн, які не мають бажання інвестувати закордон та розкривати своє "секретне знання", якщо відсутній певний рівень охорони комерційної таємниці, визнаний учасниками міжнародної торгівлі. Саме торгові та інвестиційні угоди стали імпульсом розвитку нових систем заходів охорони комерційної таємниці в законодавстві країн світу.

У розвинутих країнах Європи охорона конфіденційної комерційної інформації має свою довгу історію, хоча підходи різняться залежно від країни. Найрозвинутішу систему охорона має Об'єднане королівство, що пов'язано з промисловою революцією та традицією прецедентного права. Саме з англійської системи бере початок відповідне законодавство США. У Великобританії відсутній законодавчий захист комерційної таємниці, відповідно, не існує легального визначення цієї таємниці. Натомість, правове регулювання цих відносин розвивалось упродовж останніх століть на основі судових прецедентів і отримало назву конфіденційного права (law of confidence). Отже, охорона комерційної таємниці ґрунтується на концепції "порушення довіри" сформульовано так: "Право, що застосовується до таких дій, не залежить від якоїсь угоди. Воно залежить від широкого принципу справедливості, що полягає в тому, що той, хто отримав інформацію конфіденційно, не повинен недобросовісно здобувати з неї вигоду. Він не повинен використовувати її на шкоду тому, хто передав йому цю інформацію, якщо останній не дав своєї згоди". Отже, керівним принципом є довіра між законним власником таємниці й отримувачем конфіденційної

інформації.

Охорону комерційній інформації надано й законодавством Німеччини та Франції. Так, Розділом І Закону ФРН про недобросовісну конкуренцію встановлено відповідальність за завдання шкоди особою, яка при здійсненні підприємницької діяльності в цілях конкуренції вчиняє дії, несумісні з "чесною практикою". Хоча далі Закон і не визначає ці дії, Розділом 17 передбачено відповідальність за несанкціоноване використання або повідомлення третій особі комерційної таємниці. Під останньою розуміють інформацію, що має ознаку секретності (доступна лише відомому обмеженому колу осіб) та відповідає умові наявності у власника цієї інформації обґрунтованого інтересу в її збереженні. Передбачено кримінальну відповідальність за злочини, пов'язані з порушенням режиму комерційної таємниці. У трудовому законодавстві міститься обов'язок працівника не розголошувати комерційну таємницю після припинення трудових відносин.

Законодавство Франції містить поняття промислових або виробничих секретів (secret de fabrique) та комерційної таємниці (secret de commerce). Перша категорія походить від французького кримінального кодексу та включає конфіденційну інформацію, що має виробниче застосування та може становити комерційну цінність. Комерційна таємниця прямо не визначається законодавством, але відображає ширше, порівняно з виробничими секретами, поняття й може належати до організаційної структури підприємства, списку постачальників, особистих справ персоналу, контрактів з іншими організаціями, списків клієнтів, планів розвитку бізнесу, схеми дистрибуції тощо. Виробничі й комерційні секрети не вважаються власністю у Франції і отримують захист як делікти з недобросовісної конкуренції та договірних зобов'язань.

У США комерційна таємниця спочатку була сферою, що традиційно регулювалась загальним правом окремих штатів. Першою спробою "кодифікації" виробленого судами права комерційної таємниці був Перший Звід права деліктів 1939 р. Сучасніший підхід закріплено Третім Зводом права деліктів 1993 р. Охорона комерційної таємниці відбувається в межах делікту незаконного заволодіння комерційною таємницею, який, у свою чергу, є складовою делікту недобросовісної конкуренції. На сьогодні в більшості юрисдикцій США комерційна таємниця охороняється законами. 42 штати та Округ Колумбія прийняли ту чи іншу версію Уніфікованого Закону про комерційну таємницю (Uniform Trade Secrets Act) 1979 р. У Каліфорнії положення Закону включені в Цивільний кодекс. Законодавчі положення доповнюються договірним захистом, який виступає додатковим. Існує також значна кількість кримінальних законів щодо незаконного заволодіння комерційною таємницею, основним з яких є федеральний Закон про Економічний шпіонаж 1996 року.

Виділяють такі чотири основні елементи режиму комерційної таємниці в США. По-перше, це повинна бути "обмежена інформація", тобто інформація, яку можна відрізнити від загальновідомих знань і навичок. По-друге, елемент "секретності" – інформація не є добре відомою або такою, яку можна легко отримати. По-третє, інформація повинна мати економічну цінність, що полягає в наданні певної конкурентної переваги. І, по-четверте, власник повинен вжити розумних зусиль для того, щоб зберегти інформацію в таємниці.

Законодавство Канади про комерційну таємницю також, ґрунтується на прецедентному праві, центральним принципом якого, як і в Англії, є порушення довіри. Підставами для позову в результаті делікту є: 1) секретність інформацій; 2)

те, що її було надано конфіденційно; 3) те, що особою, якій її було надано, використано зі зловживанням. Наприклад, у справі Three Savers Int'l LTD v. Savoy колишні працівники позивача визнані відповідальними за використання списку клієнтів їхнього працедавця для ведення бізнесу конкурента, що складено працівниками після того, як вони залишили свою попередню роботу.

Відповідно до Цивільного кодексу Російської Федерації, інформація становить службову або комерційну таємницю у випадку, коли інформація має дійсну або потенційну комерційну цінність у силу її невідомості третім особам, до неї немає вільного доступу на законній підставі й власник інформації вживає заходів для охорони її конфіденційності. Відомості, які не можуть становити службову або комерційну таємницю, визначаються законом та іншими правовими актами. Особи, які незаконними методами отримали інформацію, яка становить службову або комерційну таємницю, зобов'язані відшкодувати завдані збитки. Такий самий обов'язок покладається на працівників, які розголосили таємницю всупереч трудовому договору, у тому числі контракту, і на контрагентів, які зробили це всупереч цивільному правовому договору.

У Росії вже тривалий час здійснюються спроби прийняття спеціального акту – Закону "Про комерційну таємницю".

3. Для визначення комерційної таємниці на підприємстві можна запропонувати чотири способи:

1. Тотальний. Сутність цього методу дуже простий. Виключити з переліку відомостей все, що не може бути комерційною таємницею. По-перше, відомостями, які становлять комерційну таємницю, не можуть бути відомості, що становлять державну таємницю, По-друге, Кабінет Міністрів України затвердив перелік відомостей, що не становлять комерційну таємницю. Ці відомості використовуються при здійсненні перевірок контролюючими органами, аудиторами для проведення аудита, при здачі звітності в різні фонди. Все інше, що залишилося, слід визнати комерційною таємницею підприємства. Таким чином, таємницею буде вся інформація підприємства. Цей спосіб найбільш простий і найменш ефективний. Дійсно, дуже легко оголосити всю інформацію, що підлягає захисту, секретом. От тільки як захищати? У свідомості людини, зазвичай, все — означає ніщо. Це занадто абстрактне поняття, що вимагає конкретного пояснення. Отже, або доведеться створювати відмінну працюючу систему, що займеться захистом «всього», або — змиритися з тим, що таємниця залишиться лише закріпленою на папері.

2. Плагіаторський. Треба з'ясувати, яку саме інформацію ваші партнери вважають комерційною таємницею, і зробити так само на своєму підприємстві. Природно, що повного списку вам ніхто не надасть, але підказати, які саме сфери діяльності підлягають засекречуванню і дати невелику пораду, напевно, зможуть. У крайньому випадку досить просто ознайомитися зі спеціальними матеріалами і літературою, що досліджує ці теми. Як допоміжна інформація там надається зразковий перелік інформації, що може бути віднесена до комерційної таємниці. Проте все, чого ви дізнаєтеся таким чином, буде лише сировиною, з якої вам доведеться створити необхідний продукт. У комерційній таємниці дуже небагато універсальних положень, що підходять абсолютно для всіх. Кожна ситуація вимагає індивідуального підходу, який би враховував усі нюанси та особливості.

Те, що на одному підприємстві вважається таємницею, може бути зовсім відкритим на інших і навпаки.

3. Аналітичний. Цей спосіб складніший за наведені вище, однак більш ефективний. Він полягає у використанні «рольових ігор» і давно застосовується психологами, слідчими, маркетологами та багатьма іншими. Необхідно уявити себе на місці іншої людини. Наприклад, подумайте, яка саме інформація про ваших конкурентів була б вам особливо корисна. Тепер уявіть себе на місці ваших конкурентів і розгляньте ситуацію щодо вашого підприємства. Також досить корисним буде уявити себе на місці зловмисника (злодія, шантажиста або іншого недоброзичливця), адже загроза може виходити і від них також. Якщо ваша уява працює погано, залучіть родичів, друзів. Зверніться до власного персоналу з таким завданням, і вони не тільки вам допоможуть, але й, можливо, ви знайдете в деяких своїх працівниках відмінні аналітичні якості, що раніше не використовувалися. Отримані в такий спосіб результати після необхідної обробки і варто визнати комерційною таємницею. Природно, що такого роду «сеанси перевтілення» варто проводити регулярно, адже підприємство розвивається, з'являється щось нове. Результат такої роботи, якщо вона проведена з усією серйозністю, може бути дуже ефективним.

4. Експертний. Якщо в попередніх способах описувалися ситуації, коли бізнесмен намагається самостійно вирішити свої проблеми, то в цьому випадку потрібно звернутися по допомогу до фахівців. Природно, професіонал, що займається захистом комерційної таємниці, здатний зробити це набагато краще за будь-яку непідготовлену особу. Люди, чиєю професією є захист і безпека, мають відмінну підготовку, підкріплену практичним досвідом. І їм не складе особливих труднощів виконати свою роботу.

Найкращим рішенням є створення власної служби безпеки, що складається хоча б з кількох працівників, які займаються безпосередньо питаннями захисту. Мати службу безпеки може не кожне підприємство. Тоді до вирішення питання залучають фахівця-консультанта. Доцільно не просто одноразово залучати такого спеціаліста для надання послуг, а регулярно звертатися до нього по допомогу.

Для безпосереднього визначення переліку відомостей, що становлять комерційну таємницю, на підприємстві можна створити спеціальну комісію, яка займатиметься групуванням і уточненням інформації з цього переліку. Чисельність членів такої комісії - не більше 4-5 осіб. Створюють її з найбільш кваліфікованих і компетентних фахівців основних підрозділів та представників служби безпеки підприємства, ознайомлених як із діяльністю підприємства в цілому, так і з роботою окремих підрозділів.

4. Не може бути комерційною таємницею:

По-перше, відомостями, які складають комерційну таємницю, не можуть бути відомості, що складають державну таємницю, тобто такого виду секретної інформації, котрий включає відомості в сфері оборони, економіки зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може заподіяти шкоду життєво важливим інтересам України і які визнані законом державною таємницею і підлягають охороні з боку держави.

По-друге, Кабінет Міністрів України затвердив перелік відомостей, що не складають комерційну таємницю. Ці відомості використовуються при здійсненні

перевірок контролюючими органами, аудиторами для проведення аудита, при здачі звітності в різні фонди. До них належать:

1. статутні документи, документи, що дозволяють займатися підприємницькою або господарською діяльністю і її окремими видами;
2. інформація з усіх установлених форм державної звітності;
3. дані, необхідні для перевірки вирахування і сплати податків і інших обов'язкових платежів;
4. відомості про чисельність і склад працівників, їхню заробітну плату за професіями і посадами, а так само наявність вільних місць;
5. документи про сплату податків і обов'язкових платежів;
6. інформація про забруднення навколишнього природного середовища, недотриманні безпечних умов праці, реалізацію продукції, що заподіює шкоду здоров'ю, а так само інших порушень законодавства України і розмірах заподіяних при цьому збитків;
7. документи про платоспроможність;
8. відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, союзах, об'єднаннях та інших організаціях, що займаються підприємницькою діяльністю;
9. відомості, що згідно із чинним законодавством підлягають розголошенню.

5. Для того, щоб інформація зберігалася у режимі «комерційна таємниця», суб'єкт підприємницької діяльності повинен спланувати й організувати дії правового характеру. Перш за все, це внесення відповідних положень до установчих документів.

В установчих документах з посиланням на статті 505, 506 ЦК України та статті 36, 135, 155, 162 ГК України передбачити право підприємства відносити інформацію, що йому належить, до комерційної таємниці та право приймати внутрішні документи, якими визначається її склад, обсяг та порядок захисту інформації, що є конфіденційною або комерційною таємницею.

На базі вищезазначених документів підприємство планує та організовує розробку, прийняття й упровадження основних документів підприємства. Це документи, які безпосередньо забезпечують захист комерційної таємниці підприємства, та документи, які забезпечують захист комерційної таємниці підприємства при прийомі персоналу.

До документів, які безпосередньо забезпечують захист комерційної таємниці підприємства належать:

1. *Положення про організацію роботи з комерційною таємницею* підприємства та іншою конфіденційною інформацією (Положення про комерційну таємницю). У положенні врегульовують заходи з організації охорони та захисту комерційної таємниці, порядок роботи з інформацією, що є комерційною таємницею, зобов'язання працівників щодо збереження комерційної таємниці, порядок розкриття інформації, що містить комерційну таємницю. відповідальність за порушення пов'язані з комерційною таємницею та ін.;

2. Перелік відомостей які відносяться до інформації з обмеженим доступом.

3. Положення щодо спеціального діловодства для документів, які містять інформацію з обмеженим доступом;

4. Положення про інформаційну безпеку при роботі з матеріальними носіями, що містять комерційну таємницю;

5. Інструкція про порядок виконання запитів, що надходять від правоохоронних органів, судів та інших державних установ;

6. Інструкція про проведення перевірок щодо дотримання норм інформаційної безпеки при роботі з матеріальними носіями, що містять комерційну таємницю.

Документи, які забезпечують захист комерційної таємниці підприємства при прийомі персоналу складають:

1. Трудовий договір (контракт), посадові інструкції, де прописуються питання, що стосуються роботи з комерційною таємницею та відповідальності за порушення права на використання комерційної таємниці у тому числі після звільнення працівника з посади;

2. Зобов'язання працівників підприємства щодо збереження інформації з обмеженим доступом;

3. Положення про нерозголошення комерційної таємниці підприємства та інші положення, правила, зобов'язання, підпис працівника на яких є підставою для захисту підприємством своїх інтересів.

4. Опис вимог щодо угод з третіми сторонами стосовно доступу, оброблення, передавання або управління інформацією підприємства.

Процедура віднесення інформації до комерційної таємниці – це складне багатоаспектне явище, що передбачає застосування заходів правового та організаційного характеру щодо охорони та захисту комерційної таємниці суб'єкта господарювання.

Процедура віднесення інформації до комерційної таємниці передбачає декілька чітко визначених етапів.

На *першому етапі* відбувається актуалізація певної інформації, яка потребує захисту у статусі комерційна таємниця. Далі необхідно ретельне вивчення обраної інформації, як секретної, і складання робочого варіанту Положення про комерційну таємницю та Переліку відомостей, що становлять комерційну таємницю підприємства. Відповідний перелік конфіденційної інформації може бути сформований за такими напрямками: кадрова політика підприємства, фінансова діяльність підприємства, цінова політика підприємства, збутова діяльність підприємства, забезпечення безпеки підприємства.

Для виконання такого завдання керівник підприємства призначає відповідальну особу за режим секретності щодо конфіденційної інформації та комерційної таємниці та комісію з питань комерційної таємниці. Формувати перелік відомостей, що становлять комерційну таємницю підприємства потрібно із залученням фахівців профільних підрозділів за кожним із напрямків. Тоді існуватиме можливість у разі виникнення спірних питань щодо належності тієї чи іншої інформації до категорії «комерційна таємниця» залучати в якості експертів фахівців таких підрозділів. Саме такі особи, навіть за наявності в інформації основних ознак комерційної таємниці, можуть визначати у кожному конкретному випадку, наскільки небезпечним є її розголошення.

У вітчизняному законодавстві відсутні вимоги та регламентації, що стосуються структури та змісту Положення про комерційну таємницю. Але, незважаючи на відмінності в сферах діяльності, структурах, кількості працівників і керівного складу підприємств, дослідники формулюють деякі загальні

рекомендації щодо його змісту:

1. Загальні положення.
2. Визначення переліку відомостей, що становлять комерційну таємницю та конфіденційну інформацію підприємства.
3. Порядок захисту комерційної таємниці та конфіденційної інформації підприємства.
4. Порядок видачі працівниками документів, відомостей, передання інформації, що становить комерційну таємницю та конфіденційну інформацію підприємства контрагентам, клієнтам і державним органам.
5. Процедура наймання (звільнення) працівника/співробітника підприємства.
6. Відповідальність за розголошення відомостей, що становлять комерційну таємницю та конфіденційну інформацію підприємства.
7. Прикінцеві положення.
8. Додатки.

У розділі 2 цього положення перелік відомостей доцільно охарактеризувати загальними поняттями, а для їх докладного визначення посилатися на Перелік відомостей, що становлять комерційну таємницю підприємства.

У Додатках можуть бути наведені типові документи, що стосуються питань комерційної таємниці, наприклад: «Службова записка з пропозицією віднесення інформації до комерційної таємниці», «Зобов'язання працівника щодо нерозголошення комерційної таємниці та конфіденційної інформації», «Угоди про конфіденційність з відвідувачами підприємства» тощо.

Другий етап – керівник підприємства видає наказ про затвердження та впровадження на підприємстві Положення про комерційну таємницю підприємства та порядку ознайомлення з ним.

Наступний етап – комісія формує Перелік відомостей, що становлять комерційну таємницю підприємства. На цьому етапі передбачено встановлення терміну засекречування інформації. За періодом існування комерційну таємницю можна поділити на короткострокову таємну інформацію та довгострокову таємну інформацію. Як правило, часовий відлік засекречення короткострокової інформації – до 6 місяців, довгострокової – від 6 місяців і довше.

Четвертий етап передбачає затвердження Переліку відомостей, що становлять комерційну таємницю підприємства і складається з двох стадій:

1) присвоєння за кожним видом інформації відповідного грифу секретності. «Особливо секретно» – відомості, оволодіння якими негативно відбиваються на усієї діяльності підприємства, та «секретно» – відомості, оволодіння якими може спричинити шкоду за окремим напрямком діяльності підприємства.

2) затвердження та підписання керівником підприємства Переліку відомостей, що становлять комерційну таємницю. Усім відомостям, що перелічені у вказаному документі, офіційно наданий статус комерційної таємниці підприємства.

Перелік відомостей, що становлять комерційну таємницю, має періодично корегуватися. Відомості, які втратили своє значення, стали загальнодоступними чи втратили комерційну цінність тощо, мають вилучатися, а вноситись нові, що потребують захисту.

6. Після дій правового характеру керівник організовує дії організаційного

характеру.

Перший етап – це встановлення матеріальних носіїв інформації, що становлять комерційну таємницю підприємства. Носіями конфіденційної інформації можуть виступати людина, документи, продукція, офіційні засоби інформації, технічні засоби. При цьому людина є сполучною ланкою між усіма іншими носіями комерційної таємниці, оскільки розробляє і затверджує документацію; є виробником продукції; готує матеріали для видання, оголошення та показу в засобах масової інформації; працює за комп'ютерами, друкарською машинкою, з телефонними апаратами, факсами та іншими технічними засобами. За кожним видом конфіденційної інформації вирішується, в якій якості вона буде існувати. Комерційна таємниця може мати декілька носіїв, що треба враховувати при визначені способів її захисту, а також тих осіб, які нею володіють.

На наступному етапі визначаються конкретні особи, що володіють конфіденційною інформацією, або можуть мати доступ до неї.

Розголошення комерційної таємниці здебільшого пов'язано з тим, що керівник підприємства недостатню увагу приділяє вивченню особистості особи допущеної до роботи з комерційною таємницею.

Надаючи право доступу до інформації з грифом «комерційна таємниця» керівник повинен:

– визначити потребу співробітника в конфіденційній інформації при виконанні ним службових обов'язків;

– здійснити перевірку співробітника у зв'язку з допуском до комерційної таємниці;

– ознайомити співробітника з мірою відповідальності за порушення законодавства про незаконне збирання, поширення та використання комерційної таємниці;

– оформити письмове зобов'язання працівника про нерозголошення комерційної таємниці, що буде йому довірена.

При перевірці співробітника на допуск необхідно брати до уваги таке:

– досягнення ним дієздатного віку 18 років;

– наявність судимості за злочини, пов'язані з розголошенням державної чи комерційної таємниці, а також у фінансово-господарській сфері;

– наявність психічних захворювань, схильність до вживання алкоголю та наркотиків;

– факти надання в процесі підготовки матеріалів для оформлення допуску недостовірних відомостей про себе;

– наявність підозрілих зв'язків із співробітниками підприємств-конкурентів.

Третій етап – вибір способів захисту комерційної таємниці на підприємстві.

Щоб розробити дійову систему захисту комерційної таємниці, необхідно вивчити всі можливі шляхи незаконного оволодіння нею.

Найбільш частими протиправними діями, що дозволяють оволодіти конфіденційною інформацією підприємства є:

– підкуп співробітників підприємства, що володіють або мають доступ до конфіденційної інформації;

– підслуховування телефонних переговорів;

– дистанційне звукове прослуховування;

– копіювання носіїв інформації;

– розшифровка радіовипромінювання комп'ютерів, факсів, телетайпів;

– візуальний та слуховий контроль приміщення;

– розміщення мікропередавачів в приміщеннях і автомобілях;

– використання шпигунів-професіоналів;

– переманювання працівників конкурента

– засилання агентів до службовців або фахівців конкурента.

Незаконним оволодінням комерційною таємницею сприяють низький рівень контролю за досягненням заходів безпеки, незадовільні умови праці, неефективна система заохочування працівників, економія на технічних засобах захисту, плинність кадрів, недосконала система праці, тощо.

Дієвими способами захисту є:

1. Створення режимно-секретного підрозділу з функціями підтримки і контролю за дотриманням встановленого режиму секретності, діяльність якого визначається відповідними інструкціями, положеннями чи наказами.

Як основні функції режимно-секретного підрозділу доцільно визначити такі :

– розробка, впровадження та забезпечення функціонування дозвільної системи доступу до інформації;

– розробка й упровадження маркування документації та носіїв інформації, віднесеної до комерційної таємниці та дій щодо їх збереження;

– розробка та впровадження секретного діловодства;

– планування й організація дій технічного характеру щодо охорони носіїв інформації та інформаційних мереж;

– дії, що спрямовані на виявлення витоку інформації, джерел такого витоку та локалізації негативних наслідків тощо;

– планування, організація та здійснення дій психологічного характеру: інструктаж персоналу, роз'яснювальна робота, перевірки та ін.;

– контроль, аналіз і надання рекомендацій з поліпшення.

У разі доцільності на режимно-секретний підрозділ можуть бути покладені функції забезпечення захисту майна та персоналу підприємства.

2. На підприємстві потрібно забезпечити жорсткий режим доступу до інформації конфіденційного характеру. Це передбачає:

– пропускний режим до приміщень, де зберігаються відомості, що становлять комерційну таємницю;

– ретельний підбір кадрів, що працюють з конфіденційною інформацією. Відомо, що чим менше людей мають доступ до таких відомостей, тим більше ймовірність зберегти їх в таємниці. Отже, необхідне обмежене коло осіб, що можуть мати доступ до тієї чи іншої секретної інформації.

У разі звільнення співробітника, який був допущений до комерційної таємниці, ним підписується попередження-зобов'язання про нерозголошення відомостей, які стали йому доступні в процесі роботи на підприємстві. Мета відбору такого попередження-зобов'язання про нерозголошення – профілактика розголошення співробітником, що звільняється, комерційної таємниці і створення юридичних підстав для відшкодування збитків у разі розголошення таких відомостей.

3. Введення відповідного маркування носіїв з конфіденційною інформацією.

Відомості, що становлять комерційну таємницю, можуть бути диференційовані підприємством за ступенем важливості з присвоєнням відповідного грифу.

Наприклад:

1. Для конфіденційної інформації – гриф «Для службового користування» або «ДСК»;

2. Для різних режимів секретності, за необхідності, комерційної таємниці: гриф «Для службового користування. Комерційна таємниця –секретно» або «ДСК: КТ-С»; гриф «Для службового користування. Комерційна таємниця – суворо секретно» або «ДСК: КТ-ССО»; гриф «Для службового користування. Комерційна таємниця – особливо секретно» (або «ДСК: КТ-ОС») тощо.

Вищезазначене маркування наноситься на носії з інформацією, а в разі зберігання інформації в електронному вигляді, гриф має передувати відкриттю безпосередньо інформації.

4. Забезпечення збереженості документів, що містять комерційну таємницю.

Документи, що містять комерційну таємницю, потребують особливого режиму зберігання. Їх треба зберігати у службових приміщеннях у шафах (сейфах), сховищах, що надійно замикаються й опечатуються.

Документи, видані для роботи працівникам-виконавцям, повертають до служби діловодства (секретарю) або в архів того самого дня. У деяких випадках з дозволу керівника служби діловодства чи особи, відповідальної за архів підприємства, документи можуть зберігатися у працівника протягом терміну, потрібного йому для виконання завдання, за умови цілковитого забезпечення їх збереженості. При цьому документи не дозволяється залишати на столі, закінчивши роботу, їх треба покласти до шафи, що замикається, або сейфа.

Документи, що містять комерційну таємницю, не дозволяється виносити за межі підприємства. Лише за умови потреби їх погодження з фахівцями з інших підприємств, що територіально розташовані в одному населеному пункті, керівник підприємства може видати працівникам письмовий дозвіл на винесення цих документів за межі підприємства.

Працівникам, відрядженим з виробничою метою до інших населених пунктів, забороняється мати при собі документи, що містять комерційну таємницю підприємства. Такі документи заздалегідь пересилають за призначенням.

Наявність документів, що містять комерційну таємницю, щорічно переглядає комісія, спеціально призначена наказом керівника підприємства. До складу комісії входять особи, яким доручено облік і зберігання цих документів, а також працівники режимно-секретного підрозділу підприємства.

В архівах і бібліотеках, де зберігається значна кількість документів із грифом обмеженого доступу, перевірка їх наявності може проводитися *один раз на п'ять років*.

Результати перевірок завжди оформляють протоколом. Виявивши у ході перевірки втрату документів з грифом *«КТ»* або розголошення відомостей, що містять комерційну таємницю, про це терміново доповідають керівництву підприємства, керівникам режимно-секретного відділу і служби діловодства, а також службі безпеки підприємства, якщо така на підприємстві є.

Для розслідування факту втрати документів або розголошення інформації, що міститься в них, наказом керівника підприємства призначається комісія, висновок якої, незалежно від результатів, затверджує керівник підприємства.

5. Застосування технічних засобів захисту комерційної таємниці. Технічні заходи захисту базуються на використанні різних електронних пристроїв і спеціальних програм, що входять до складу системи обробки інформації та

виконують функції захисту. Наприклад, пошукові прилади, прилади охорони провідних комунікацій, програмне забезпечення, апаратура для виявлення диктофонів, системи акустичного і віброакустичного зашумлення, скануючі засоби, засоби виявлення каналів витоку інформації, встановлення спеціального обладнання для спостереження за приміщеннями організації тощо.

6. *Підвищення лояльності працівників* включають правильно організовану роботу з працівниками підприємства (кадрову політику) і застосування матеріальних та моральних стимулів. Одним із важливих завдань керівника потрібно вважати вірно організований добір співробітників, створення сприятливого соціально-психологічного клімату всередині організації, формування «професійного патріотизму». Завдяки вирішення питань соціального захисту працівників, організації відпочинку та дозвілля, медичного обслуговування керівник створює в колективі таке сприятливе середовище, що зводить до мінімуму ймовірність усвідомленого заподіяння шкоди підприємству його ж працівниками. Не варто нехтувати і впровадженням системи матеріальних винагород, створенням можливостей для професійного зростання та для участі персоналу в прийнятті рішень. Від умов роботи, що створює керівництво для своїх підлеглих, залежить стан психологічної атмосфери в колективі, тому отримуючи максимальне задоволення від своєї роботи, працівник здатен виконувати свої обов’язки найбільш плідно. Розвиток у них зацікавленості в успіхах підприємства має бути спрямований на те, щоб звести до мінімуму плинність кадрів і разом з тим – втрату інтелектуального потенціалу підприємства і можливість розголошення конфіденційної інформації.

Тема 5. Доступ до інформації та забезпечення безпеки їх використання.

Поняття «допуск» та «доступ» до інформації з обмеженим доступом. Форми допуску до державної таємниці. Організація допуску до відомостей, що становлять державну таємницю. Порядок отримання спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею. Допуск до інформації, що містить комерційну таємницю. Юридичні зобов’язання співробітників підприємства, які отримали допуск до комерційної таємниці. Дозвільна система доступу до комерційної таємниці. Обов’язкові умови, пов’язані із забезпеченням безпеки використання, збереження та захисту державної та комерційної таємниці. Технічний захист інформації, що містить державну та комерційну таємницю.

1. Доступ фактично є певною дозвільною процедурою, яка полягає в отриманні згоди компетентного органу (особи) на одержання документа або інформації, отримання якої безпосередньо пов'язане з реалізацією права на інформацію, і, відповідно, обмежує це право.

Відповідно до ЗУ«Про інформацію», вчинення права на отримання інформації пов'язане з поняттям доступу до інформації. Доступ до інформації − це передбачений правовими нормами порядок отримання, використання, поширення та зберігання інформації. По суті, порядок доступу до інформації є різновидом спеціальних правових режимів, які встановлюють сукупність правил, закріплених в юридичних нормах, що регулюють певну діяльність людей.

Головними характеристиками порядку доступу до інформації є: суб'єкт визначення доступності цієї інформації; коло суб'єктів, які мають доступ до цієї інформації; особливі вимоги і правила збереження та поширення цієї інформації; термін дії порядку.

Суб'єктом визначення доступності інформації є особа, в компетенцію якої входить вирішення питань щодо встановлення обмежень на доступ до інформації та її матеріальних носіїв, а також надання права доступу до такої інформації.

Суб'єкт, який має доступ до інформації − це особа, якій надано право ознайомлення з матеріальними носіями інформації або їх використання.

Надання особі права доступу до інформації, зазвичай пов'язане з взяттям нею на себе зобов'язань з нерозголошення отриманої інформації.

Порядок доступу до інформації означає певну сукупність правил, якими позначені особливі вимоги і правила зберігання та поширення інформації.

Ці правила визначають діяльність осіб, на яких покладено відповідальність за зберігання матеріальних носіїв інформації, встановлюють необхідність застосування певних правових, організаційних, технічних та криптографічних засобів захисту інформації.

Ці правила також визначають порядок надання доступу до такої інформації

Допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації. Доступ до державної таємниці – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

2. Спеціальний порядок допуску та доступу громадян до державної таємниці є складовою частиною комплексу заходів спрямованих на запобігання витоку секретної інформації. Існування такого порядку обумовлюється необхідністю вивчення та обмеження кола осіб, діяльність яких буде пов'язана з державною таємницею. Порядок надання, переоформлення та скасування громадянам допуску до державної таємниці передбачений Законом України "Про державну таємницю" і встановлюється Кабінетом Міністрів України.

Згідно ст. 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 його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання, наказом чи письмовим розпорядженням керівника установи, де працює громадянин."

Необхідність роботи із секретною інформацією та форма допуску визначаються керівником установи згідно з номенклатурою посад працівників управління, які підлягають оформленню на допуск до державної таємниці. Номенклатура посад складається, виходячи із штатного розпису установ, підприємств, організацій посадових інструкцій та характеру роботи з урахуванням положень Зводу відомостей, що становлять державну таємницю та розгорнутого переліку цих відомостей, до неї включаються лише посади, умови діяльності яких потребують доступу до державної таємниці.

Залежно від ступеня секретності інформації встановлюються такі форми допуску до державної таємниці:

– форма 1 – для роботи з секретною інформацією із ступенем секретності „особливої важливості”, „цілком таємно” і „таємно” терміном дії – 5 років;

– форма 2 - для роботи з секретною інформацією із ступенем секретності „цілком таємно” і „таємно” терміном дії – 10 років;

– форма 3 - для роботи з секретною інформацією із ступенем секретності „таємно” терміном дії – 15 років.

3. 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 керівники органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, в яких виконуються роботи, пов'язані з державною таємницею, або зберігаються матеріальні носії секретної інформації Відмова надати громадянинові України доступ до конкретної секретної інформації та її матеріальних носіїв можлива лише у разі відсутності підстав, передбачених вище.

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 ними письмового зобов'язання щодо збереження державної таємниці.

Іноземцям та особам без громадянства доступ до державної таємниці надається у виняткових випадках на підставі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, або письмового розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України.

В окремих випадках, які визначаються міністерствами, іншими центральними органами виконавчої влади, за погодженням з СБУ громадянам віком від 16 років може надаватись допуск до державної таємниці із степенем секретності"цілком таємно", "таємно", а 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 після надходження до органу державної влади,органу місцевого самоврядування, підприємства,,установи організації висновків по матеріалах його перевірки у зв'язку з допуском до державної таємниці

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 також 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.

Призначення громадян установи, організації, підприємства на посади, включені до номенклатури посад, здійснюється лише після надання їм у встановленому порядку допуску до державної таємниці.

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, проводиться співбесіду з метою попереднього з’ясування відсутності чи наявності обставин, за яких громадянину установи, організації, підприємства може бути відмовлено у наданні допуску до державної таємниці.

– подає дві фотокартки розміром 4,5 х 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 громадянам установи, організації, підприємства , згідно до спільного наказу Міністерства охорони здоров'я та Служби безпеки України від 13 травня 2002 року № 174/136 " Перелік психічних захворювань / розладів /, які можуть завдати шкоди охороні державної таємниці і за наявності яких допуск до державної таємниці громадянину не надається" . Цим же наказом передбачено, що порядок надання зазначеної інформації визначається чинним законодавством.. У разі наявності у працівникам установи психічних

захворювань документи щодо надання йому допуску до державної таємниці до органу СБУ не подаються.

Надалі готуються та відправляються в підрозділ Управління СБ України наступні документи:

1. 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.

2. Заповнену і завірену у встановленому порядку анкету з фотокарткою громадянина, щодо якого розглядається питання про надання допуску до державної таємниці, розміром 4,5 х 6 сантиметрів. Слід пам’ятати, що відповіді на запитання повинні бути повними, перекреслювання не допускаються.

3. Один примірник облікової картки з фотокарткою громадянина, щодо якого розглядається питання про надання допуску до державної таємниці, розміром 4,5 х 6 сантиметрів, засвідченої, працівником РСО та скріпленої його печаткою . Анкетні дані заповнюються на друкарської машинці РСО, інші відомості – на друкарської машинці РСО або розбірливим почерком чорними чи фіолетовими чорнилами.

Обліковій картці, з дати її заповнення, надається гриф обмеження доступу „Для службового користування ”, і вона підлягає реєстрації в журналі обліку таких карток.

4. 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.

5. 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). Якщо працівник установи, щодо якого розглядається питання про надання допуску до державної таємниці, або хто-небудь з його близьких родичів змінював прізвище, то на кожне прізвище заповнюється додаткова картка. Картки заповнюються на друкарській машинці працівником РСО установи, що подає органу Служби безпеки України і документи для оформлення працівника управління допуску до державної таємниці. Підписами посадових осіб картка не засвідчується.

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

За результатами перевірки громадянина орган СБУ, який проводив перевірку, виносить мотивований висновок (далі - висновок) щодо надання йому допуску до державної таємниці чи відмову у наданні такого допуску. Висновок

органу СБУ , який провів перевірку працівника управління, щодо якого розглядається питання про надання допуску до державної таємниці, повинен ґрунтуватися на достовірних, об'єктивних і перевірених відомостях. Мотивований висновок органу СБУ є обов'язковим для виконання посадовими особами, уповноваженими приймати рішення про надання допуску до державної таємниці, але не виключає повторного запиту із цього приводу в разі зміни обставин, за яких допуск до державної таємниці визнано не можливим.

Якщо в результаті перевірки орган СБУ дійшов висновку про відсутність підстав для відмови у наданні працівнику допуску до державної таємниці, в обліковій картці робиться такий 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)".

Висновок в обліковій картці підписується керівником органу СБУ, із зазначенням дати і скріплюється печаткою. Заповнена таким чином облікова картка з одним примірником картки повертається до установи, організації, підприємства, що оформляло допуск до державної таємниці.

У разі коли за результатами перевірки зроблено висновок про неможливість надання працівнику допуску до державної таємниці, орган СБУ з посиланням на конкретні статті Закону України "Про державну таємницю" письмово повідомляє управління, про причини та підстави, внаслідок яких надання працівнику управління допуску неможливо. Висновок підписується керівником органу СБУ і надсилається разом з незаповненою обліковою карткою. Такий висновок не повинен містити відомостей, що становлять державну таємницю. Висновок про неможливість надання працівнику управління допуску до державної таємниці є обов'язковим для виконання посадовими особами установи, які уповноважені приймати рішення про надання такого 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 позитивного висновку органу СБУ та облікової картки..

Рішення про надання працівнику установи допуску до державної таємниці оформляється у формі наказу, після чого до СБУ надсилається заповнена картка, на зворотному боці якої зазначається номер та дата наказу про надання допуску.

В обліковій картці робиться відповідний запис із зазначенням форми допуску до державної таємниці, дати та номера наказу про його надання. Цей запис засвідчується підписом працівника РСО та скріплюється печаткою РСО.

У разі коли такий наказ не видано у визначений термін, висновок органу СБУ про відсутність підстав для відмови у наданні працівнику управління допуску до державної таємниці втрачає чинність. Про причини ненадання працівнику установи допуску до державної таємниці письмово інформується орган СБУ . Доцільно тим же наказом про надання допуску до державної таємниці працівнику управління одночасно надавати доступ до конкретної інформації, що становить державну таємницю.

4. Процедура і перелік документів для направлення до органів СБ України з метою отримання підприємством, установою і організацією спеціального дозволу

на провадження діяльності, пов’язаної з державною таємницею, визначені статтею 20 Закону України „Про державну таємницю” (далі – Закон) та Порядком 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 № 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.

Утворення, реорганізація чи ліквідація РСО здійснюється за попереднім погодженням з підприємствами, установами, організаціями вищого рівня або замовниками секретних робіт та органом СБУ. У своїй діяльності РСО взаємодіють з органом СБУ та РСО підприємств, установ, організацій вищого рівня або замовників секретних робіт.

До складу РСО входять підрозділи режиму, криптографічного, технічного захисту інформації, секретного діловодства та інші підрозділи, що безпосередньо забезпечують охорону державної таємниці, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації.

Для розгляду питання щодо погодження створення РСО керівник підприємства, установи, організації, до повноважень якого належить право прийняття такого рішення, подає органу СБУ вмотивований запит, у якому викладаються відомості про підпорядкованість РСО, його організаційно-штатну структуру, чисельність працівників підприємства, установи, організації, яким планується надати допуск до державної таємниці, характер секретних робіт, характеристику відомостей (ступені секретності, статті Зводу відомостей, що становлять державну таємницю, затвердженого наказом СБ України від 12.08.2005, які планується обробляти в ході провадження діяльності, пов’язаної з державною таємницею.

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, у якому роз'яснюються питання щодо необхідності призначення особи на таку посаду, викладаються відомості про попереднє погодження цієї кандидатури з РСО підприємства, установи, організації вищого рівня або замовника секретних робіт. У запиті також викладаються відомості про наявність на підприємстві, в установі, організації спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею, строк його дії та встановлену категорію режиму секретності.

До вмотивованого запиту додаються: копія документа, який містить інформацію про функціональні обов'язки, що передбачені за посадою, призначення на яку погоджується (у разі погодження покладення на працівника підприємства, установи, організації обов'язків щодо забезпечення режиму секретності також надсилаються 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, яка заповнюється і підписується особою, засвідчується підписом посадової особи підрозділу кадрового забезпечення та РСО і скріплюється печаткою 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).

До заявки додається акт перевірки стану режиму секретності на підприємстві, в установі, організації.

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. За наявності на підприємстві, в установі, організації органу спеціального зв'язку, до складу комісії включається особа, яка має допуск до шифрів та шифрувальної роботи.

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:

1) 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;

2) 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;

3) 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;

4) 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;

5) організацію і стан пропускного та внутрішньооб’єктового режиму, перелік інженерно-технічних засобів охорони із зазначенням їх відповідності вимогам до забезпечення режиму секретності;

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

7) наявність спеціальних засобів зв’язку та органу спеціального зв’язку, використання державних шифрів і криптографічних засобів, стан їх обліку;

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

9) 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);

10) пропозиції щодо надання підприємству, установі, організації спеціального дозволу.

Акт перевірки стану режиму секретності підписується членами комісії та затверджується керівником підприємства, установи, організації.

У разі коли спеціальний дозвіл надається підприємству, установі, організації вперше, заявка і акт перевірки стану режиму секретності оформляються та подаються органу СБУ підприємством, установою, організацією вищого рівня або замовником секретних робіт. В акті перевірки зазначаються відомості:

1) 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;

2) 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;

3) 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;

4) пропозиції щодо надання підприємству, установі, організації спеціального дозволу.

Після отримання зазначених документів орган СБУ призначає спеціальну експертизу.

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, оголошення рішення про проведення мобілізації та/або введення воєнного стану питання щодо надання спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею, органам військового управління, військовим частинам, установам і організаціям, іншим структурним підрозділам Збройних Сил України, інших військових формувань, правоохоронних органів спеціального призначення, Державної спеціальної служби транспорту, Державної служби спеціального зв'язку та захисту інформації України, що відмобілізовуються, доукомплектовуються, заново формуються, розглядається органом СБУ у десятиденний строк з дня отримання відповідних документів.

Для проведення спеціальної експертизи орган СБУ утворює спеціальну експертну комісію. У разі потреби до її складу можуть бути включені фахівці інших підприємств, установ, організацій за погодженням з їх керівниками.

За наявності на підприємстві, в установі, організації органу спеціального зв'язку чи шифрувального органу та/або використання ними державних шифрів і криптографічних засобів захисту секретної інформації до складу спеціальних експертних комісій входять представники Держспецзв'язку.

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.

Надання (переоформлення) дозволу здійснюється безкоштовно.

Строк дії спеціального дозволу установлюється органом СБУ залежно від обсягу секретних робіт, що проводяться відповідним підприємством, установою, організацією, ступеня секретності та обсягу пов'язаних з цими роботами відомостей, що становлять державну таємницю, категорії режиму секретності, але не може перевищувати п'яти років.

Якщо спеціальний дозвіл надається підприємству, установі, організації вперше, категорія режиму секретності встановлюється згідно із ступенем секретності робіт, які передбачено проводити відповідно до їх повноважень, державних завдань, програм, замовлень, договорів (контрактів), а строк дії такого спеціального дозволу не повинен перевищувати один рік.

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.

Повідомлення стосовно прийнятого рішення про відмову в наданні спеціального дозволу органи СБУ надсилають у письмовій формі підприємствам, установам, організаціям, що подали заявку, а також підприємствам, установам, організаціям вищого рівня чи замовникам секретних робіт. У повідомленні викладаються вимоги та рекомендації щодо подальших дій підприємства, установи, організації для недопущення витоку секретної інформації.

Наявність спеціального дозволу є підставою для обов'язкового укладення підприємством, установою, організацією договорів з підрозділами Державної фельд'єгерської служби та Державного підприємства спеціального зв'язку про доставку секретної кореспонденції.

Переоформлення спеціального дозволу здійснюється в порядку, передбаченому для його надання.

У разі закінчення строку дії спеціального дозволу матеріали для його переоформлення подаються органу СБУ не пізніше ніж за місяць до закінчення строку його дії.

Органам військового управління, військовим частинам, установам і організаціям, іншим структурним підрозділам Збройних Сил України, інших військових формувань, які змінюють умовне найменування та/або місце дислокації у разі оголошення рішення про проведення мобілізації, введення воєнного стану, спеціальний дозвіл не переоформляється. Про такі зміни орган військового управління надсилає у триденний строк до органу СБУ, який надав спеціальний дозвіл, відповідне повідомлення.

5. На підприємстві обов'язково на законодавчій основі повинні бути вжиті заходи по регулюванню прав володіння, користування та розпорядження конфіденційною інформацією, що складає його комерційну таємницю. Для запобігання витоку конфіденційної інформації необхідно встановити порядок допуску до комерційних секретів певних осіб персоналу підприємства.

За основу організації роботи по допуску до комерційної таємниці доцільно взяти вимоги, які належать до порядку допуску до державних секретів.

Під допуском до комерційної таємниці слід розуміти письмове розпорядження керівника (власника) підприємства або уповноваженої ним особи, яке надає конкретному співробітникові підприємства право на роботу або ознайомлення з документами, виробами та іншими носіями інформації, які класифіковані підприємством як комерційна таємниця .

На підприємстві, як правило, встановлюється триступенева система важливості комерційної таємниці, яка позначається такими обмежувальними грифами:

"Комерційна таємниця – особливо важливо" ("КТ-ОВ") "Комерційна таємниця – суворо конфіденційно "("КТ-СК") "Комерційна таємниця – конфіденційно" ("КТ-К").

З урахуванням цього допуск конкретному співробітникові оформлюється до одного із вказаних ступенів важливості відомостей в залежності від посади співробітника або характеру виконуваної ним роботи.

Допуск до комерційної таємниці надається дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої, комерційної, наукової чи іншої діяльності. Допуск вважається правомірним, що має юридичну силу, якщо він надається співробітнику підприємства наказом керівника (власника) підприємства або уповноваженої ним особи.

Надання допуску передбачає:

– перевірку співробітника в зв'язку з допуском до комерційної таємниці;

– ознайомлення співробітника зі ступенем відповідальності за порушення законодавства, пов'язаної з розголошенням ним комерційної таємниці.

При вирішенні питання про надання допуску до комерційної таємниці слід враховувати такі фактори:

– наявність у співробітника підприємства обґрунтованої необхідності в роботі з комерційною таємницею;

– відсутність у співробітника судимості за тяжкі злочини і, перш за все, за протиправні дії, пов'язані з комерційним шпигунством, розголошенням державної та комерційної таємниці, зловживаннями в сфері кредитно-фінансової і економічної діяльності;

– відсутність у співробітника психічних захворювань або розладів, вживання наркотичних засобів, алкоголю;

– повідомлення про себе недостовірних відомостей в процесі підготовки матеріалів до оформлення допуску;

– відсутність в оформлюваного зв'язків з числа співробітників конкуруючих фірм.

Співробітник підприємства, якому наданий допуск до комерційної таємниці, зобов'язаний:

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

– не сприяти вітчизняним та іноземним конкурентам у здійсненні діяльності, яка завдає шкоди інтересам підприємства;

– виконувати вимоги режиму, який встановлений "Положенням про комерційну таємницю підприємства та правила її збереження";

– дотримуватись інших вимог законодавства про комерційну таємницю.

Оформлення допуску співробітника підприємства до комерційної таємниці передбачає і можливість його позбавлення на законних підставах. Причинами та підставами позбавлення допуску можуть бути:

– розголошення співробітником довіреної йому комерційної таємниці;

– грубе порушення співробітником "Положення про комерційну таємницю підприємства та правила її збереження";

– втрата співробітником документів та інших матеріальних носіїв, які містять комерційну таємницю;

– надходження відносно співробітника відомостей, що компрометують його, які він приховував і які не могли бути враховані при вирішенні питання про його допуск;

– переведення співробітника на іншу ділянку роботи або посаду, що не пов'язана з необхідністю допуску до відомостей, які складають комерційну таємницю.

Позбавляти співробітника допуску мають право ті ж особи, які санкціонували йому допуск до комерційної таємниці. Якщо співробітник не згоден

з таким рішенням власника підприємства або уповноваженої ним особи, він, відповідно до конституційного, цивільного та трудового права може оскаржити його в судовому порядку.

Власник підприємства або уповноважена ним особа мають право розробляти та використовувати власну, але таку що не суперечить чинному законодавству, методологію вивчення та перевірки кандидата для роботи, пов'язаної з відомостями, що складають комерційну таємницю .

Правомірне використання у вивченні та перевірці кандидатів на допуск до комерційних секретів поліграфа (детектора брехні, ідея якого належить відомому українському вченому Олександру Романовичу Лур'є з Харкова), але його застосування можливо лише з особистої згоди особи, що перевіряється. Результати перевірки не повинні приховуватись від кандидата на роботу з комерційною таємницею (згідно зі ст. 32 Конституції України і ст. 9 закону "Про інформацію").

Організація роботи по оформленню допуску до комерційної таємниці повинна бути покладена на підрозділ безпеки. Доцільно, щоб цим підрозділом, спільно з керівниками інших підрозділів, передбачених статутом або положенням про підприємства, був розроблений перелік посад співробітників, які за своїм службовим становищем або за родом виконуваної роботи обов'язково повинні мати допуск до тієї чи іншої категорії важливості відомостей, які становлять комерційну таємницю підприємства. Керівник (власник) підприємства або уповноважена ним особа повинні затвердити даний перелік.

6. Від співробітника, якому оформлений допуск до комерційної таємниці, береться письмове зобов'язання про нерозголошення комерційної таємниці, яка буде йому довірена. Зобов'язання може мати довільну форму, але воно повинно мати такі реквізити:

– прізвище, ім'я, по-батькові співробітника;

– займана посада;

– зобов'язання не розголошувати відомості, що складають комерційну таємницю;

– попередження про те, що у випадку розголошення довірених секретів з працівником може бути розірвана трудова угода за ініціативою власника підприємства, або він може бути притягнутий до відповідальності в порядку, встановленому законодавством України;

– дата та власноручний підпис співробітника, який дав зобов'язання;

– підпис представника служби безпеки, який проінструктував співробітника, що підписав зобов'язання (типовий зразок зобов'язання додається).

При звільненні співробітника підприємства, який мав допуск до комерційної таємниці і дійсно володів нею, у нього слід, згідно зі ст. 34 Конституції України і "Положення про комерційну таємницю підприємства та правила її збереження", відібрати так зване попередження-зобов'язання про нерозголошення ним після звільнення комерційних секретів, до яких він мав доступ (типовий зразок попередження-зобов'язання додається).

Мета відбору такого попередження-зобов'язания :

– застерегти співробітника від розголошення комерційних секретів, які стали йому відомі під час роботи на підприємстві;

– створити юридичні гарантії для попередження можливого витікання комерційної таємниці до конкурентів через колишнього співробітника

підприємства;

– юридично гарантувати право підприємства на відшкодування можливих матеріальних або моральних збитків у випадку порушення колишнім співробітником своїх зобов'язань перед підприємством.

7. Доступ до комерційної таємниці – це письмова санкція власника підприємства або уповноваженої ним особи на ознайомлення або роботу з конкретними відомостями, що складають комерційну таємницю, співробітників підприємства та представників сторонніх організацій (під представниками сторонніх організацій слід розуміти співробітників органів державної влади і управління, аудиторських структур, українських та зарубіжних партнерів, клієнтів, контрагентів, конкурентів).

Допуск і доступ до комерційної таємниці являють собою дві різні юридичні категорії.

Допуск штатного співробітника підприємства до комерційної таємниці відрізняється від доступу тим, що останній, маючи допуск навіть найвищого рівня ("Комерційна таємниця – особливо важливо") не може отримати доступ до інформації більш нижчого рівня секретності за власного ініціативою або за вказівкою безпосереднього начальника без письмової санкції на це керівника підприємства. Іншими словами, співробітник підприємства може отримати право на ознайомлення з будь-якою комерційною таємницею лише в тому випадку, якщо вона дійсно необхідна йому в зв'язку з виконанням ним службових обов'язків або для виконання окремого доручення керівника підприємства.

Рішення про надання доступу до конкретної комерційної таємниці і її матеріальних носіїв здійснюється у вигляді резолюції власника підприємства на документі, з яким знайомиться представник сторонньої організації, або шляхом оформлення окремого письмового розпорядження.

З метою попередження витоку відомостей, з якими були ознайомлені особи, що отримали доступ до комерційної таємниці, від цих осіб береться зобов'язання про її збереження.

Закон "Про інформацію" вводить поняття режиму доступу до інформації. Режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації. За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Держава здійснює контроль за режимом доступу до інформації. Завдання контролю за режимом доступу до інформації полягає у забезпеченні додержанні вимог законодавства про інформацію всіма державними органами, підприємствами, установами та організаціями.

Питання юридичних гарантій збереження в таємниці конфіденційної інформації підприємства, до якої отримали доступ представники органів державного управління та ділових кіл, може бути вирішене наступними способами.

По-перше, шляхом взяття у осіб, які ознайомились з відомостями, що складають комерційну таємницю підприємства, зобов'язання про збереження ними в таємниці відомостей, які стали їм відомі. Таким юридичним документом може бути угода про конфіденційність, яка підписується особою, яка отримала доступ до інформації, що охороняється, і представником підприємства – власника комерційної таємниці (типовий зразок додається). Цей юридичний документ ґрунтується на інституті зобов'язального права України. Він широко

використовується в світовій практиці підприємництва.

По-друге, шляхом передачі (при необхідності) представникові сторонньої організації копії документа, що містить комерційну таємницю, під розписку на оригіналі .

По-третє, шляхом передачі інших матеріальних носіїв комерційної таємниці під розписку про їх отримання та попередження в письмовій або усній формі про необхідність збереження в таємниці відомостей, які містяться в переданому документі або іншому матеріальному носії комерційної таємниці.

Порядок доступу до комерційної таємниці повинен визначатися "Положенням про дозвільну систему доступу співробітників підприємства і представників сторонніх організації до відомостей, що складають, комерційну таємницю підприємства". При розробці дозвільної системи особливо ретельно слід відпрацьовувати положення, пов'язані з доступом до інформації, що охороняється, представників правоохоронних органів, органів державного управління, які здійснюють контроль за господарською діяльністю підприємстві згідно з законодавством мають право доступу до комерційної таємниці. В Положенні необхідно чітко визначити характер та обсяг інформації, з якою дозволяється або доцільно знайомити представників сторонніх організацій, а також посадових осіб підприємства, яким надається право вирішувати питання доступу до комерційної таємниці.

На підприємстві доцільно створити систему накопичення інформації про осіб, які мали доступ до конкретних відомостей, що складають комерційну таємницю. Її основне призначення – забезпечення оперативності, виграш в часі у випадку виявлення факту витікання інформації, що захищається. Вона дозволить при службовому розгляді факту витікання інформації визначити, хто і коли мав до неї відношення.

Система може передбачати:

– ведення на кожного співробітника підприємства, що має доступ до комерційної таємниці, особового рахунку, в який заносяться дані про всі відомості, з якими він знайомився у процесі роботи;

– ведення картотеки на найбільш важливі для підприємства відомості, що складають комерційну таємницю, і хто конкретно знайомився з ними.

Як показує практика, така система виправдовує себе. Вона дає можливість швидко і з максимальним успіхом відреагувати на факт витоку інформації. Її також можна використовувати для проведення різноманітних аналітичних досліджень, пов'язаних зі станом захисту комерційної таємниці підприємства.

Керівник підприємства може дозволити користування будь-якою захищеною інформацією будь-якому працівнику підприємства або особі, що прибула на об'єкт з іншої організації для вирішення певних питань, якщо щодо цих даних не встановлені обмеження на ознайомлення виробничо-комерційними партнерами по спільному виробництву тощо.

На невеликих підприємствах з обмеженим обсягом закритих робіт (документів і виробів) керівник має можливість особисто розподіляти всю закриту інформацію, що надходить ззовні й створюється всередині підприємства між працівниками незалежно від їхніх посад. У цьому випадку здійснюється так званий прямий розподіл класифікованої інформації. Однак прямий розподіл неможливий на підприємстві з великим обсягом закритих робіт, розосередженим по різних підрозділах і ділянках, у яких задіяні співробітники різних посадових категорій. За

таких умов керівник підприємства фізично не має можливості особисто регулювати потоки класифікованої інформації і розподіляти її між працівниками. Зростає ймовірність помилок у вигляді неправильного адресування відомостей або дозволу на доступ особам, що не мають до них прямого виробничого відношення.

Для якісного виконання управлінських функцій в даних умовах керівник підприємства частину своїх прав на розпорядження рухом класифікованих відомостей передає (делегує) керівникам нижчестоящих рівнів. При визначенні повноважень кожного з нижчестоящих керівників виконується ряд умов. Повноваження особи повинні відповідати й здійснюватися в рамках її посадового становища (прав і обов'язків) і поширюватися тільки на певні категорії виконавців закритих робіт і документів.

Найважливіше значення для збереження комерційної таємниці має надійність співробітника, якому дозволяють працювати з цінною інформацією. У зв'язку з цим система доступу має бути заснована на переконанні, що особа, яка одержує дозвіл на доступ до закритих відомостей, лояльна стосовно підприємства (віддана фірмі). Такий висновок можуть зробити в процесі спільної діяльності служба безпеки й відділ кадрів. Ці підрозділи затверджують у директора список співробітників, які за своїми особистими якостями можуть бути допущені (або не допущені) до роботи з відомостями, що складають комерційну таємницю. Відповідні виписки передаються для обліку керівникам підрозділів, яким директором делеговане право видавати дозволи на доступ до конкретних відомостей, що входять у Перелік захищуваної інформації.

Керівник, як правило, залишає за собою право розпоряджатися найбільш цінними відомостями, що складають КТ (конфіденційні договори з фірмами, звіти про результати робіт з перспективних виробів тощо). Перелік таких документів, затверджений директором, має знаходитися в службі безпеки (СБ). Відповідно до цього переліку вся класифікована інформація й вироби, що надійшли ззовні чи створені на підприємстві, доповідаються керівництву СБ. Інша інформація надходить зі СБ безпосередньо керівникам підрозділів відповідно до діючої на підприємстві дозвільної системи. Вони й розподіляють її між виконавцями. Кількість рівнів посадової ієрархії і посадових осіб, яким можуть бути надані повноваження на розподіл класифікованої інформації, залежить від структури підприємства, кількості й складності проведених закритих робіт.

Правила ефективної роботи дозвільної системи підприємства:

– Дозвільна система в якості обов'язкового для виконання правила містить у собі диференційований підхід до дозволу доступу, що враховує важливість класифікованих відомостей, щодо яких вирішується питання про доступ.

– Необхідне документальне відображення виданого дозволу на право користування тими або іншими відомостями. Це означає, що керівник, який дав дозвіл на право користування, повинен його обов'язково зафіксувати в письмовому вигляді на відповідному документі або в діючій на підприємстві обліковій формі. Жодні усні вказівки й прохання про доступ будь-кого (за винятком керівника підприємства) не мають юридичної чинності й не є обов'язковими для працівників СБ. Ця вимога стосується і керівників усіх рівнів, що працюють з класифікованою інформацією та її носіями. Таким чином, тільки письмовий дозвіл керівника (у рамках повноважень) є дозволом для видачі тій або іншій особі відомостей, що охороняються.

– Слід суворо дотримуватися принципу контролю з боку СБ. Це означає, що

будь-який дозвіл (тут можливі вилучення за узгодженням з керівником) на ознайомлення із закритими документами, відомостями й об'єктами має бути погоджений з начальником СБ. Кожний дозвіл повинен мати дату його оформлення, видачі та терміну чинності.

Значного поширення набув такий традиційний вид дозволу, як резолюція керівника на класифікованому документі. Такий дозвіл повинен містити перелік прізвищ співробітників, зобов'язаних ознайомитися з документами або виконати їх, термін виконання, інші вказівки, підпис керівника і дату. Керівник може за необхідності передбачити обмеження в доступі конкретних співробітників до певних відомостей.

Резолюція, як вид дозволу, застосовується головним чином для оперативного доведення до зацікавлених осіб закритої інформації, що міститься в документах і виробах, які надходять як ззовні, так і створюються на підприємстві.

Керівник підприємства може дати дозвіл на доступ у розпорядницьких документах: наказах, вказівках, розпорядженнях. В них повинні міститися прізвища, посади осіб, конкретні класифікаційні документи й вироби, до яких вони можуть бути допущені (ознайомлені).

Інший вид дозволів - списки осіб за прізвищами, що мають право знайомитися і здійснювати будь-які дії з класифікованими документами й виробами. Списки затверджуються директором підприємства або, відповідно до діючої дозвільної системи керівниками, що посідають, як правило, посади не нижчі керівники відповідних підрозділів. Вони можуть використовуватися при організації доступу до класифікованих документів і виробів, що мають особливо важливе значення для підприємства, при оформленні доступу в режимні приміщення, на закриті заходи (конференції, наради, виставки, засідання науково-технічних рад тощо). У списках за прізвищами можуть бути визначені конкретні керівники, які допускаються керівником до всіх закритих документів і виробів без відповідних письмових дозволів. У них вказується П.І.Б. виконавця робіт, відділ, займана посада, категорія документів і виробів, до яких він допущений. На практиці застосовується і варіант посадових списків, у яких вказується: посада виконавця, обсяг документів (категорії документів) і типи виробів, якими необхідно користуватися працівникам підприємств, які займають відповідну списку посаду. Слід зазначити, що для підприємств з невеликим обсягом класифікованих документів і виробів може виявитися достатнім використання таких видів дозволу, як резолюція керівника на самому документі, списки за прізвищами, посадові списки.

В організаційному плані списки за прізвищами повинні готуватися зацікавленими керівниками структурних підрозділів. Перелік співробітників, що ввійшли в список, візується начальником СБ і затверджується керівником підприємства, що може делегувати права затвердження іншим особам з числа дирекції.

Поряд зі списками можуть бути використані персональні картки-дозволи.

Дозвільна система має відповідати таким вимогам:

– поширюватися на всі види класифікованих документів і виробів, що є на підприємстві, незалежно від їхнього місця перебування і створення;

– визначати порядок доступу всіх категорій співробітників, які одержали право працювати з КТ, а також фахівців, що тимчасово прибули на підприємство і мають відношення до спільних закритих замовлень;

– встановлювати простий і надійний порядок оформлення дозволів на доступ до документів і виробів, які охороняються, що дозволяє негайно реагувати на зміни в області інформації на підприємстві;

– чітко розмежовувати права керівників різних посадових рівнів в оформленні доступу відповідних категорій виконавців;

– виключати можливість безконтрольної і несанкціонованої видачі документів і виробів будь-кому;

– не дозволяти особам, які працюють з класифікованою інформацією й об'єктами, вносити зміни в парні дані, а також підмінювати облікові документи.

При розробці дозвільної системи особлива увага має приділятися виділенню головних, особливо цінних для підприємства відомостей, що дозволить забезпечити до них суворо обмежений доступ. За наявності спільних робіт з іншими підприємствами (організаціями), іноземними фірмами або їхніми окремими представниками необхідно передбачити порядок доступу цих категорій працівників до комерційної таємниці підприємства. Доцільно визначити порядок взаємодії з представниками обслуговуючих державних організацій: технаглядом, санітарно-епідеміологічною станцією, податковими, правоохоронними та митними органами тощо.

У межах дозвільної системи керівники середньої ланки управління повинні:

– давати дозвіл (у рамках повноважень) на доступ до класифікованих документів і відомостей виконавцям свого підрозділу, виконавців інших підрозділів за клопотанням їхніх керівників і в межах їхніх функціональних обов'язків;

– знати ступінь важливості проведених робіт, розроблювальних виробів та виробів що знаходяться в процесі документації, і завдання та функціональні обов'язки своїх підлеглих;

– негайно повідомляти в СБ про зміни функціональних обов'язків співробітників, не допускаючи адресування їм документів і виробів до переоформлення функціональних обов'язків у спеціальних рішеннях (посадових інструкціях тощо);

– не допускати з боку підлеглих дій, що тягнуть порушення вимог дозвільної системи, вживати заходів для уникання невиправданого ознайомлення з тими відомостями, що не відносяться до обов'язків працівника;

– здійснювати контроль за адресуванням класифікованих документів і виробів, ознайомленням з ними відряджених осіб.

Співробітники СБ фірми повинні контролювати:

– правомірність видачі інформації, яка охороняється і виробів співробітникам підприємства і відряджених осіб;

– правомірність адресування класифікованих документів і виробів з одного підрозділу в інший;

– порядок оформлення доступу до комерційної таємниці фірми.

У Положенні про дозвільну систему фірми необхідно зазначити, що передача класифікованих документів і виробів від одного виконавця до іншого можлива тільки в межах структурного підрозділу і з дозволу його керівника. Передача, повернення таких документів здійснюється за встановленим на фірмі порядком і тільки протягом конкретного робочого дня.

Вся класифікована документація й вироби, що надійшли на підприємство і розроблені на ньому, приймаються і враховуються працівниками СБ. Після

реєстрації документація передається на розгляд керівнику підприємства під розписку. Керівники можуть передавати документи і вироби на виконання після їх реєстрації тільки через СБ.

Попередній розгляд оперативного листування, оцінка ступеня важливості виробів здійснюється начальником (або спеціально виділеним референтом директора), що визначає необхідність надання отриманої інформації керівнику фірми. Документи і вироби, що не потребують обов'язкового розгляду директором фірми, надаються іншим керівникам фірми і начальникам структурних підрозділів. Розглянуті директором вхідні й внутрішні документи та вироби адресуються відповідним керівникам і виконавцям структурних підрозділів, які роблять позначки про дозвіл на самих документах (супровідних паперах до виробів). Контроль за правильністю адресування документів і виробів здійснюється керівництвом підрозділу економічної безпеки.

Переадресування класифікованих документів і виробів здійснюється керівниками фірми, зазначеними в дозвільній системі, начальниками структурних підрозділів у межах свого підрозділу. При невідповідності документа і виробу функціональним обов'язкам виконавця питання вирішується на відповідному рівні за участю СБ.

Відряджені особи можуть бути допущені до закритих відомостей тільки з дозволу керівника фірми або його заступників, яким таке право передане. Дозвіл надається письмово. Він повинен чітко визначати обсяг комерційної таємниці і коло питань, з яких можна надавати інформацію. У ньому обов'язково вказується посадова особа, відповідальна за прийом і роботу з відрядженими.

У картці про допуск відрядженого керівник повинен зазначити, які об'єкти, служби, приміщення має право відвідати відряджений. Він може бути присутнім на нарадах, які розглядають тільки питання, визначені для нього керівником підприємства.

У Положенні про дозвільну систему фірми необхідно вказати, що закриті наради зі службових питань проводяться тільки з дозволу керівника фірми або його заступників. Особливі вимоги можуть поширюватися на засідання вчених рад, наради з розгляду результатів НДДКР і фінансово-комерційної діяльності тощо. На такі заходи рекомендується обов'язково оформляти дозвільні списки і включати в них лише тих співробітників, які мають безпосереднє відношення до запланованих заходів і участь в яких викликана службовою необхідністю.

Як уже зазначалося, співробітники інших фірм можуть брати участь у закритих нарадах тільки з персонального дозволу керівництва фірми. Готує списки, як правило, відповідальний за організацію наради в контакті із зацікавленими керівниками структурних підрозділів. Список є підставою для організації контролю за допуском на дану нараду. Перед початком наради співробітник СБ попереджає присутніх, що обговорювана інформація має закритий характер і не підлягає розголошенню поза встановленою фірмою сферою обігу, і видає інструкції щодо порядку ведення записів.

Важливо підкреслити, що встановлення на фірмі певного порядку обігу закритої інформації і виробів істотно підвищує надійність захисту комерційної таємниці, знижує імовірність її розголошення, втрати носіїв цих відомостей.

8. Створення ефективної системи інформаційної безпеки є неможливим без чіткого визначення загроз інформації, що охороняється. 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.

Фахівці встановлюють, у середньому, таке співвідношення зовнішніх і внутрішніх загроз: 82 % загроз створюються співробітниками фірми або за їх прямої чи опосередкованої участі; 17 % загроз виникає ззовні - зовнішні загрози; 1 % загроз створюється випадковими особами.

Основними загрозами інформації є її розголошення, витік і несанкціонований доступ до її джерел.

Розголошення інформації. Розголошення комерційних секретів, мабуть, найбільш розповсюджена дія власника (джерела), що призводить до неправомірного оволодіння конфіденційною інформацією за мінімальних витрат зусиль з боку зловмисника. Для цього він користується в основному легальними шляхами і мінімальним набором технічних засобів.

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).

Як правило, 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 загалом можна розглядати як неправомірний вихід конфіденційної інформації за межі організації або кола осіб, яким ця інформація була довірена.

Витік інформації за своєю суттю завжди припускає протиправне (таємне або явне, усвідомлене або випадкове) оволодіння конфіденційною інформацією, незалежно від того, яким шляхом це досягається.

Причини витоку полягають, як правило, у недосконалості норм щодо збереження комерційних секретів, порушенні цих норм, а також відступі від правил поводження з відповідними документами, технічними засобами, зразками продукції та іншими матеріалами, що містять конфіденційну інформацію.

Умови передбачають різні фактори й обставини, що складаються у процесі наукової, виробничої, рекламної, видавничої, звітної, інформаційної та іншої

діяльності підприємства (організації) і створюють передумови для витоку комерційних секретів. До таких факторів і обставин можуть, наприклад, належати:

- недостатнє знання працівниками підприємства правил захисту комерційної таємниці та нерозуміння (або непорозуміння) 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 які володіють інформацією, що становить комерційну таємницю.

Таким чином, значна частина причин і умов, що створюють передумови і можливість неправомірного оволодіння конфіденційною інформацією, виникають через недбалість керівників підприємств та їхніх співробітників.

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

До інших способів несанкціонованого доступу до інформації, які не порушують норм закону, але знаходяться 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.

Перехід від абстрактного до конкретного захисту зазвичай розпочинається з виявлення та аналізу найбільш уразливих місць. Таким місцем, безумовно, є джерела, що містять інформацію конфіденційного характеру.

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

1. Документація підприємства або просто документи (вхідні-вихідні, накази, бізнес-плани, ділова переписка тощо).

Важливою особливістю документів є те, що вони іноді є єдиним джерелом найважливішої інформації (наприклад контракт, боргова розписка), а отже, їхня втрата, викрадення чи знищення може завдати непоправної шкоди. Розмаїття форм і змісту документів за призначенням, спрямованістю, характером руху і використанням є досить привабливим джерелом для зловмисників, що, природно, привертає їхню увагу до можливості одержання цінної інформації. Важливим напрямом інформаційної безпеки у цьому напрямі буде створення системи секретного та конфіденційного діловодства на підприємстві.

2. Робочий персонал або просто особи (до цього поняття належать усі без винятку працівники підприємства).

Фізичні особи серед джерел конфіденційної інформації посідають особливе місце як активний елемент, здатний виступати не тільки джерелом, а й суб’єктом зловмисних дій. Люди є і власниками, і розповсюджувачами інформації у межах

своїх функціональних обов'язків. Крім того, що вони мають інформацію, вони ще здатні її аналізувати, узагальнювати, запам'ятовувати, робити відповідні висновки, а також, за певних умов, ховати, продавати, змінювати тощо.

3. Партнери, контрагенти або клієнти. Всі знають, що відносини між партнерами завжди мають правову форму. Зміст цих документів переважно містить для конкурентів цінну комерційну інформацію. Тому необхідно забезпечити конфіденційність таких документів або ж передбачити відповідальність за протиправне розголошення змісту таких документів третім особам.

Забезпечити комерційну таємницю, що міститься в угодах з партнерами, можна двома шляхами:

1) включити до змісту договору окремі пункти про збереження комерційної таємниці, де передбачити, яка інформація становить комерційну таємницю, які підстави і порядок розголошення цієї інформації третім особам (контролюючим органам, судовим інстанціям, іншим підприємствам тощо), яка відповідальність за несанкціоноване розголошення комерційної таємниці;

2) якщо ж відносини з партнерами і контрагентами мають тривалий і стійкий характер, то доцільним буде окремий договір (угода) про збереження комерційної таємниці, де більш детально буде розроблений режим збереження комерційної таємниці.

4. Продукція підприємства або послуги, що надаються. Продукція є особливим джерелом інформації, за характеристиками якої досить активно полюють конкуренти. Особливої уваги заслуговує нова, що готується до виробництва, продукція. Вважають, що для продукції існують визначені етапи «життєвого циклу»: задум, макет, зразок, іспити, серійне виробництво, експлуатація, модернізація і зняття з виробництва. Кожний із цих етапів супроводжується специфічною інформацією у вигляді різних фізичних ефектів, які можуть розкрити охоронювану інформацію.

5. Технічні засоби забезпечення виробничої діяльності. Технічні засоби як джерела конфіденційної інформації є широкою в інформаційному плані групою джерел. Засоби забезпечення виробничої діяльності можуть бути найрізноманітнішими, такі, зокрема, як телефони і телефонний зв'язок, телевізори і промислові телевізійні установки, радіоприймачі, радіотрансляційні системи, системи гучномовного зв'язку, підсилювальні системи, охоронні й пожежні системи тощо, котрі за своїми параметрами можуть бути джерелами перетворення акустичної інформації на електричні та електромагнітні поля, здатні утворювати електромагнітні канали витоку конфіденційної інформації.

6. Непрямі джерела (сміття, реклама, публікації). Велика частина інформації добувається саме з непрямих джерел. Професійно проведена аналітична робота дає змогу іноді одержати чудовий результат. Крім того, цьому джерелу, звичайно, не надається особливої уваги, а отже, він найбільш доступний. Наприклад, відходи виробництва, що називають непридатним матеріалом, можуть багато чого розповісти про матеріали, що використовуються, їхній склад, особливості виробництва, технології. Тим більше їх одержують майже безпечним шляхом на смітниках, місцях збору металобрухту, у кошиках кабінетів. Вмілий аналіз цих «відходів» може багато чого розповісти про секрети виробництва. Публікації — це інформаційні носії у вигляді найрізноманітніших видань: книги, статті, монографії, огляди, повідомлення, рекламні проспекти, доповіді, тези тощо, в яких ви можете, самі того не бажаючи, розкрити всі секрети.

Джерела конфіденційної інформації дають повні зведення про склад, зміст і напрям діяльності підприємства (організації), що досить цікаво для конкурентів. Природно, що така інформація їм вкрай необхідна, і вони докладуть усіх зусиль, знайдуть необхідні способи, щоб одержати необхідну їм інформацію. Тому грамотна система захисту, розроблена з урахуванням усіх особливостей, дозволить запобігти багатьом проблемам.

Беручи до уваги все викладене вище, забезпечення інформаційної безпеки можна поділити на такі основні напрями:

- у будь-якій організації необхідно розробляти і вводити просту систему класифікації ступеня конфіденційності інформації, що обробляється (гриф обмеження доступу). Гриф можна присвоїти за допомогою штампів, спеціальних оцінок, а можна і за допомогою кольору (наприклад документи загального користування — білого кольору, документи службового — жовті, а таємні — червоного);
- обов'язково встановити процедуру передання конфіденційної інформації від одного співробітника іншому, порядок її обробки і збереження залежно від ступеня таємності. (Це неминуче призведе до включення до цієї процедури аспектів забезпечення комп'ютерної безпеки, а також порядку ведення діловодства загалом і встановлення правил роботи з конфіденційними документами.) Краще, якщо робота з контролю за документами буде доручена окремому співробітнику (наприклад інспектору по режиму роботи з документами), в ідеалі цим повинна займатися група режиму служби безпеки підприємства;
- необхідно постійно проводити з персоналом компанії розмова про правила поводження з конфіденційною інформацією [5, 6].

Таким чином, створення системи інформаційної безпеки є масштабною роботою, яка вимагає серйозних зусиль. Тому фахівці радять, насамперед, найбільш точно визначити ризики, які існують для інформаційної безпеки підприємства, і не вживати додаткових заходів забезпечення безпеки, якщо це реально не відобразиться на зростанні самого бізнесу.

9. Технічні заходи захисту базуються на використанні різних електронних пристроїв і спеціальних програм, що входять до складу системи обробки інформації та виконують функції захисту. Наприклад, пошукові прилади, прилади охорони провідних комунікацій, програмне забезпечення, апаратура для виявлення диктофонів, системи акустичного і віброакустичного зашумлення, скануючі засоби, засоби виявлення каналів витоку інформації, встановлення спеціального обладнання для спостереження за приміщеннями організації тощо.

Апаратні засоби захисту застосовуються для вирішення таких завдань:

1. перешкоджання візуальному спостереженню і дистанційному підслуховуванню;
2. нейтралізація паразитних електромагнітних випромінювань і наводок;
3. виявлення технічних засобів підслуховування і магнітного запису, несанкціоновано встановлених або які пронесено до установ підприємства, банку;
4. захист інформації, що передається засобами зв'язку і знаходяться в системах автоматизованої обробки даних.

За своїм призначенням апаратні засоби захисту поділяються на засоби виявлення і засоби захисту від несанкціонованого доступу. Слід зазначити, що універсального

засобу, який би дозволяв виконувати всі функції, не існує, тому для виконання кожної функції відповідно до виду засобів несанкціонованого доступу існують свої засоби пошуку та захисту. За таких умов заходи щодо протидії незаконному вилученню інформації за допомогою цих засобів досить трудомісткі та дорогі і вимагають спеціальної підготовки фахівців.

Захист інформації від копіювання здійснюється завдяки виконанню таких функцій:

1. Ідентифікація середовища, з якого може запускатись програма;
2. Аутентифікація середовища, із якого запущена програма;
3. Реакція на запуск із несанкціонованого середовища;
4. Реєстрація санкціонованого копіювання;
5. Протидія вивченню алгоритмів роботи системи.

Тема 6. Організація внутрішньо-об’єктного та пропускного режиму на підприємствах, що здійснюють роботу з відомостями визначеними державною таємницею

Структура та повноваження режимно-секретних органів. Внутрішньо - об’єктний режим та його задачі. Підрозділи підприємства, які вирішують завдання по організації внутрішньо-об’єктного режиму. Організаційні засоби захисту інформації

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

Створення, реорганізація чи ліквідація РСО здійснюються за погодженням із Службою безпеки України. У своїй роботі РСО взаємодіють з органами Служби безпеки України. До складу режимно-секретного органу входять підрозділи режиму, секретного діловодства та інші підрозділи, що безпосередньо забезпечують охорону державної таємниці, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації.

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях із значним обсягом робіт, пов'язаних з державною таємницею, вводиться посада заступника керівника з питань режиму, на якого покладаються обов'язки та права керівника РСО.

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях з незначним обсягом робіт, пов'язаних з державною таємницею, де штатним розписом не передбачено створення РСО, 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. На них поширюються обов'язки та права працівників РСО.

Призначення осіб на посади заступників керівників з питань режиму, начальників РСО та їх заступників, а також видання наказу про покладення на окремого працівника обов'язків щодо забезпечення режиму секретності здійснюється за погодженням з органами Служби безпеки України та РСО вищестоящих державних органів, органів місцевого самоврядування, підприємств, установ і організацій.

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

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.

Передача функцій РСО будь-яким іншим підрозділам державного органу, органу місцевого самоврядування, підприємства, установи та організації не допускається.

2. Внутрішньо-об’єктний і пропускний режими встановлюються, як правило, на підприємствах, що здійснюють в передбаченому законодавством порядку роботу з відомостями, що становлять державну таємницю. Внутрішньо-об’єктний і пропускний режими являють собою основні елементи системи захисту інформації

підприємства.

Організація зазначених режимів – обов'язкова вимога нормативно-методичних документів щодо захисту державної таємниці, що надають підприємству право на проведення робіт, пов'язаних з використанням відомостей, що становлять державну таємницю. Внутрішньо-об’єктний 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. Організація і забезпечення внутрішньо-об’єктного і пропускного режимів на підприємстві спрямовані на дотримання всіма співробітниками підприємства і відрядженими особами належного режиму секретності.

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. Таким чином, внутрішньо-об’єктний і пропускний режими є невід'ємною частиною комплексу заходів, спрямованих на захист відомостей, що становлять державну таємницю, і збереження їх носіїв.

Внутрішньо-об’єктний 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 внутрішньо-об’єктного 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, хто приймається на роботу громадянами.

Завдання по організації внутрішньо-об’єктного режиму на підприємстві покладаються, як правило, на заступника керівника підприємства, який відповідає за питання захисту державної таємниці. Заступник керівника підприємства роботу по формуванню системи внутрішньо-об’єктного режиму організовує на основі всебічного аналізу можливих каналів витоку відомостей, що становлять державну таємницю, при проведенні підприємством всіх видів робіт.

В ході виконання цієї роботи керівництвом підприємства використовуються такі основні підходи до організації внутрішньо-об’єктного 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.

Керівник підприємства та відповідні посадові особи повинні забезпечити дотримання основних принципів формування системи внутрішньо-об’єктного режиму: принципу персональної відповідальності керівників структурних підрозділів, інших посадових осіб і співробітників підприємства за виконання завдань у сфері захисту державної таємниці; принципу комплексного використання наявних сил і засобів для вирішення завдань щодо захисту державної таємниці; принципу повного охоплення всіх напрямків діяльності підприємства, в ході роботи по яким може бути витік відомостей, що становлять державну таємницю, або втрата носіїв цих відомостей.

Внутрішньо-об’єктний режим передбачає наступні 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 розсекречення 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 щодо захисту державної таємниці, і визначення їх функцій;

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

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

• проведення роботи серед співробітників, допущених до державної таємниці, щодо роз'яснення вимог режиму секретності, підвищенню 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 проведені 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.

Найважливішу роль в організації внутрішньо-об’єктного режиму відіграють керівник підприємства і його заступник, що відповідно до своїх посадових обов'язків безпосередньо очолюють роботу із захисту державної таємниці. Відповідно до нормативних актів безпосередня відповідальність за організацію і здійснення заходів щодо захисту державної таємниці покладається на керівника підприємства. Керівник підприємства, з урахуванням аналізу стану захисту державної таємниці і результатів контролю ефективності вирішення завдань щодо захисту державної таємниці посадовими особами та структурними підрозділами підприємства, визначає (уточнює) завдання цим посадовим особам і структурним підрозділам.

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 халатності 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.

Заступник керівника підприємства відповідає за практичну діяльність структурних підрозділів підприємства і посадових осіб щодо захисту державної таємниці. В рамках діяльності по організації внутрішньо-об'єктного режиму він виконує наступні 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, що 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. Для організації внутрішньо-об'єктного режиму використовується сукупність наявних на підприємстві структурних підрозділів, що виконують функції захисту державної таємниці, а також інших підрозділів, які вирішують завдання в даній сфері, і застосовуваних цими підрозділами засобів захисту інформації. В організації внутрішньо-об'єктного режиму беруть участь наступні 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).

Провідну роль в організації внутрішньо-об'єктного режиму на підприємстві, а також здійснення контролю ефективності проведених в цих цілях заходів посідає режимно-секретний підрозділ. Він виконує такі основні завдання:

• розробка спільно з іншими підрозділами підприємства заходів щодо організації внутрішньо-об'єктного режиму;

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

• організація та ведення обліку, 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 по виключенню 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 засекречування, в роботі експертних комісій з розсекречення 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 ведення обліку 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 відомостей, що становлять державну таємницю;

• 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 ведення обліку 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 при вирішенні покладених на них завдань 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.

Поряд з режимно-секретним підрозділом важливу роль в організації

внутрішньо-об’єктного режиму на підприємстві відіграє служба безпеки. Вона створюється рішенням керівника на підприємствах, що виконують роботи одночасно з декількома видами конфіденційної інформації, в тому числі і з відомостями, що становлять державну таємницю. В такому випадку режимно-секретний підрозділ підприємства може структурно входити до складу служби безпеки, і завдання, що на них покладені, підлягають виконанню службою безпеки.

Разом з тим поряд зі службою безпеки в структурі підприємства може діяти самостійний режимно-секретний підрозділ. У цьому випадку завдання служби безпеки підприємства в області організації внутрішньо-об’єктного режиму наступні:

• забезпечення економічної безпеки, охорони власності підприємства;

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

• захист конфіденційної інформації під час здійснення зовнішньоекономічної діяльності підприємства;

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

• виявлення і закриття можливих каналів витоку конфіденційної інформації;

• розробка системи організаційних і технічних заходів, що регламентують внутрішньо-об'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 і т.п.);

• 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 внутрішньо-об’єктного режиму на підприємстві;

• взаємодія з правоохоронними та іншими державними органами з питань забезпечення безпеки підприємства.

Підрозділи підприємства, які вирішують завдання по організації внутрішньо-об’єктного режиму, у своїй діяльності використовують різні засоби захисту інформації.

4. У вирішенні задач організаційного забезпечення інформаційної безпеки підприємства важливу роль відіграють організаційні засоби захисту інформації.

Під організаційними засобами захисту інформації розуміється комплекс заходів, що плануються і здійснюються з метою організації внутрішньо-об’єктного режиму. Вони є, по суті, сполучною ланкою між персоналом підприємства і різними технічними та іншими засобами, використовуваними в цілях організації та забезпечення режиму секретності.

Найбільш ефективні такі заходи щодо 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.

Порядок організації внутрішньо-об’єктного режиму, завдання, які вирішуються посадовими особами та структурними підрозділами підприємства, відображаються в розроблюваних на підприємстві внутрішніх організаційно-розпорядчих документах, що затверджуються керівником підприємства. Співробітники, в установленому порядку допущені до інформації з обмеженим доступом та здійснюють безпосередню роботу з цією інформацією, несуть відповідальність за дотримання вимог нормативних актів з порядку поводження з носіями конфіденційної інформації і за збереження цих носіїв.

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 тієї 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);

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

• забезпечувати на своєму робочому місці таке розташування носіїв конфіденційної інформації, яке дозволяє виключити несанкціоноване ознайомлення з ними (їх 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 службових приміщень і робочих місць;

• 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.

Перераховані обов'язки доводяться до відома всім співробітникам підприємства, що працюють з конфіденційною інформацією (її носіями), під розписку в журналі, що зберігається в режимно-секретному підрозділі (службі безпеки). Ці обов'язки доводяться також до відома осіб, новопризначених на відповідні посади (які прибули на підприємство).

Організація внутрішньо-об’єктного і пропускного режимів має на меті виключення проникнення сторонніх осіб в режимні приміщення підприємства, а також несанкціонованого відвідування таких приміщень співробітниками підприємства і відрядженими особами, які не мають прямого відношення до проведених в них робіт. До приміщень, призначених для ведення робіт з використанням відомостей, що становлять державну таємницю, або для зберігання їх носіїв, пред'являється ряд вимог. На практиці дані вимоги, як правило, поширюються на службові приміщення і сховища підприємства, в роботі яких використовуються або зберігаються не тільки названі відомості, а й інші види конфіденційної інформації (або її носії). Це дозволяє забезпечити збереження у конфіденційності проведених у зазначених приміщеннях робіт, а також надійне збереження носіїв конфіденційної інформації.

Розміщення і обладнання вказаних режимних приміщень повинні виключати можливість безконтрольного проникнення в них сторонніх осіб і гарантувати збереження носіїв конфіденційної інформації, що в них знаходяться. Тому до даних приміщень пред'являються особливі вимоги режиму секретності. Вхідні двері цих приміщень обладнуються замками, що гарантують надійне закриття приміщень в неробочий час, в них також можуть встановлюватися кодові і електронні замки і автоматичні турнікети.

Режимні приміщення, в яких в неробочий час зберігаються носії конфіденційної інформації, оснащуються охоронною сигналізацією, пов'язаної 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.

Перед початком експлуатації режимні приміщення обстежуються комісією, яка призначається керівником підприємства, і атестуються на відповідність вимогам, що пред'являються до приміщень для проведення робіт з конкретним видом конфіденційної інформації. Результати роботи комісії оформляються актом придатності приміщення для проведення конкретних видів робіт, що затверджується керівником підприємства. Обстеження та атестація режимних приміщень проводиться не рідше одного разу на 5 років, а також після їх ремонту або реконструкції.

У ці приміщення допускається строго обмежене коло співробітників підприємства, що мають пряме відношення до робіт, що в них проводяться. Крім того, в них допускаються керівник підприємства, його заступник, керівник служби безпеки, керівник режимно-секретного підрозділу та їх заступники. Доступ інших співробітників підприємства в ці приміщення в разі крайньої службової необхідності може бути дозволений заступником керівника підприємства, керівником режимно-секретного підрозділу або його заступником.

Для здійснення прийому і видачі носіїв конфіденційної інформації режимні приміщення відповідних структурних підрозділів (режимно-секретного підрозділу або служби безпеки) обладнуються спеціальними вікнами, що не виходять в загальний коридор, або виділяється частина робочої кімнати, ізольована бар’єром. Розмір режимних приміщень визначається виходячи з функцій цих приміщень . Щоб дізнатися більше про роботи з носіями конфіденційної інформації в приміщеннях служби безпеки (режимно-секретного підрозділу) виділяються спеціальні кімнати (кабіни).

У режимних приміщеннях служби безпеки (режимно-секретного підрозділу) забороняється працювати з документами, що не мають безпосереднього відношення до основної діяльності даної служби (підрозділу), а також зберігати сторонні предмети. Для зберігання носіїв конфіденційної інформації приміщення забезпечуються необхідною кількістю сховищ, замки яких обладнуються пристосуваннями для опечатування. Сховища і ключі від сховищ зберігаються і облікуються в службі безпеки (режимно-секретному підрозділі). Сховища, а також вхідні двері приміщень, в яких вони знаходяться, обладнуються надійними замками з двома примірниками ключів від них, один з яких в опечатаному пеналі (пакеті) зберігається у керівника служби безпеки (режимно-секретного підрозділу). Другий примірник ключів в опечатаному вигляді зберігається у керівника підприємства або у його заступника.

У неробочий час ключі від сховищ і від вхідних дверей режимних приміщень, в окремих пеналах, опечатаних черговим по службі безпеки (режимно-секретного підрозділу), передаються на зберігання службі охорони або черговому по підприємству. Після закінчення робочого дня всі сховища і режимні приміщення закриваються і опечатуються. Сховища і вхідні двері приміщень, в яких вони знаходяться, опечатуються різними печатками. При опечатування

мастика (пластилін) або сургуч накладаються таким чином, щоб унеможливити їх зняття без пошкодження відбитка печатки.

Режимні приміщення, в яких зберігаються носії конфіденційної інформації, з опечатаними вхідними дверима і пенали з ключами від них здаються під охорону службі охорони або черговому по підприємству із зазначенням часу прийому-здачі та проставленням відповідних відміток про включення і виключення охоронної сигналізації.

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 їх підписів. Списки знаходяться в службі охорони або у чергового по підприємству. Співробітники підприємства, яким надано право на відкриття, здачу під охорону та опечатування приміщень, відповідають за дотримання в цих приміщеннях встановлених вимог режиму секретності.

При відсутності співробітників підприємства, відповідальних за приміщення, в яких зберігаються носії конфіденційної інформації, дані приміщення можуть бути розкриті комісією, яка створюється за вказівкою керівника підприємства (його заступника) зі складанням акту. Перед розкриттям приміщень співробітники, відповідальні за них, перевіряють цілісність печаток і справність замків. При виявленні порушення цілісності відбитків печаток, пошкодження замків, а також інших ознак, що вказують на можливе проникнення в ці приміщення або сховища сторонніх осіб, відкриття не провадять, а про те, що трапилося складають акт і негайно доводять до відома керівника підприємства, керівника служби безпеки (режимно-секретний підрозділ) і орган безпеки. Одночасно приймаються заходи з охорони місця події, до прибуття співробітників органу безпеки в ці режимні приміщення ніхто не допускається.

Тема 7. Організація роботи з документами що становлять комерційну таємницю

Інструкція з організації роботи з документами, що містять комерційну таємницю. Облік документів, що містять комерційну таємницю. Друкування та розмноження документів. Формування документів у справи. Доступ до документів, що містять комерційну таємницю, та користування ними. Забезпечення збереженості документів, що містять комерційну таємницю. Зняття грифа обмеженого доступу та відбір документів, що містять комерційну таємницю, для знищення.

1. Конфіденційне діловодство – це окремий напрям діловодства. Для забезпечення його ефективного функціонування важливе значення має розроблення спеціальної інструкції та додатків до неї, складання списку конфіденційної інформації, проставлення грифа обмеження доступу. При веденні конфіденційного діловодства слід приділити увагу відповідній підготовці документів, що містять комерційну таємницю, належному порядку робіт з ними, зокрема на електронних носіях.

Конфіденційне діловодство здійснюється шляхом вирішення комплексу організаційно-правових, інженерно-технічних, криптографічних та оперативно-пошукових заходів, спрямованих на запобігання розголошення інформації з обмеженим доступом та втратами її матеріальних носіїв. Технологічні процеси цієї практичної сфери діяльності загалом базується на тих самих принципах, що і загального (відкритого) діловодства, але відрізняються низькою суттєвих відмінностей.

До організаційно-технологіних особливостей конфіденційного діловодства належать:

– жорстке регламентування складу документів та процесу документування, у т.ч. і стосовно проектів створюваних документів;

– облік усіх примірників конфіденційних документів, включаючи їх проекти;

– реєстрування максимально повних даних про кожен документ обмеженого доступу;

– фіксування проходження кожного документа та місця його перебування;

– проведення систематичних перевірок наявності документів;

– дозвільна система допуску до документів і справ;

– суворі вимоги до умов зберігання документів і до їх використання;

– персональна та обов`язкова відповідальність за облік, збереження документів і порядок користування ними.

Сукупність організаційних, трудових та інших аспектів організації роботи з конфіденційною інформацією може бути подана в Інструкції з організації роботи з документами, що містять комерційну таємницю .

Основними завданнями локальної Інструкції є встановлення загальних правил збереження інформації, яка наявна у документах обмеженого доступу, єдиного порядку документування й організації роботи з документами, що містять комерційну таємницю. Таку інструкцію розробляють для захисту підприємства від несанкціонованого витоку інформації. Для цього винаходять нові методи удосконалення роботи з документами, що містять КТ, методи організації захищеного документообігу та його упорядкування, принципи оптимізації технологічних процесів роботи з документами, що містять КТ.

При розробці Інструкції слід керуватися Інструкцією 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 року №1893, Інструкцією про порядок відбору та передавання секретних документів на архівне зберігання, затвердженою спільним наказом Державного комітету України з питань державних секретів та технічного захисту інформації і Головного архівного управління при Кабінеті Міністрів України (нині Держкомархівом України) від 3 березня 1997 року № 25/7 та відомчими нормативно-правовими та нормативно-методичними актами.

Усі працівники, які займаються веденням діловодства на підприємстві, мають бути ознайомлені з правилами та положеннями Інструкції під розписку при прийнятті на роботу, а також у разі внесення до неї змін або доповнень.

Інструкція може складатися з таких розділів: Загальні положення. Перелік відомостей, що становлять КТ. Підготовка службових документів, що містять КТ. Порядок роботи з документами, що містять КТ, на електронних носіях. Прийняття і облік документів, що містять КТ. Розмноження і розсилання (відправлення)

документів. Формування справ виконаних документів. Відбір документів для зберігання і знищення. Забезпечення збереження документів. Перевірка їх наявності. Облік, зберігання і використання печаток, штампів і бланків.

До Інструкції можуть додаватися численні додатки, як то: Акт про відсутність вкладень у конверті (пакеті); Журнал обліку документів та видань з грифом «КТ»; Картка обліку документів та видань з грифом «КТ»; Журнал обліку магнітних носіїв інформації з грифом «КТ»; Картка обліку магнітних носіїв інформації з грифом «КТ»; Журнал обліку та розподіл видань з грифом «КТ»; Картка обліку справ і видань, що містять гриф «КТ»; Опис справ постійного зберігання; Акт про знищення документів і справ, що не підлягають зберіганню; Акт перевірки наявності та стану документів і справ; Журнал обліку бланків тощо.

Вимоги до порядку зберігання архівних документів з обмеженим доступом можуть урегульовуватися окремою інструкцією або ж долучатися до цієї. У такому разі окремими розділами Інструкції можуть бути: підготовка документів з обмеженим доступом до передавання на архівне зберігання; складання і оформлення описів справ та актів про відбір для знищення документів, що не підлягають зберіганню; оформлення справ з обмеженим доступом; передавання документів з обмеженим доступом і справ на архівне зберігання; зберігання архівних документів з обмеженим доступом у державних архівних установах.

2.. Облік документів, що містять комерційну таємницю, охоплює: присвоєння та проставлення в облікових формах і на документах реєстраційних номерів; запис облікових і пошукових даних (дати, автора, заголовка, кількості сторінок, відомостей про місцезнаходження тощо) про документи.

Обліку підлягають усі без винятку виготовлені на підприємстві документи з грифом обмеженого доступу. Їх обліковують за кількістю сторінок, а друковані видання (книги, журнали, брошури) – за кількістю примірників. Документи, що містять комерційну таємницю, реєструють один раз. Облік ведеться у журналі обліку конфіденційних документів та видань або на картках, зазвичай окремо від обліку документів загального діловодства.

Облік магнітних носіїв інформації з грифом обмеженого доступу ведеться окремо від обліку паперових документів. Одержавши документ, який містить комерційну таємницю, працівник підприємства повинен: звірити номер отриманого документа з його номером у журналі реєстрації; перевірити кількість аркушів цього документа; розписатися за отриманий документ. Повертаючи документ, що містить комерційну таємницю, працівник служби діловодства (секретар) зобов'язаний: звірити номер документа з відповідним номером у журналі реєстрації; перевірити кількість аркушів цього документа; розписатися у відповідній графі журналу за повернутий документ і проставити дату повернення у присутності працівника, який щойно повернув цей документ.

Сторінки реєстраційних журналів нумерують, прошнуровують і опечатують. На останній обліковій сторінці робиться запис про кількість сторінок у журналі. Цей запис має засвідчувати працівник служби діловодства (секретар), проставивши відбиток печатки для пакетів.

При незначному обсязі документів з грифом обмеженого доступу можна за рішенням керівництва підприємства вести їх облік (реєстрацію) разом з документами загального діловодства. При цьому на картці (у журналі) до реєстраційного номера документа чи видання, що містить комерційну таємницю,

додається відповідна відмітка, скажімо: «12-Д СК» «123 - Конф.» «567-КТ» тощо.

Тираж видання з грифом обмеженого доступу, отриманий для розсилання, реєструють під одним вхідним номером у журналі обліку і розподілу видань з відповідними грифами. Додатково розмножені примірники документа (видання) враховують за номером цього документа (видання), про що роблять відмітку на розмноженому документі (виданні) та в усіх облікових формах. При цьому нумерація додатково розмножених примірників ведеться від останнього номера примірників, розмножених раніше.

3. Друкують документи, що містять комерційну таємницю, у друкарському бюро чи у структурних підрозділах підприємства.

Відповідальність за збереження й нерозголошення таємної інформації несуть керівники цих підрозділів.

На звороті останньої сторінки кожного примірника документа друкарка повинна вказати:кількість надрукованих примірників; прізвище працівника — виконавця документа; власне прізвище; дату виконання документа.

Надруковані й підписані примірники вихідних документів з грифом обмеженого доступу разом із чернетками чи попередніми варіантами передають для реєстрації працівникові служби діловодства (секретарю), який здійснює їх облік. Чернетки й варіанти знищує виконавець документа у присутності працівника служби діловодства (секретаря), про що на копії вихідного документа (т. зв. відпуску документа), що підшивається до справи підприємства, роблять запис: «Чернетки і варіанти знищено»,проставляють дату, ставлять підписи. Розмножують документи, що містять комерційну таємницю, з дозволу керівника підприємства чи структурного підрозділу, котрий відповідає за безпеку підприємства, під контролем служби діловодства (секретаря). Копіювально-розмножувальна техніка, використовувана при цьому, має оснащуватися технічними засобами захисту інформації.

Облік розмножених документів ведеться за кількістю примірників. У реєстраційних формах, які веде друкарське бюро, до реєстраційного номера чи назви документа додається відповідна відмітка: «ДСК», «Конф.» або «КТ» Розсилання документів, що містять комерційну таємницю, здійснюється на підприємства і керівником служби діловодства, із зазначенням облікових номерів примірників, що розсилаються.

Відправляють документи цінними або рекомендованими поштовими відправленнями, або доставляють кур’єри під розписку в реєстрі. Документи, що надсилаються до інших підприємств, установ і організацій (далі— підприємство), слід укладати у конверти або упаковувати так, щоб унеможливити доступ до них. При цьому конверти мають бути світлонепроникними, а пакети щільно заклеєними. На конвертах або інших упакуваннях обов’язково вказують: назву і адресу підприємства-одержувача; назву і адресу підприємства-відправника; номери вкладених документів із зазначенням відповідної відмітки «ДСК», «Конф.» або «КТ».

4. Документи, що містять комерційну таємницю, після їх виконання формують у справи. Порядок їх формування відповідає порядку формування справ у загальному діловодстві й здійснюється на підставі номенклатури справ підприємства. При цьому до номенклатури справ включають усі документи з

грифами обмеженого доступу, а також довідкові й реєстраційні картотеки й журнали до них.

Документи, що містять комерційну таємницю, залежно від виробничої і довідково-інформаційної потреби дозволяється формувати у справи окремо або разом з несекретними документами з одного й того самого питання. Втім, якщо на підприємстві створюється значна кількість документів однакового виду (як-от, плани, звіти, інструкції, накази тощо) з грифом обмеженого доступу, доцільно передбачити їх формування в окремі справи. При цьому у першій графі номенклатури справ, що має назву «Індекс справи», до номера справи з документами, які містять комерційну таємницю, додається відповідна відмітка, скажімо «03-11-КТ».

У разі укладення документа з грифом обмеженого доступу до справи з документами, що не мають такого грифа, на справі ставиться відповідна відмітка, скажімо «ДСК», а до номенклатури справ вносяться відповідні зміни.

Якщо у процесі діяльності підприємства створюється незначна кількість документів , що містять комерційну таємницю, номенклатурою справ може передбачатися запровадження лише однієї справи із заголовком «Документи з грифом «Для службового користування» або «Документи з грифом «Комерційна таємниця».

Строк зберігання такої справи не встановлюється, а у відповідній графі номенклатури справ проставляється відмітка «ЕК»

Після закінчення діловодного року таку справу переглядають поаркушно члени експертної комісії (ЕК) і в разі потреби ухвалюють рішення про переформування документів справи. Таким чином документи постійного зберігання, що містяться у справі, формують в окрему справу, якій надається окремий заголовок і яку додатково включають до номенклатури справ, а документи тимчасового зберігання залишаються у попередній розформованій справі згідно із затвердженою номенклатурою справ.

Якщо у справі з грифом обмеженого до ступу містяться лише документи тимчасового зберігання, її дозволяється не переформовувати. Строк зберігання такої справи встановлюється відповідно до найбільшого строку зберігання документів, що містяться в ній. Скажімо, якщо у справі разом сформовано документи, що мають строки зберігання 3, 5 і 10 років, справі слід установити відповідний максимальний строк зберігання, тобто 10 років. У такому разі відмітка «ЕК» у графі «Строк зберігання» номенклатури справи закреслюється і замінюється уточненим строком зберігання.

Справи, у яких накопичуються окремі документи, що містять комерційну таємницю, належать до категорії обмеженого розповсюдження й використання. На обкладинках і титульних аркушах цих справ також проставляється гриф обмеженого доступу, а у номенклатуру справи вносяться відповідні уточнення. Ще один важливий аспект, на який слід звернути увагу: справи з документами, що містять конфіденційну інформацію, повинні мати внутрішні описи.

5. Доступ до документів, що містять комерційну таємницю, здійснюється лише на підставі письмового дозволу керівника підприємства. Дозвіл на доступ може оформлятися як: резолюція керівника підприємства на документі; оформлене у змісті розпорядчого документа (наказу, розпорядження або рішення) доручення щодо виконання документа із зазначенням посади і прізвища працівника —

виконавця документа; окремо оформлений письмовий дозвіл на видавання документів (зокрема архівних документів і справ).

Доступ до вхідних конфіденційних документів, що надійшли до підприємства, здійснюється на підставі резолюції керівника на самому документі або на супровідному листі до нього. Із супровідного листа зміст резолюції переноситься на документ і засвідчується підписом особи, відповідальної за облік, опрацювання та зберігання документів з грифом обмеженого доступу із зазначенням дати.

Доступ виконавців до документів, що містять комерційну таємницю, здійснюється відповідно до затвердженого списку посадових осіб, які мають право працювати з такими документами. Зміни до цих списків, пов'язані з розширенням або, навпаки, з обмеженням зазначеного кола осіб, вносяться з письмового дозволу керівника підприємства на підставі відповідних доповідних записок керівників структурних підрозділів. Виконавець документа (якщо він і далі працює з тією самою тематикою) та особи, які візували й підписували документ, допускаються до нього без спеціального дозволу.

У разі відсутності виконавця у зв'язку з відрядженням, відпусткою чи хворобою його документами мають право користуватися керівник структурного підрозділу, у якому він працює, або за письмовим дозволом керівника — інші працівники того самого підрозділу, які мають стосунок до зазначених документів.

Якщо відсутній виконавець, документи, що містять комерційну таємницю, з якими він працював, вилучає із сейфа у встановленому на підприємстві порядку спеціально призначена комісія, обов'язково склавши акт.

Відомості, що містяться в конфіденційних документах, не дозволяється використовувати у відкритих виступах чи публікувати в засобах масової інформації, а також забороняється експонувати такі документи на відкритих виставках, демонструвати на стендах, вітринах тощо.

Знімати копії і робити витяги з внутрішніх документів, що містять комерційну таємницю, можна лише з дозволу керівника підприємства чи керівника відповідного структурного підрозділу, який відповідає за ці документи. Копіювати вхідні документи з грифом обмеженого доступу, отримані від інших підприємств, можна лише з дозволу підприємств – авторів цих документів.

Справи з грифом обмеженого доступу можна видавати з архіву підприємства чи відомчих бібліотек закритого типу таким особам:працівникам підприємства за списком, затвердженим керівником цього підприємства або за його письмовим дозволом; працівникам інших підприємств – за їхнім письмовим зверненням і на підставі письмового дозволу керівника підприємства-фондоутворювача.

Справи й видання, що містять комерційну таємницю, видають виконавцям для роботи й приймають від них під розписку в журналі обліку та видавання справ і видань, що містять комерційну таємницю.

6. Документи, що містять комерційну таємницю, потребують особливого режиму зберігання. Їх треба зберігати у службових приміщеннях у шафах (сейфах), сховищах, що надійно замикаються й опечатуються.

Документи, видані для роботи працівникам-виконавцям, повертають до служби діловодства (секретарю) або в архів того самого дня. У деяких випадках з дозволу керівника служби діловодства чи особи, відповідальної за архів підприємства, документи можуть зберігатися у працівника протягом терміну,

потрібного йому для виконання завдання, за умови цілковитого забезпечення їх збереженості. При цьому документи не дозволяється залишати на столі, закінчивши роботу, їх треба покласти до шафи, що замикається, або сейфа.

Документи, що містять комерційну таємницю, не дозволяється виносити за межі підприємства. Лише за умови потреби їх погодження з фахівцями з інших підприємств, що територіального розташовані в одному населеному пункті, керівник підприємства може видати працівникам письмовий дозвіл на винесення цих документів за межі підприємства. Працівникам, відрядженим з виробничою метою до інших населених пунктів, забороняється мати при собі документи, що містять комерційну таємницю підприємства. Такі документи заздалегідь пересилають за призначенням.

Наявність документів, що містять комерційну таємницю, щорічно переглядає комісія, спеціально призначена наказом керівника підприємства. До складу комісії входять особи, яким доручено облік і зберігання цих документів, а також працівники режимно-секретного підрозділу підприємства.

В архівах і бібліотеках, де зберігається значна кількість документів із грифом обмеженого доступу, перевірка їх наявності може проводитися один раз на п’ять років. Результати перевірок завжди оформляють протоколом. Виявивши у ході перевірки втрату документів з грифом «КТ» або розголошення відомостей, що містять комерційну таємницю, про це терміново доповідають керівництву підприємства, керівникам режимно-секретного відділу і служби діловодства, а також службі безпеки підприємства, якщо така на підприємстві є. Для розслідування факту втрати документів або розголошення інформації, що міститься в них, наказом керівника підприємства призначається комісія, висновок якої, незалежно від результатів, затверджує керівник підприємства.

7. Справи постійного та тривалого (понад 10 років) зберігання з грифом обмеженого доступу «ДСК», «Конф.», «КТ» тощо періодично (зазвичай один раз на 5–10 років) переглядають, аби зняти відповідний гриф. Рішення про зняття грифа зі справ або видань ухвалює експертна комісія підприємства — автора відповідних документів або його правонаступника. Рішення комісії оформляється актом і затверджується керівником підприємства. В акті зазначають заголовки й номери за описом справ, з яких знімається гриф. На обкладинках справ гриф обмеженого доступу погашається штампом або записом від руки із зазначенням дати й номера акта. Аналогічні відмітки вносять до опису й номенклатури справ.

Про зняття грифа обмеженого доступу з документа інформують усі підприємства, яким надсилався цей документ.

Знімається з інформації статус комерційної таємниці після закінчення контрольного строку або втрати цього статусу через певні обставини, як-от: поява нової технології, методу, зразка, формули тощо або витік інформації до компанії-конкурента.

Публікуючи або представляючи у публічному виступі інформацію, яка доти була закритою, рекомендуємо наголошувати на її практичній цінності й ексклюзивності, щоб зацікавити споживачів у її використанні як у межах країни, так і за кордоном.

Разом з тим обсяг опублікованих або оприлюднених іншим способом даних не повинен бути достатнім для їх самостійного впровадження споживачами без додаткової інформації розробника.

На документи постійного строку зберігання або зі строком зберігання «До ліквідації підприємства» і тривалого (понад 10 років) зберігання з грифом обмеженого доступу складають описи справ, оформляють обкладинки справ, а також самі справи відповідно до архівних правил. Відібрані для знищення документи, строк зберігання яких минув, включають до акта про вилучення документів для знищення. Якщо документи з грифом обмеженого доступу включають до загального акта разом з несекретними справами, то в графі «Заголовок справи» після номерів цих справ проставляють відповідну відмітку. Знищують документи лише після затвердження цього акта керівником підприємства.

Відібрані для знищення документи, що містять комерційну таємницю, перед передаванням на перероблення на макулатуру слід подрібнювати до стану, що унеможливлює їх прочитання.

Якщо обсяг справ, відібраних для знищення, є незначним, їх можна спалити, про що в акті робиться відмітка. Після знищення документів з грифом обмеженого доступу в облікових формах (картках, журналах, номенклатурах, описах справ тимчасового зберігання) робиться така відмітка: «Знищено. Акт № __ від (дата) ».
Інформаційні видання, телефонні й адресні довідники, копії документів, стенографічні записи й друкарський брак, що також можна віднести до категорії конфіденційних документів (видань), дозволяється знищувати без акта, але з позначкою в облікових формах, що засвідчуються підписами виконавця і працівника, відповідального за їх облік і зберігання.

Тема 8. Правове регулювання питань збереження комерційної таємниці при укладенні підприємницьких договорів і веденні ділових переговорів

Дотримання вимог, які надають договору достатню юридичну силу. Характеристика окремих видів договорів за якими передається комерційно-цінна інформація: збереження елемента конфіденційності предмета угоди у разі передавання науково-технічних знань, технологічного досвіду та технічних рішень; договір про НДР ТА ДКТР; договір комерційної концесії, опціонний договір; договір про конфіденційність. Особливості укладення угоди з іноземною фірмою, якщо вона має конфіденційний характер. Умови збереження комерційної таємниці у процесі ділових зустрічей партнерів.

1. Під договором про надання інформації слід розуміти договір, за яким одна особа (володілець інформації) зобов’язується надати іншій особі (отримувачу інформації) визначену інформацію, а отримувач інформації, якщо інше не передбачено договором, зобов’язується сплатити за неї певну грошову суму.

Взагалі ж договори на передачу інформації в юридичній літературі розглядаються у контексті надання комерційної таємниці.

Одним із прав суб'єкта підприємницької діяльності, який володіє комерційною таємницею, є право на розпорядження інформацією, що йому належить. Мається на увазі не тільки можливість розкрити таку інформацію, а й передання її іншим особам на договірних засадах.

Вимог, які надають договору достатню юридичну силу залежать від дотримання сторонами при його укладенні певних вимог, встановлених законом. Такі вимоги закону ще іменуються умовами дійсності договору.

Зміст договору, якій укладався, повинен відповідати вимогам закону. Зокрема, договір не може укладатися з приводу дій, що порушують норми права. Вимога законності договору тлумачилася римськими юристами розширювально, тобто вони вважали, що зміст договору не повинен суперечити не тільки нормам права, але й добрим звичаям та нормам моралі.

Волевиявлення сторін є обов'язковою умовою дійсності договору.

Воля – це внутрішнє бажання особи встановити певні права та обов'язки. У договорі воля сторін повинна бути взаємною та спрямованою на досягнення певної мети. У зв'язку з тим, що сторони у договорі мають протилежні цілі, то їх волі є зустрічними. Для укладення договору воля однієї особи має бути доведена до іншої сторони. Волевиявлення – це зовнішня об'єктивна форма виявлення волі особи. Способи волевиявлення можуть бути різноманітним: усно, письмово, жестом, певною дією, мовчанням. Для дійсності договору необхідно, щоб воля та волевиявлення співпадали. Тривалий час серед римських юристів точилася дискусія щодо того, воля чи волевиявлення (у разі їх неспівпадіння) мають враховуватися при тлумаченні договору. Врешті решт було визнано, що при розбіжності між волею та волевиявленням пріоритет надається дійсній волі.

У випадках, коли воля та волевиявлення не збігалися, мова йшла про помилку (error). Помилка (error) – це неправильне уявлення однієї сторони договору про виявлену зовні волю іншої сторони, яка спонукала останню на певне волевиявлення. Помилка була пов'язана не із незнанням права, а з незнанням фактів (обставин справи). Правові наслідки помилки залежали від того чи була ця помилка істотною (помилка щодо характеру договору, його предмету, особи контрагента) або неістотною (помилка щодо мотиву). Тільки істотна помилка могла бути підставою для визнання договору недійсним. Вчення про помилку не було у достатній мірі розроблено римськими юристами.

Волевиявлення особи мало юридичне значення тільки, якщо ця особа за законом була здатна до волевиявлення, тобто мала цивільну правоздатність та дієздатність.

Не має юридичної сили договір, зміст якого є не визначеним взагалі. Римське право поділяло договірні зобов'язання на визначені та невизначені. Але такій поділ стосувався тільки договорів із визначеним змістом, тобто дійсних договорів. Предмет визначених договорів визначався чітко (індивідуально-визначена річ), а предмет невизначених договір окреслювався загальним ознаками (речі, визначені родовими ознаками). Форма договору – це форма волевиявлення. У різні часи формами договорів були: манципація, стипуляція, письмова форма. Форми для окремих видів договорів встановлювалися у законі. Недодержання сторонами форми договору призводило до його недійсності.

Для дійсності договору юридичне значення мала здійсненність встановлених ним обов'язків боржника. При вирішенні питання чи має юридичну силу той чи інший договір враховувався той факт чи існує реальна можливість вчинення дії, яка передбачена у договорі. Неможливість виконання договірного зобов'язання може бути фізична або юридична. Неможливість виконання боржником свого обов'язку може настати під час існування договору. У цьому разі договірне зобов'язання припиняється у зв'язку з неможливістю його виконання. Якщо ж буде встановлено, що вже в момент укладення договору вбачалося, що він не може бути виконаний, він визнається недійсним.

2. В процесі розвитку та вдосконалення ринкових відносин, виникнення нових зв'язків між підприємствами відбувається створення проблем двостороннього захисту комерційної таємниці торгових партнерів. В практичній роботі зарубіжних підприємств передбачений перелік спеціальних договорів, щодо двостороннього захисту інформації, яка передана одним підприємством іншому в процесі ділового співробітництва. Для відповідності інтересів продавців (що не бажають повідомити будь-яку інформацію про власний товар до підписання угоди на постачання) з інтересами покупців (які не бажають отримувати товар, про який відсутня поки що повна інформація) відбувається використання опціонної угоди. Суть цієї угоди полягає в тому, що покупці на умовах конфіденційності і за визначену плату отримують додаткову інформацію про товари, до складу якої можуть становити відомості, які містять в собі комерційну таємницю. Договору предметом якого є відомості , що становлять комерційну таємницю більш детальну увагу буде зосереджено в наступному питанні.

В ЦК України немає закріпленої узагальнюючої норми, яка б врегульовувала договір про конфіденційність. Але все таки, в ньому є перелік окремих норм, які врегулюють конфіденційність інформації окремих видів договорів.

Так, ст. 862 ЦК України передбачено конфіденційність отриманої інформації всіма сторонами за договором підряду. Згідно з цим якщо одна сторона в договорі внаслідок виконання умов договору отримала від іншої сторони інформацію про якесь нове рішення, про певні знання технічного характеру, загалом і такі, які не передбачають захист на підставі закону, включаючи також інформацію, яка може становити собою комерційну таємницю, то їй заборонено розповсюджувати таку інформацію іншим зацікавленим особам, без згоди другої сторони.

Захист та збереження комерційної таємниці передбачено і в договорі про страхування. Згідно ст. 40 Закону України «Про страхування» конфіденційні відомості, щодо фінансового стану і діяльності страхувальника – клієнта страховика, що стала відома йому в процесі взаємовідносин з клієнтами чи із третіми особами, при здійсненні діяльності в сфері страхування, розголошення якої може завдати моральних чи матеріальних збитків клієнтові, є таємницею страхування.

Конфіденційність інформації може бути передбачено і в умовах ліцензійного договору .

До договорів, які покликані впорядковувати суспільні відносини в інформаційній сфері відносять договір на виконання науково-дослідних або дослідно-конструкторських та технологічних робіт.

Відповідно до ст. 892 ЦК України, за договором на виконання науково-дослідних або дослідно-конструкторських та технологічних робіт підрядник (виконавець) зобов'язується провести за завданням замовника наукові дослідження, розробити зразок нового виробу та конструкторську документацію на нього, нову технологію тощо, а замовник зобов'язується прийняти виконану роботу та оплатити її.

Предметом зазначеного договору є виконання науково-дослідних або дослідно-конструкторських робіт. Сутність таких робіт полягає у зборі та обробці інформації, в результаті чого виникає нова інформація – результат діяльності виконавця, котра передається змовнику у вигляді науково-дослідної чи конструкторської документації.

Стаття 895 ЦК України «конфіденційність відомостей про договір»

закріплює, що на замовника і виконавця покладено обов'язок забезпечувати збереження таємності інформації, що стосується предмету договору щодо проведення технологічних, дослідно-конструкторських і науково-дослідних робіт, процесу його здійснення і отриманих результатів, якщо інше не закріплено положеннями договором. Об'єм інформації, яка належить до конфіденційної, встановлюється умовами договору.

Укладення та виконання таких договорів призводить до появи у замовника нової інформації, яка передається йому виконавцем. Виконавець, надаючи інформацію замовнику, здійснює дії щодо поширення інформації, відповідно має місце здійснення права на інформацію юридичним способом.

Комерційна концесія – один з нових правових інститутів, що знайшов своє відображення у ЦК України. Метою договору комерційної концесії в українському цивільному законодавстві є надання права використання в підприємницький діяльності комплексу виключних майнових прав інтелектуальної власності. У міжнародному праві існує аналог договору комерційної концесії – франчайзинг.

Експерти ВОІВ визначають договір франчайзингу (договір комерційної концесії) як «договір, згідно з яким одна особа (правоволоділець), яка має розроблену систему ведення певної діяльності, дозволяє іншій особі (користувачу) використовувати цю систему відповідно до вимог правоволодільця в обмін на винагороду.

Згідно зі ст. 1115 ЦК України за договором комерційної концесії одна сторона (правоволоділець) зобов’язується надати другій стороні (користувачеві) за плату право користування відповідно до її вимог комплексом належних цій стороні прав з метою виготовлення та/або продажу певного виду товару та/або надання послуг.

Договір комерційної концесії укладається суб’єктами господарювання. Ними можуть виступати тільки комерційні юридичні особи і фізичні особи, зареєстровані як суб’єкти підприємницької діяльності у встановленому законом порядку – правоволоділець і користувач.

Правоволоділець – виробник товарів (робіт, послуг), який використовує належні йому права в підприємницькій діяльності, має комерційний досвід і ділову репутацію та зацікавлений у розширенні свого бізнесу.

Користувач – юридична або фізична особа, зареєстрована як суб'єкт підприємницької діяльності і має намір скористатися комплексом прав правоволодільця.

Особливістю предмета договору комерційної концесії полягає в тому, що він являє собою комплекс виключних прав, які необхідні для використання в певній сфері підприємницької діяльності. Відповідно до ст. 1116 ЦК України предметом договору є:

1) право на використання об’єктів права інтелектуальної власності. До цих прав законом віднесені, зокрема, право на використання торговельних марок, промислових зразків, винаходів, комерційних таємниць тощо. Іншими словами, йдеться про виключні права на результати інтелектуальної діяльності, і, насамперед, про ті з них, які спрямовані на індивідуалізацію продукції. Перелік прав, передбачений ч. 1 ст. 1116 ЦК України, не є вичерпним, однак загальною рисою їх є майновий характер та можливість відчуження.

2) право на використання комерційного досвіду, що включає технічну та комерційну документацію, та іншу інформацію, необхідну для здійснення прав,

наданих користувачеві за договором комерційної концесії, а також відповідне професійне навчання персоналу, спеціальний інструктаж протягом строку дії договору з різних питань щодо господарської діяльності та управління, експлуатації обладнання, ведення обліку та звітності, обслуговування клієнтів тощо.

3) право на використання ділової репутації. Ділова репутація – це сукупність підтвердженої інформації про особу, що дає можливість зробити висновок про професійні та управлінські здібності такої особи, її порядність та відповідність її діяльності вимогам закону. Її формування відбувається шляхом всебічного сприйняття юридичної особи, її оцінки різними групами осіб: споживачами, діловими партнерами, громадськими організаціями, органами державної влади.

Договір комерційної концесії є взаємним, таким чином, правам однієї сторони кореспондують обов'язки іншої.

Правоволоділець зобов'язаний передати користувачеві технічну та комерційну документацію і надати іншу інформацію, необхідну для здійснення прав, наданих йому за договором комерційної концесії, а також проінформувати користувача та його працівників з питань, пов'язаних із здійсненням цих прав.

Правоволоділець зобов'язаний, якщо інше не встановлено договором комерційної концесії: забезпечити державну реєстрацію договору; надавати користувачеві постійне технічне та консультативне сприяння, включаючи сприяння у навчанні та підвищенні кваліфікації працівників; контролювати якість товарів (робіт, послуг), що виробляються (виконуються, надаються) користувачем на підставі договору комерційної концесії.

З урахуванням характеру та особливостей діяльності, що здійснюється користувачем за договором комерційної концесії, користувач зобов'язаний: використовувати торговельну марку та інші позначення правоволодільця визначеним у договорі способом; забезпечити відповідність якості товарів (робіт, послуг), що виробляються (виконуються, надаються) відповідно до договору комерційно ї концесії, якості аналогічних товарів (робіт, послуг), що виробляються (виконуються, надаються) правоволодільцем; дотримуватися інструкцій та вказівок правоволодільця, спрямованих на забезпечення відповідності характеру, способів та умов використання комплексу наданих прав використанню цих прав правоволодільцем; надавати покупцям (замовникам) додаткові послуги, на які вони могли б розраховувати, купуючи (замовляючи) товари (роботи, послуги) безпосередньо у правоволодільця; інформувати покупців (замовників) найбільш очевидним для них способом про використання ним торговельної марки та інших позначень правоволодільця за договором комерційної концесії; не розголошувати секрети виробництва правоволодільця, іншу одержану від нього конфіденційну інформацію.

Договір комерційної концесії є одним із видів договорів, в яких найбільш вагомого значення набуває збереження комерційної таємниці.

Важливість збереження комерційної таємниці у даному договорі зумовлена тим, що, як зазначається в літературних джерелах, одним з основних елементів предмету франчайзингового договору є передання франчайзером франчайзі створеної і перевірених на практиці конкурентноздатної системи організації і ведення будь-яких видів підприємницької діяльності (комерційної таємниці). Проблеми із збереження в таємниці основних елементів системи, є одними з найважливіших проблем, які виникають при укладенні і реалізації договору

франчайзингу (комерційної концесії).

Основним об'єктом, який передається за договором комерційної концесії, є певні секретні відомості, які стають відомими користувачам тільки після підписання договору. І тому, на момент його укладення користувач має тільки загальне враження про них. Пересвідчитись користувач , наскільки відсотків вони відповідають дійсності, зможе лише після того, коли він почне працювати за франчайзинговою схемою і буде інвестувати власні кошти для її розвитку . Якщо взяти до уваги існування об'єктів конфіденційного характеру про франшизу, користувачі можуть мати помилкове уявлення про неї. Часто вони можуть діяти внаслідок впливу обману чи помилки з боку правоволодільця.

Зважаючи на такі можливі обставини, деякі країни затвердили спеціальні правила підписання договору франчайзингу, що забов'язують оприлюднення франшизіаром відомостей, на основі яких франшизіат буде мати уявлення про важливі умови, які мають особливе значення для договору франчайзингу.

Щоб зберегти таємність переданої партнерові інформації, між сторонами можуть і мають бути укладені угоди про конфіденційність.

Ціль угоди про конфіденційність – захист всієї інформації для сторони, що вступає в переговори. Договір про конфіденційність покладає на сторону, що отримує інформацію, обов'язок повідомляти її тільки тим своїм працівникам, яким ця інформація необхідна для роботи (перевірки, випробувань, оцінки, адаптації), заради виконання якої її передають. Своєю чергою, ці працівники повинні зобов'язатися не розголошувати. Якщо за характером переданих відомостей передбачається копіювання інформації, в договір найчастіше вносять зобов'язання позначати всі такі копії відповідним грифом. Рекомендується вносити в договір про конфіденційність недвозначний запис про відсутність прав одержувача інформації на будь-яке її використання, крім обговореного в договорі.

Договір про конфіденційність часто передбачає передання інформації (зокрема й інформації, що міститься в зразках продукції, приладах, базах даних, комп’ютерних програмах) на певний термін, наприклад, на півроку, рік або два. Тоді в ньому передбачається або повернення всіх носіїв інформації первинному власникові, або знищення їх, якщо повернення економічно не виправдане, а також встановлюється, що зобов'язання конфіденційності зберігаються визначений період і після завершення терміну.

Угоду про конфіденційність укладають для того, щоб сторона, яка передала інформацію, могла бути впевнена в тому, що одержувач інформації триматиме її в секреті від інших сторін і використовуватиме тільки для себе й лише для визначених обговорених цілей. У такій угоді сторона, що має цінну інформацію й збирається надати її третій стороні, може бути названа «Сторона, що надає інформацію», а та, що одержала інформацію, відповідно, «Одержувач». Обоє, «Сторона, що надає інформацію» та «Одержувач», можуть бути окремими особистостями або організаціями.

Отже, можлива форма угоди про конфіденційність зводиться до такого. «Одержувач» погоджується поводитись з інформацією як з конфіденційною і не розголошувати її іншій особі або організації. Первинна інформація, що має бути розкрита, звичайно зазначається в описі, який формують сторони угоди. Однак якщо в перебігу обговорення або візитів «Одержувач» отримує більше інформації, ніж це розкрито в переданих йому первинних документах, то він зобов'язаний поводитися з цією інформацією так само, як з конфіденційною.

Використання інформації «Одержувачем» звичайно визначається в загальних умовах (часто коротких) в описі, що є частиною угоди. Ці умови можуть відноситися до використання інформації для того, щоб провести тести та випробовування, виконати оплачені роботи, використовувати її для технічного розвитку тощо.

До цієї умови можна долучити кілька вимог, що визначають, як «Одержувач» повинен контролювати за отриманням інформації, а саме:

– тримати інформацію окремо від інших досьє компанії «Одержувача»;

– обмежити копіювання тільки копіями, необхідними для погодженого використання цього матеріалу;

– повертати ці матеріали за вимогою «Сторони, що надає інформацію».

Перший пункт будь-якої угоди про конфіденційність має містити короткий, але чіткий опис переданої інформації.

Має бути вміщене ґрунтовне означення, що саме варто вважати конфіденційною інформацією: *«У цій угоді під конфіденційною інформацією розуміється будь-які відомості або дані конфіденційного характеру, що містять інформацію технічного характеру, відомості про розробку, маркетинг, продажі, експлуатацію, технічні характеристики, вартість, ноу-хау, про саме підприємство та технологічний процес, наявності програмного забезпечення всіх видів носіїв, що містять або розкривають подібну інформацію, методи, що стають доступними відповідно до цієї угоди».*

Зробивши посилання на означення конфіденційної інформації в наступних пунктах, можна з їх допомогою дістати необхідний захист, не зважаючи на характер інформації, що розкривається. В подальшому можлива процедура передачі інформації. Бачиться також корисним здійснити чітке розмежування між конфіденційною та не конфіденційною інформаціями:

За цим має слідувати зобов'язання власника інформації забезпечити партнерові доступ до неї, а також зобов'язання одержувача інформації використовувати її з обмеженою метою.

До угоди про конфіденційність додатково слід внести статтю про повернення всієї переданої інформації. У ній можна зазначити два моменти: повернення всієї інформації за вимогою її власника та зобов'язання, що вся інформація буде повернута власникові у випадку, якщо переговори призведуть до негативного результату.

Зобов'язання, що містяться в угоді про збереження конфіденційності, залишаються чинними протягом наступних 5 років після завершення терміну дії цієї угоди.

Ці пункти можна використовувати як зразок під час складання угоди про конфіденційність. Але така угода ніколи не замінить двох складових елементів, на яких мають ґрунтуватися будь-які переговори: 1) довіра один до одного між усіма залученими сторонами; 2) розумна передбачливість власника інформації.

При проведенні переговорів про передання комерційної інформації, яка є не запатентованою і зберігається в таємниці (те, що називають ноу-хау), партнери поводяться надто обережно. Власник ноу-хау, природно, побоюється розкривати його до укладання договору. Зі свого боку, покупець може не бути впевненим у повній готовності об'єкта угоди. У низці випадків йому для ухвалення остаточного рішення про укладання договору потрібна перевірка можливості реалізації й ефективності ноу-хау в себе на виробництві або, наприклад, у спеціальних

кліматичних умовах. Іноді зацікавленому покупцеві, для того щоб визначитися, бракує технічної інформації, а продавець зводить її в ранг ноу-хау.

Щоб розв'язати цю проблему, партнери укладають опціонний договір на ноу-хау з такими суттєвими умовами:

– Продавець передає покупцеві технічну документацію або інший обговорений матеріал, що будь-яким чином розкриває ноу-хау.

– Покупець дістає право протягом обговореного терміну зробити дослідну перевірку технології за ноу-хау на своєму підприємстві.

– Покупець зобов'язується (протягом кількох років або безстроково) дотримувати конфіденційність стосовно ноу-хау.

– Покупець зобов'язується після закінчення терміну дії опціонного договору не використовувати ноу-хау без висновку основного договору про передання ноу-хау.

– Продавець, якщо покупець після дослідної перевірки побажає, гарантує укладання договору про передання ноу-хау.

– Продавець повинен гарантувати, що до закінчення терміну опціонного договору не пропонуватиме ноу-хау третім особам.

За змогу ознайомитись з ноу-хау, за ризик, пов'язаний з його розкриттям, а також за тимчасове, на термін договору, припинення дій продавця з реалізації ноу-хау покупець виплачує продавцеві визначену опціонним договором суму винагороди. За окрему винагороду продавець може поставити покупцеві зразок продукції, що виготовляється з використанням ноу-хау (установку, прилад тощо).

Отже, покупець дістає змогу оцінити економічну доцільність придбання ноу-хау. Якщо протягом передбаченого опціонним договором терміну між сторонами буде укладено основний договір про передання ноу-хау, то сума, сплачена за опціонним договором, може бути зарахована в рахунок винагороди. Сума, сплачена за опціонним договором, поверненню не підлягає, якщо основний договір про передання прав не буде укладено.

Важливою умовою опціонного договору є зобов'язання покупця використовувати технічну документацію та будь-яку інформацію, отриману від продавця, тільки для цілей дослідної перевірки можливості використання ноу-хау, а також зберігати конфіденційність, починаючи необхідні заходи, зокрема й обмежуючи відповідними зобов'язаннями свій персонал. При порушенні цього зобов'язання, що стало наслідком розкриття ноу-хау, покупець відшкодовує продавцеві зазнані збитки. Не менш важливими умовами є гарантії продавця тимчасово не пропонувати ноу-хау нікому іншому, а також укладати договір про передання ноу-хау, якщо покупець після дослідної перевірки, оцінивши можливість та економічну доцільність використання ноу-хау на своєму підприємстві, прийме рішення про придбання.

Якщо економічна доцільність укладання договору про передачу ноу-хау не буде встановлена, то покупець поверне продавцеві технічну документацію, а також інформацію, на підставі якої приймалося рішення.

Очевидно, що обидві сторони дістають вигоди від подібного договору. Зокрема, продавець має змогу частково відшкодувати витрати з проведення НДДКР за рахунок винагороди. Як правило, ціна опціонного договору становить 20-30% від вартості передбачуваної майбутньої угоди й не повертається покупцеві в разі його відмови від ліцензійного договору. Інформація, на підставі якої покупець приймав рішення про недоцільність придбання ноу-хау, допомагає

продавцеві доробити, поліпшити свою розробку.

Покупець також знаходить переваги. На більш пільгових умовах, ніж придбання ноу-хау, він дістає право оцінити власні можливості щодо впровадження новації. При цьому він одержує зразки продукції, яку може випускати в майбутньому, і необхідну технічну допомогу продавця. Це гарна підмога для вивчення ринку майбутнього товару. Така форма угоди, як опціонний договір, є зручною й вигідною для обох сторін.

3. Перед укладанням угод з іноземною фірмою доцільно, із залученням юристів-міжнародників, досконало вивчити національне законодавство країни, з представником якої передбачається укласти угоду.

В угоді з іноземною фірмою доцільно передбачити:

– зобов'язання сторін вживати всі необхідні заходи для запобігання розголошенню комерційної таємниці;

– документи або дослідні зразки виробів повинні розглядатись сторонами як суворо конфіденційні;

зобов'язання сторін вживати необхідні заходи для запобігання порушення прав користування цими документами або дослідними зразками виробів;

– зобов'язання сторін не передавати без попередньої згоди іншої сторони оригіналів документів або дослідних зразків виробів, або їх копій третім особам;

– зобов'язання сторін забезпечити ознайомлення з комерційною таємницею предмета та умов угоди лише суворо обмеженого кола своїх співробітників.

Практика свідчить, що при укладанні угод з іноземною фірмою не завжди застосовується термінологія, прийнята міжнародними правилами. З цієї причини між партнерами виникають конфліктні ситуації, які викликані тим, що одна із сторін по-своєму (нерідко навмисно) розуміла договірно-правові терміни та їх значення. Ці обставини призводять до невиконання або неналежного виконання договірних зобов'язань.

У зв'язку з цим при укладенні зовнішньоекономічних угод необхідно керуватись положеннями "Міжнародних правил інтерпретації комерційних термінів" (Правила "Інкотермс"). Ці Правила дають вичерпний перелік не лише обов'язкових, а й факультативних умов угоди та регулюють весь комплекс взаємопов'язаних операцій щодо їх виконання.

Певною мірою підвищити надійність та ефективність угод, їх правовий захист допоможе письмова угода сторін про збереження в таємниці певної інформації. Підписання аналогічних угод виправдане і у випадках, коли діловий партнер висловлює побажання про надання йому всієї конфіденційної інформації для оцінки реального стану контрагента з метою прийняття рішення про укладення угоди. Однак до задоволення таких бажань слід ставитись дуже обережно.

Угода необхідна також на той випадок, коли в діловій бесіді один з партнерів повідомив іншому конфіденційні відомості, після чого останній, отримавши необхідну інформацію, відмовляється від укладення угоди, мотивуючи це різними обставинами, в тому числі і тим, що повідомлені конфіденційні відомості йому нібито були вже відомі.

Перевірка ділових партнерів. Обережність у виборі партнерів, перевірка та переперевірка відомостей про них, особливо у випадках, коли викликає сумніви щирість пропозицій, що надійшли, та намірів, є обов'язковими елементами сучасної ділової практики.

На заході вже багато десятиріч функціонує галузь інформаційного бізнесу. Цим бізнесом займаються спеціальні фірми. Надання ними послуг інформаційного характеру про партнера, який цікавить, коштує в межах 500-2000 $ за видачу бізнес-довідки.

Крім того, відомості про виробничу, науково-дослідну, фінансову, збутову та іншу діяльність фірм містяться в каталогах, рекламних проспектах, періодичних бюлетенях, прейскурантах, різноманітних довідкових виданнях, що видаються приватними спеціалізованими виданнями, спілками підприємців та торговельними палатами.

В Україні платні послуги, пов'язані з отриманням інформації про суб'єктів підприємницької діяльності України та зарубіжних країн, надають: Торговельно-промислова палата України;Українська федерація працівників недержавних служб безпеки (підрозділ "Інфоцентр"); Міжбанківська служба безпеки "СКИФ"; Фірма "Сакура", яка надає інформацію про надійність та платоспроможність українських і зарубіжних партнерів, дає гарантії виконання партнерами умов комерційних угод.

Навести довідки про іноземного партнера можна у торговельного аташе посольства відповідної країни.

Перевірку партнера можна здійснити, використовуючи можливості самого підприємства (власна служба безпеки). Можна довідатись про адресу партнера, тривалість роботи на ринку, показники виробництва, балансові показники тощо.

Ще одним шляхам одержання інформації про ділового партнера є систематичне відслідковування і аналіз періодичних видань, таких як "Бізнес", "Галицькі контракти", "Діловий вісник", "Закон і бізнес" тощо. Доцільно на підприємстві вести картотеку на наявних та потенційних ділових партнерів, конкурентів на основі певного переліку необхідних відомостей (анкети) (зразок анкети додається).

4. Наради і ділові переговори, в процесі яких можуть обговорюватися відомості, що складають таємницю фірми або її партнерів, іменуються зазвичай конфіденційними. Порядок проведення подібних нарад і переговорів регламентується спеціальними вимогами, що забезпечують безпеку конфіденційной інформації, яка в процесі цих заходів розповсюджується в санкціонованому (дозволеному) режимі.

Причини, по яких інформація може розголошуватися на конфіденційних нарадах або переговорах, загальновідомі: слабке знання співробітниками складу цінної інформації і вимог по її захисту, умисне невиконання цих вимог, помилки співробітників, відсутність контролю за виданням рекламної і рекламно-виставкової продукції та ін. Оголошення цінній інформації в санкціонованому режимі повинне бути виправдане діловою необхідністю і доцільністю для конкретних умов і характеру обговорюваних питань.

Дозвіл на проведення конфіденційних нарад і ділових переговорів із запрошенням представників інших організацій і фірм повинен давати виключно, перший керівник фірми.

Планові і непланові конфіденційні наради, що проходять без запрошення сторонніх осіб, проводяться першим керівником, його заступниками, відповідальними виконавцями (керівниками, головними фахівцями) по напрямах роботи.

Доступ співробітників фірми на будь-які конфіденційні наради повинен здійснюватися на основі дозвільної системи доступу персоналу, що діє у фірмі, до конфіденційної формації. Запрошення на такі наради осіб, що не є співробітниками фірми, санкціонуються тільки у разі крайньої необхідності їх особистої участі в обговоренні конкретного питання. Присутність їх при обговоренні інших питань повинно бути виключено.

Відповідальність за забезпечення захисту цінної інформації і збереження таємниці фірми в ході наради несе керівник, організуючий дану нараду. Служба безпеці здійснює контроль за перекриттям можливих каналів втрати інформації (включаючи технічні).

В процесі підготовки конфіденційної наради складаються програма його проведення, порядок денний, інформаційні матеріали, проекти рішень і список учасників з кожного питання порядку денного. Всі документи, що складаються в процесі підготовки конфіденційної наради, повинні мати гриф, що свідчить про рівень їх конфіденційності, виготовлятися і видаватися відповідно до вимог інструкції по обробці і зберіганню конфіденційних документів.

Документи (зокрема проекти договорів, контрактів і ін.), призначені для роздачі учасникам наради, повинні містити мінімум конфіденційних відомостей. Цифрові значення найбільш цінної інформації (технічні і технологічні параметри, суми, відсотки, терміни, об'єми і тому подібне) в проектах рішень і інших документах не указуються або фіксуються як загальноприйняте значення, що характерне для операцій подібного роду і є стартовою величиною при обговоренні.

Список учасників конфіденційної наради складається окремо з кожного обговорюваного питання. До участі в обговоренні питання притягуються тільки ті співробітники фірми, які мають безпосереднє відношення до цього питання. Це правило стосується і керівників.

Документом, підтверджуючим повноваження представника сторонньої організації (якщо це не перший керівник) при веденні переговорів і ухваленні рішень з конкретного питання, може служити лист, розпорядження, довіреність фірми, що представляється особою, рекомендаційний лист авторитетної юридичної або фізичної особи, письмова відповідь фірми на запит про повноваження представника, в окремих випадках телефонне або факсимільне підтвердження повноважень першим керівником фірми, що представляється.

Служба безпеки і відповідальний організатор визначають місце проведення наради, порядок доступу учасників наради в це приміщення, порядок документування ходу обговорення питань і ухвалюваних рішень, а також порядок розсипки (передачі) учасникам наради оформлених рішень і підписаних документів.

Будь-яка конфіденційна нарада організовується в спеціальному (виділеному) приміщенні, обладнаному засобами технічного захисту інформації. Доступ в такі приміщення співробітників фірми і представників інших фірм і організацій вирішується керівником служби безпеки.

Перед початком конфіденційної наради співробітник служби безпеки зобов'язаний переконатися у відсутності в приміщенні несанкціоновано встановлених аудіо- і відеозаписуючих пристроїв і в якісній роботі засобів технічного захисту на всіх можливих каналах просочування інформації.

У приміщенні для проведення конфіденційних нарад не повинні знаходитися прилади, устаткування і технічні засоби, які безпосередньо не використуються для

забезпечення ходу наради (наприклад, телефон міської мережі, ПЕВМ, телевізійні і радіоприймачі і ін.) .При необхідності вони розміщуються в сусідній, ізольованій кімнаті. Аудіо- і відеозапис конфіденційних нарад, фотографування ведуться тільки по письмовій вказівці першого керівника фірми і здійснюються одним із співробітників фірми, що готували нараду.

Доступ учасників конфіденційної наради в приміщенні, в якому воно буде проводиться, здійснює відповідальний організатор наради під контролем співробітника служби безпеки відповідно до затвердженого списку її учасників. Перед початком обговорення кожного питання склад присутніх коректується.

Протокол (стенограма), що складається, повинен мати гриф конфіденційності необхідного рівня і оформлятися в стенографічному зошиті, зареєстрованому в секретаріаті.

Доцільність запису учасниками ходу наради визначає керівник, що організував нараду, виходячи із змісту інформації, яка оприлюднилася.

Учасникам конфіденційної наради, незалежно від посади і статусу на нараді, забороняється:

- вносити до приміщення, в якому проводиться нарада, фото-, кіно- і відеоапаратуру, комп'ютери, магнітофони, плеєри, диктофони, радіоприймачі, радіотелефони і іншу апаратуру, а також користуватися нею;

- робити виписки з документів, використуваних при вирішенні питань на нараді і що мають гриф обмеження доступу, на неврахованих носіях;

- обговорювати питання, винесені на нараду, в місцях загального користування;

- інформувати про нараду (питаннях порядку денного, складі учасників, часі і місці проведення, ході обговорення питань, змісту рішень і т. п.) будь-яких осіб, не пов'язаних з проведенням даної наради, в тому числі співробітників фірми.

Після закінчення конфіденційної наради співробітник служби безпеки оглядає приміщення, замикає, опечатує і здає під охорону.

Документи, прийняті на нараді, оформляються, підписуються, при необхідності розмножуються і розсилаються (передаються) учасникам наради відповідно до вимог по роботі з конфіденційними документами фірми. Всі екземпляри цих документів повинні мати гриф обмеження доступу.

При веденні переговорів не слід відразу ж передавати партнерові всю запрошувану ним інформацію в повному об'ємі. Перш за все слід з'ясувати, з якою метою йому необхідні ці відомості і як знання цих відомостей відіб'ється на ході подальшої співпраці з ним. Проте після юридичного оформлення взаємин і підписання партнерами, клієнтами зобов'язання про не розголошування цінних відомостей вони можуть бути детальніше ознайомлені з предметом договору. У договорі за підсумками переговорів повинно знайти віддзеркалення взаємне зобов'язання сторін про захист цінних і особливо конфіденційних відомостей, неприпустимості передачі їх без попередньої згоди сторін третій особі, необхідності ознайомлення з предметом договору обмеженого числа співробітників, які заздалегідь повинні під писати зобов'язання про збереження в таємниці отриманих відомостей.

У комерційній практиці місцем проведення переговорів часто стають торгові або торговельно-промислові виставки, що постійно діють і періодичні, і ярмарки.

Будь-яка виставка с, з одного боку, відмінним джерелом корисної для бізнесу інформації, об'єктом добросовісного маркетингового дослідження ринків

товарів, а з іншої - небезпечним каналом несанкціонованого отримання конфіденційних відомостей, що стосуються нових ідей, технологій і продукції.

Узагальнено джерела цінних відомостей в процесі виставкової діяльності включають: експозицію, персонал фірми, що бере участь у виставці, і рекламний - виставкові матеріали. Втрата цінної інформації відбувається в результаті спілкування фахівців споріднених професій, але різних фірм і наявності у виставковій експозиції найновішого продукту.

Прес-конференції, семінари, презентації фірм і товарів, що проводяться паралельно з виставковими заходами, створюють додаткову загрозу збереженню цінної інформації.

Робота персоналу фірми з відвідувачами виставки повинна бути строго регламентована, перш за все в частині складу оголошених відомостей про продукцію, технічних і технологічних нововведеннях, вкладених в дану продукції. Обов'язково враховується, що склад цих відомостей диференціюється залежно від категорії відвідувачів – масового відвідувача дилетанта ("любителя») і відвідувача - фахівця в даній області («експерта»). Доцільно використовувати метод «чорного ящика», при якому відвідувачеві повідомляється все, що стосується призначення продукції і її споживчих якостей, але залишаються в таємниці технологія, способи, якими досягнуті ці якості, функціональні можливості продукції.

Тому персоналу, обслуговуючому експозицію фірми, повинні бути недоступні відомості про продукцію, віднесені до виробничої або комерційної таємниці. У свою чергу, фахівці фірми, обізнані її секретах, не повинні брати участь в роботі виставкового стенду. Пояснюється це тим, що фахівець в процесі дискусії з відвідувачем може захопитися і повідомити більший об'єм відомостей, чим передбачено. Не допускається знайомити відвідувачів, клієнтів і партнерів з винахідниками, конструкторами, технологами, що працюють над новими ідеями і новою продукцією.

Рекламно-виставкові матеріали (проспекти, прес-релізи, прайс-листи, брошури і тому подібне) слід розглядати як контрольований канал розповсюдження цінних відомостей. При цьому слід пам'ятати, що цей канал ретельно і глибоко аналізується конкурентом з метою виявлення тих відомостей, які складають таємницю фірми, що видала рекламні матеріали.

Захист інформації в рекламно-виставковій діяльності передбачає завчасний аналіз, експертизу призначеною для широкого оголошення будь-якій інформації про діяльність фірми і її продукції в цілях виявлення в змісту або елементах відображення (таблицях, формулах, малюнках, фотографіях, схемах) конфіденційних відомостей. Матеріали, що не пройшли експертизу, публікувати забороняється.

Разом з тим повинен дотримуватися розумний баланс: рекламно-виставкові матеріали не повинні бути мало інформативними для відвідувачів, всі найбільш важливі параметри нової продукції повинні знайти в них віддзеркалення.

Тема 9. Види і процедури юридичної відповідальності за розголошення державної таємниці

Загальні підстави застосування юридичної відповідальності за розголошення державної таємниці. Кримінальна відповідальність за розголошення державної таємниці. Втрата документів, що містять державну таємницю.

Адміністративна відповідальність за порушення режиму державної таємниці. Відповідальність за розголошення державної таємниці у нормах законодавства зарубіжних країн.

1. 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;

невжитті заходів щодо забезпечення охорони державної таємниці та незабезпеченні контролю за охороною державної таємниці;

провадженні діяльності, пов'язаної з державною таємницею, без одержання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщенні державних замовлень на виконання робіт, доведенні мобілізаційних завдань, пов'язаних з державною таємницею, в державних органах, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

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

невиконанні норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї інформації або просочення її технічними каналами, -

– несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно із законом «Про державну таємницю».

2. Розглядаючи питання кримінальної відповідальності за розголошення державної таємниці, необхідно зупинитися на чіткому визначенні усіх конститутивних ознак складу злочину, передбаченого ст. 328 Кримінального кодексу України. По-перше, суспільна небезпечність будь-якого злочину полягає в

суттєвій шкоді, яка завдається цим злочином об'єкту кримінально-правової охорони, або у небезпеці завдання такої шкоди. Суспільна небезпечність розголошення державної таємниці досить висока. Практично кожний факт порушення встановлених правил поводження з державною таємницею становить джерело небезпеки. Як указується 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 тяжких наслідків з великими матеріальними або моральними збитками: дипломатичних ускладнень, науково-технічних і технологічних втрат, загроз життю й волі осіб, які співробітничають із правоохоронними органами тощо.

Разом з у Кримінальному кодексі України кримінально-правова норма, що передбачає відповідальність за розголошення державної таємниці, розміщена не в розділі "Злочини проти основ національної безпеки", а в розділі "Злочини у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації". Тим самим, законодавець дещо применшує значення, що має для національної безпеки схоронність державної таємниці, та об'єднує окремі склади злочинів за старою кримінально-правовою традицією як такі, що посягають на "обороноздатність держави".

Однією з головних ознак складу злочину, передбаченого ст. 328 КК, є предмет даного злочину – інформація, що становить державну таємницю. Таким чином, у визначенні державної таємниці мають місце наступні 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. Даний 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.

З об'єктивної сторони складу розголошення державної таємниці вирішальне значення має перш за все поняття "розголошення ". Кримінальне законодавство України не визначає цього поняття й способів вчинення даного злочину.

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 невжиття належних заходів 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 статті 328 КК України поняття "стороння особа" відсутнє. Втім дана дефініція набуває значення конститутивної ознаки складу розголошення державної таємниці.

Сторонньою особою визнається будь-яка фізична особа, яка не належить до кола тих, кому державна таємниця довірена або стала відома у зв'язку з виконанням службових обов'язків і якій винний не мав права довіряти відомості, що становлять державну таємницю. До таких осіб належать усі громадяни, що не мають допуску до даного роду відомостей, а також ті, кому й за наявності загального допуску дані відомості не були доступні по службі чи роботі. Таким чином, критерієм визначення сторонньої особи необхідно визнати доступ до державної таємниці. Тому під сторонньою особою необхідно розуміти таку особу, яка виконуючи покладені на неї обов'язки, відповідно до її службових повноважень не має доступу до секретної інформації, що розголошується.

Кримінальна відповідальність настає незалежно від того, скільком стороннім особам стали відомі відомості, що становлять державну таємницю. Ця обставина може враховуватися судом при вирішенні питання про призначення винному конкретної міри покарання.

Оскільки адресат розголошення є обов'язковою ознакою діяння, автор пропонує в диспозицію статті 328 КК України включити поняття "стороння особа", котра є реальним учасником процесу розголошення та визначає суть діяння. Чим точніше виражені сутнісні ознаки в кримінально-правовій нормі, тим менша кількість помилок може бути зроблена при кваліфікації вчиненого.

Не менш важливо визначити також зміст поняття "сприйняття", від якого досить часто залежить, чи буде діяння особи містити склад закінченого злочину, передбаченого ч. 1 ст. 328 нового КК України. Сприйняття як одна з форм пізнання є відображення у свідомості людини предмета чи явища в цілому в сукупності його властивостей при їх безпосередньому впливі на органи почуттів людини. Разом з тим у сприйнятті завжди проявляються особливості особистості сприймаючого суб'єкта, тобто в його свідомості інформація, що розголошується, може відбитися лише частково або трансформуватися, спотворитися. Якщо особа усвідомила зміст відомостей, що були їй розголошені, та може їх відтворити в обсязі, який свідчить про перехід державної таємниці у власність такої особи, то це закінчений склад злочину. Якщо ж стороння особа нічого не запам'ятала або ж володіє розголошеною інформацією в такому обсязі, який свідчить про необізнаність даної особи з державною таємницею, то умисне діяння суб'єкта необхідно кваліфікувати як закінчений замах на розголошення державної таємниці за статтями 15 і 328 КК України.

Таким чином, розголошення державної таємниці, передбачене ч. 1 ст. 328 нового КК, слід вважати закінченим з моменту, коли відомості, що становлять державну таємницю, були сприйняті сторонньою особою в обсязі, який свідчить про перехід даної інформації у власність такої особи.

Іноді можливі ситуації, коли з причин, які не залежали від волі винного, умисно розголошені їм 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.

При протиправному розголошенні державної таємниці винна особа завжди порушує встановлені правила (порядок) поводження (використання, зберігання, передачі, оголошення тощо) з відомостями, що становлять державну таємницю, які встановлюються Законом України "Про державну таємницю" і відповідними нормативно-правовими актами – інструкціями, наказами тощо. Однак не можна ототожнювати розголошення державної таємниці з порушенням правил поводження з нею. Тільки при порушенні таких правил розголошення фактично немає, а та обставина, що відомості могли бути сприйняті сторонніми особами, є лише можливим наслідком порушення. При розголошенні ж ознайомлення з державною таємницею сторонніх осіб необхідна ознака злочинного діяння.

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: 1) порушення певних вимог нормативних актів, які встановлюють порядок поводження з державною

таємницею, що виявляється в дії або бездіяльності; 2) сприйняття відомостей, що становлять державну таємницю, сторонньою особою; 3) 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.

Розглядаючи питання щодо наявності вини в діях підозрюваного, важливо встановити, чи усвідомлював він, що розголошені ним відомості становлять державну таємницю. Якщо не знав про це і не повинен був за родом службової діяльності знати, то він і не несе відповідальності за це діяння.

При розголошенні суб'єкт усвідомлює, що доводить державну таємницю до сторонньої особи (або що не вживає для запобігання цьому належних заходів), але не усвідомлює й не може усвідомлювати істинний характер адресата у випадку його належності до іноземної держави чи організації і не має наміру ознайомити з такими відомостями іноземну державу, іноземну організацію чи їх представників.

Передаючи державну таємницю іноземній державі, іноземній організації чи їх представникам, суб'єкт державної зради чи шпигунства усвідомлює, що ці відомості будуть використані на шкоду інтересам зовнішньої безпеки України, й бажає цього. При умисному ж розголошенні особа не бажає заподіяння шкоди зовнішній безпеці держави, а в крайньому випадку може лише допускати такі наслідки. У цьому полягає докорінна й принципова відмінність умисного розголошення державної таємниці, передбаченого ст. 328 КК, від випадків розголосу таких відомостей, що утворюють склади державної зради (ст. 111 КК) або шпигунства (ст. 114 КК).

Характеризуючи ознаки суб'єкта розголошення державної таємниці, необхідно зазначити, що кримінальній відповідальності за розголошення державної таємниці за безпосередньою вказівкою закону підлягають тільки такі особи, яким конкретна секретна інформація була довірена або стала відома у зв'язку з виконанням службових обов'язків. Інакше кажучи, йдеться про спеціального суб'єкта злочину.

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. 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 по рядку 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 та кого.

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

1. Об'єкт цього злочину аналогічний об'єктові злочину, передбаченого ст. 328.

2. Предметом злочину є 1) документи, що містять державну таємницю, 2) інші матеріальні носи секретної інформації, що містять державну таємницю, 3) 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 кінота 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 носи інформації, що становить державну таємницю, які не є документами (зразки зброї, військової та спеціальної техніки, обладнання, палива, сировини 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 носи 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 містигь склад злочину, передбаченого ст. 329, лише у випадку якщо воно стосувалось порядку, встановленого законом, а не будь-яким іншим нормативне 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.

Ключовим поняттям в цьому складі злочину є поняття "втрата". Втрата передбачає вихід хоча б одного носія інформації, що містить державну таємницю, або предмета, відомості про який становлять таку таємницю, поза волею особи, якій вони були довірені, із її правомірного володіння - назавжди або на певний час. Злочин слід вважати закінченим з моменту втрати носія інформації (предмета), незалежно від того, чи ознайомились з ним сторонні особи. Проте, якщо в результаті втрати такого носія інформації (предмета) з ним реально не мали можливості ознайомитися сторонні особи (наприклад, якщо втрата предмета була поєднана з його негайним знищенням), склад цього злочину відсутній, адже шкода об'єкту у такому випадку не заподіюється.

У випадках, коли в результаті втрати вказаного носія інформації (предмета) на території режимного об'єкта з ним ознайомились тільки особи, які мали відповідний допуск, це діяння може розглядатися з урахуванням правил ч. 2 ст. 11 як таке, що через малозначність не становить суспільної небезпеки.

Якщо порушення порядку поводження з зазначеними носіями інформації (предметами) не потягло їх втрати, або якщо їх втрата не була результатом порушення вказаного порядку (наприклад, документ викрадено у працівника фельд'єгерського зв'язку під час грабежу чи розбійного нападу), кримінальна відповідальність за ст. 329 виключається.

За відсутності ознак шпигунства передавання сторонній особі вказаного документа (матеріалу, предмета) для ознайомлення з ним кваліфікується за ст. 328 як розголошення державної таємниці.

4. Суб'єктом злочину є особа, яка мала відповідний допуск до документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, а також до предметів, відомості про які становлять державну таємницю. Про поняття такої особи див. коментар до ст. 328.

Військовослужбовці та військовозобов'язані під час проходження ними зборів за втрату документів, матеріалів, що містять державну таємницю у сфері оборони, або предметів, відомості про які становлять державну таємницю у будь-якій сфері, несуть відповідальність за ч. 2 ст. 422, а за втрату документів і матеріалів, що містять державну таємницю в інших сферах, - за ст. 329.

5. Суб'єктивна сторона злочину передбачає тільки необережну вину - злочинну самовпевненість або злочинну недбалість. При цьому ставлення до порушення правил поводження з вказаними документами (предметами) може бути й умисним,

Умисне знищення чи приховування документів, що містять державну таємницю, вчинене з метою помсти особі, якій вони були довірені, має кваліфікуватися за ст. 357,

Для кваліфікації цього злочину має істотне значення, чи сталася втрата вказаних матеріальних носіїв секретної інформації (предметів) внаслідок дій або бездіяльності особи, яка здійснювала володіння ними, чи внаслідок умисних дій інших осіб (скажімо, крадіжки документа підлеглим) або їхньої необережності (необережного викидання прибиральницею документа до сміття тощо). Оскільки кримінальна відповідальність базується на принципі суб'єктивного ставлення у вину, відсутність вини особи виключає притягнення її до кримінальної відповідальності. При цьому вина, як і в інших складах злочинів, розглядається окремо стосовно дій і стосовно наслідків. Так, якщо особа не прибрала таємний документ у сейф у час, коли вона не працює з ним, вона умисно або з необережності порушила порядок поводження з цим документом. Вини ж особи у тому, що документ вкрадено або знищено третьою особою, немає. Адже діяння інших осіб, якщо суб'єкт не перебуває з ними у змові, взагалі знаходяться за межами його психічного ставлення. Наявність вини тільки стосовно порушення зазначеного порядку може потягнути лише дисциплінарну відповідальність особи.

Від розголошення державної таємниці злочин, передбачений ст. 329, відрізняється переважно змістом суб'єктивної та об'єктивної сторони. Крім того, на відміну від розголошення державної таємниці, відповідальність за втрату матеріальних носіїв інформації, що містять державну таємницю, або предметів, відомості про які становлять державну таємницю, несуть тільки особи, яким ці документи (предмети) було довірено.

У багатьох випадках, коли відповідний носій (предмет) втрачено, буває неможливим встановити, де саме і за яких обставин він вийшов із володіння особи, котрій був довірений. Якщо всебічно й об'єктивно перевірено різні версії (документ викрадено колегою, який працює в цьому ж кабінеті, документ знищено замість іншого, документ знищено, але його забули зняти з обліку тощо), але жодна з них не знайшла підтвердження, особа, якій документ було довірено, відповідно до ст. 62 Конституції України не може нести відповідальність за ст. 329. У такому випадку може йтися лише про дисциплінарну відповідальність.

Як службова недбалість за ст. ст. 367 (425) втрата матеріального носія інформації, що містить державну таємницю, або предмета, відомості про який становлять таку таємницю (що є істотною шкодою), може бути кваліфікована, якщо така втрата допущена службовою особою внаслідок невиконання або неналежного виконання нею службових обов'язків через несумлінне ставлення до них.

6. Кваліфікованим видом розглядуваного злочину є втрата матеріального носія інформації, що містить державну таємницю, або предмета, відомості про який становлять таку таємницю, яка спричинила тяжкі наслідки. Про їх поняття див. коментар до ст. 328.

4. Порушення законодавства про державну таємницю, а саме:

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

2) засекречування інформації: про стан довкілля, 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;

3) безпідставне засекречування інформації;

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

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

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

7) провадження діяльності, пов'язаної з державною таємницею, без отримання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщення державних замовлень на виконання робіт, доведення мобілізаційних завдань, пов'язаних з державною таємницею, в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

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

9) невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності,- 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 б 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: 1) оборони; 2) економіки, науки і техніки; 3) зовнішніх відносин; 4) 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.

Об'єктивна сторона правопорушення полягає у порушенні законодавства про державну таємницю, а саме вчиненні діянь зазначених пп. 1-9 ч. 1 статті. 212.2 Кодексу про адміністративні правопорушення.

Суб'єктивна сторона правопорушення характеризується наявністю вини у формі умислу.

Суб'єктами цього правопорушення можуть бути як посадові особи, так і громадяни.

5. 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 по забезпеченості охорони державної таємниці в законодавстві пострадянських держав – Азербайджанської Республіки, Республіки Білорусь, Грузії, Латвійської Республіки, Російської Федерації.

Так, система охорони та захисту таємниць, існуюча у Великобританії, базується на законі про державну таємницю, прийнятому ще в 1911 р. До нього було прийнятий 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, що 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, коли 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» – групу ядерних держав. 4 липня 1960 був прийнятий указ про таємниці, в якому давалася 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, що проголошує 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 розсекречення і розголошенню на будь-яку галузь. У 1978 р парламент Франції прийняв закон, що проголошує 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 розсекречення і розголошенню. 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 г.», «Про атомну енергію 1954 г.», «Про спостереження за іноземною розвідкою 1978 г.», «Про внутрішню безпеку 2002 г.») 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 г. «Про нерозголошення важливої технічної інформації», згідно з якою винуватцю загрожує тюремне ув'язнення або штраф в 1 мільйон доларів США або на суму, в п'ять разів перевищує вартість збитку, нанесеного розголошенням інформації. Проводячи аналогію з українським законодавством, слід зазначити, що ч. 1 ст. 328 КК України передбачає за розголошення державної таємниці можливість призначення 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 (ст. 98: а) необережне надання або створення доступу до секретної інформації; б) кримінальної 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 вітчизняним законодавством: 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 закритою або секретної кореспонденції або документації в сфері національної оборони. Можна зробити висновок, що кримінальний закон Іспанії диференційовано підходить до питання про покарання різних категорій злочинних посягань в залежності 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 з усіх країн підходить до охорони державної таємниці.

На пострадянському просторі склалася наступна ситуація з охороною державної таємниці. У РФ кардинальна перебудова системи захисту охоронюваних державою відомостей почалася з прийняттям в 1993 р Закону РФ «Про державну таємницю», що регламентує відносини, що виникають у зв'язку з віднесенням інформації до державної таємниці, засекречуванням і розсекреченням відомостей і їх захистом в інтересах забезпечення безпеки країни. Правовий режим захисту державної таємниці регламентується приблизно 26 нормативними актами, з яких близько 20 – підзаконні. Відповідно до ст. 2 Закону РФ «Про державну таємницю» державна таємниця – захищені державою відомості в області військової, зовнішньополітичної, економічною, розвідувальної, контр розвідувальної і оперативно-розшукової діяльності, поширення яких може завдати шкоди безпеці РФ. У КК РФ, структура Особливої частини якого відрізняється від структури Особливої частини КК України, в розділі X поміщені злочини проти державної влади, а в главі 29 наведені норми про кримінальну відповідальність за розголошення державної таємниці та втрату документів, що містять державну таємницю.

Подібні положення 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 РФ.

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, як і в КК РФ, 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 наступне.

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
2.	Російська Федерація	Глава 29. Злочини проти основ конституційного ладу та безпеки держави, ст. 283. 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 одинадцятий. 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.	Узбекистан	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
13.	Туркменистан	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 Узбекистана (ст. 162), Республіки Таджикистан (ст. 311), Російської

Федерації (ст. 283), Республіки Вірменія (ст. 306), Киргизької Республіки (ст. 300), Туркменистану (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 [38]), 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.

Тема 10. Відповідальність за порушення законодавства про комерційну таємницю

Застосування норм господарського та цивільного законодавства за порушення прав на комерційну таємницю. Застосування дисциплінарної і матеріальної відповідальності, передбаченої трудовим законодавством за порушення права суб'єкта господарювання на комерційну таємницю. Адміністративна відповідальність за розголошення комерційної таємниці. Кримінальна відповідальність за порушення законодавства про комерційну таємницю. Застосування норм господарського законодавства за неправомірне збирання, розголошення або використання відомостей, що є комерційною таємницею.

1. Захист порушених суб'єктивних прав на комерційну таємницю може здійснюватися в двох формах: юрисдикційній і неюрисдикційній. Під формою захисту розуміється комплекс внутрішньо узгоджених організаційних заходів щодо захисту суб'єктивних прав і охоронюваних законом інтересів.

Юрисдикційна форма захисту є діяльність уповноважених державних органів щодо захисту порушених прав або оспорюваних суб'єктивних прав. Суть даної форми виражається в тому, що суб'єкт господарювання, чиє право на комерційну таємницю порушено, звертається за захистом до державних або інших

компетентних органів.

Юрисдикційна форма захисту права на комерційну таємницю здійснюється як в судовому, так і в адміністративному порядку.

Судовий порядок захисту передбачає звернення з позовом про захист порушеного права до суду. Оскільки основними користувачами права на комерційну таємницю виступають суб'єкти господарювання, то дані позови в більшості випадків відносяться до підвідомчості господарських судів.

Справи у спорах про порушення майнових прав інтелектуальної власності розглядаються господарським судом за місцем вчинення порушення. Виняток становлять випадки, коли в якості відповідача виступає працівник, що розголосив комерційну таємницю всупереч трудовому договору, або ж фізична особа (не суб'єкт підприємницької діяльності), що розголосила комерційну таємницю всупереч цивільно-правовому договору, а також якщо особа притягується до кримінально-правової (ст. 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю», ст.232 «Розголошення комерційної таємниці» КК) або адміністративно-правової відповідальності передбачену положеннями про недобросовісну конкуренцію. В даному випадку справа підлягає розгляду в суді загальної юрисдикції. У порядку цивільного судочинства позови можуть подаватися до суду загальної юрисдикції за місцем знаходження позивача .

Згідно ч.2 ст.155 ГК України на комерційну таємницю, як на об’єкт права інтелектуальної власності розповсюджуються загальні умови захисту прав інтелектуальної власності, визначені в ЦК України. Ст. 432 ЦК України закріплює специфічні, прийнятні лише щодо об’єктів права інтелектуальної власності способи захисту, що реалізуються в судовому порядку, так: як: застосування негайних заходів з попередження порушення права інтелектуальної власності та збереження відповідних доказів; зупинення пропуску через митний кордон України товарів, імпорт або експорт яких здійснюється з порушенням права інтелектуальної власності; вилучення з цивільного обороту товарів, виготовлених або введених у цивільний обіг з порушенням права інтелектуальної власності; вилучення з цивільного обороту матеріалів і знарядь, використаних переважно для виготовлення товарів з порушенням права інтелектуальної власності; застосування разового грошового стягнення замість відшкодування збитків за неправомірне використання об’єкта права інтелектуальної власності; опублікування в засобах масової інформації відомостей про порушення права інтелектуальної власності та зміст судового рішення щодо такого порушення. Крім зазначених способів захисту ст.16 ЦК України закріплює можливість визнання угоди недійсною, відшкодування моральної (немайнової) шкоди.

Згідно ст. 20 ГК України основними способами захисту права на комерційну таємницю (у числі прав суб’єктів господарювання) є: визнання права на комерційну таємницю; відновлення становища, що існувало до порушення права, і припинення дій, що порушують право або створюють загрозу його порушення; визнання недійсним повністю або частково акта державного або іншого органу, що суперечить законодавству і порушує право банка як суб’єкта господарювання на комерційну таємницю; відшкодування збитків, завданих порушенням права банка на комерційну таємницю; застосування відповідних штрафних, оперативно-господарських та адміністративно-господарських санкцій.

Серед вище зазначених законодавчо закріплених способів захисту прав на

комерційну таємницю найчастіше застосованими є наступні.

1. Визнання права на комерційну таємницю. Такий спосіб може бути використаний суб'єктом господарювання, коли право оспорюється будь-ким, коли третя особа вимагає від суб'єкта господарювання без встановлених законом підстав розкрити інформацію, що становить комерційну таємницю. Прикладом застосування такої норми може послужити ситуація, за якої працівник створивши об'єкт права інтелектуальної власності (винахід або корисну модель у зв'язку з виконанням службових обов'язків чи дорученням роботодавця за умови, що трудовим договором (контрактом) не передбачене інше), робить спробу подачі заявки на видачу патенту, або хоче іншим чином розкрити сутність досягнутого їм результату, незважаючи на рішення роботодавця зберігати останній у режимі «комерційна таємниця». При виникненні такої ситуації роботодавець може захистити свої інтереси шляхом подачі позову в суд загальної юрисдикції про визнання права на комерційну таємницю.

2. Відновлення становища, яке існувало до порушення права, і припинення дій, що порушують право або створюють загрозу його порушення. Такий спосіб є застосованим у випадку, коли відомості, що становлять комерційну таємницю, були отримані третьою особою у незаконний спосіб, але вона або не мала ще можливість з ними ознайомитися, або в разі, коли відомості були придбані незаконним способом з метою їх подальшої передачі і передача таких відомостей особі, зацікавленій в їх отриманні, ще не відбулася. Повинно мати місце можливість ліквідації наслідків порушення. Наприклад, на особу, яка заволоділа інформацією за допомогою незаконних способів може бути покладено обов'язок щодо повернення незаконно отриманої документації або знищення матеріальних носіїв інформації, та заборону на використання придбаної незаконним способом інформації, що становить комерційну таємницю, для особистих цілей.

3. Виконання обов'язку в натурі є застосованим у разі, коли особа отримала відомості, що становлять комерційну таємницю за договором, який передбачає обов'язок по виплаті винагороди власнику права на комерційну таємницю, і не здійснила своєчасно такої виплати. Суд може за позовом потерпілої сторони винести рішення про присудження до виконання обов'язку в натурі.

4. В рамках судової форми захисту можливо також застосування таких заходів як відшкодування збитків, штрафних санкцій. У той же час, слід зазначити, що суб'єкт господарювання, чиє право порушено, не повинен збагачуватися за рахунок особи, яка порушила право на комерційну таємницю. Він має законне право відновити своє становище, а при неможливості відновлення – компенсувати свої втрати. Компенсація за своїм характером є мірою відповідальності, однак вона не повинна застосовуватися як додаткове обтяження разом з відшкодуванням збитків. Компенсація не повинна замінювати відшкодування збитків, а повинна застосовуватися виключно в особливих випадках, коли у суду немає сумніву в наявності у потерпілого збитків, однак, визначення їх точного розміру є неможливим. Що стосується розміру компенсації, то встановлення чітких грошових кордонів не представляється, а тому, слід виходити із загальних засад, закріплених в ст. 432 ЦК України: розмір грошового стягнення визначається відповідно до закону з урахуванням вини особи та інших обставин, що мають істотне значення.

5. Ще одним дієвим способом захисту. що має місце у міжнародній практиці є – примусове укладення з суб'єктом господарювання, що порушив право на

комерційну таємницю, договору про передачу ноу-хау, предметом якого буде виступати незаконно отримана комерційна таємниця.

Примусове укладення договору про передачу ноу-хау дозволить суб'єкту господарювання, чиє право на комерційну таємницю порушено, отримати компенсацію у формі платежів за договором, розмір яких буде визначатися виходячи з прибутку, отриманої порушником внаслідок застосування незаконно отриманої комерційної таємниці. Такий спосіб захисту є доцільним, коли комерційна таємниця вже стала відома конкуренту.

2. Неюрисдикційна форма захисту охоплює собою дії суб'єкта господарювання щодо захисту його права на комерційну таємницю, які вчиняються ним самостійно, без звернення за допомогою до державних або інших компетентних органів.

У ЦК України право на використання даної форми закріплено в ст.19. Особа має право на самозахист свого цивільного права та права іншої особи від порушень і протиправних посягань. Кодексом встановлено певні обмеження при використанні даного права. Засоби протидії повинні бути не заборонені законом і не суперечити моральним засадам суспільства. Способи захисту повинні відповідати змісту порушеного права, характеру дій, якими воно порушене, а також наслідкам, заподіяних цим порушенням. По суті, це право зводиться до виведення з ладу технічних засобів, незаконно введених третіми особами з метою отримання інформації, дезінформації осіб, які незаконно отримали засекречені відомості, з метою нейтралізації події, а також до застосування оперативно-господарських санкцій.

В межах неюрисдикційної форми захисту може застосовуватися дисциплінарна відповідальність передбачена ст. 147 КЗпП України за порушення трудової дисципліни, що виражається в розголошенні комерційної таємниці шляхом оголошення догани або звільнення.

2. Матеріальна відповідальність може бути покладена незалежно від притягнення працівника до дисциплінарної, адміністративної чи кримінальної відповідальності.

Дисциплінарна відповідальність в теорії права розглядається як різновид юридичної відповідальності та здійснюється у формі накладення адміністрацією підприємств і установ інших організацій дисциплінарних стягнень внаслідок:

а) порушень правил внутрішнього розпорядку;

б) у порядку підлеглості;

в) відповідно до дисциплінарних статутів і положень.

До заходів дисциплінарної відповідальності відносять: зауваження, попередження, догана, переведення на іншу роботу та ін.

Дисциплінарна відповідальність може бути загальною і спеціальною.

Загальна дисциплінарна відповідальність настає на основі норм КЗпП України і правил внутрішнього трудового розпорядку. Вона поширюється на переважну більшість працюючих, включаючи сезонних і тимчасових працівників, на яких не поширюється дія статутів і положень про дисципліну та інших спеціальних положень. Навіть у тих галузях економіки, де діють статути чи положення про дисципліну, значна частина працівників несе загальну дисциплінарну відповідальність.

Спеціальна дисциплінарна відповідальність передбачена тільки для

конкретно визначених категорій працівників на основі статутів та положень про дисципліну і спеціальних нормативних актів. Вона характеризується спеціальним суб'єктом дисциплінарного проступку, особливим характером дисциплінарного проступку, спеціальними видами дисциплінарних стягнень, особливим порядком накладення та оскарження дисциплінарного стягнення.

3. В рамках юрисдикційної форми захисту можна виділити адміністративний порядок захисту права на комерційну таємницю. Даний порядок передбачений Законом України «Про захист від недобросовісної конкуренції» від 7 червня 1996 року. Згідно з нормами Закону володілець права на комерційну таємницю вправі звернутися із заявою про порушення права на комерційну таємницю до відповідного територіального органу АМК (Антимонопольного комітету України), який в свою чергу зобов'язаний розглянути обставини справи і винести обов'язкове для виконання розпорядження про усунення порушення [8].

При вчиненні незаконних дій щодо комерційної таємниці АМК згідно ст. 30 Закону може прийняти рішення про визнання факту недобросовісної конкуренції, припинення недобросовісної конкуренції, накладення штрафу. Зазначені заходи носять характер адміністративно-господарських санкцій (згідно ст.238 Господарського кодексу України).

Для відшкодування збитків, завданих актом недобросовісної конкуренції, суб'єкт господарювання повинен звернутися в суд (ст.24 Закону України «Про захист від недобросовісної конкуренції»).

Рішення АМК і його територіальних відділень, прийняті у справах про недобросовісну конкуренцію можуть бути оскаржені до суду (ст.32 Закону України «Про захист від недобросовісної конкуренції»).

Ст. 16-19 ЗУ «Про захист від недобросовісної конкуренції» та ч. 2 ст. 36 ГК України одним із видів правопорушень, що визнаються недобросовісною конкуренцією, є: 1) неправомірне збирання комерційної таємниці, яке являє собою добування протиправним способом зазначених відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання; 2) розголошення комерційної таємниці, тобто ознайомлення іншої особи без згоди особи, уповноваженої на те, з відомостями, що відповідно до закону становлять комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання; 3) схилення (схиляння) до розголошення комерційної таємниці, а саме спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків відомості, що відповідно до закону становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання; 4) неправомірне використання комерційної таємниці, тобто впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи неправомірно здобутих відомостей, що становлять відповідно до закону комерційну таємницю.

4. Кримінальна відповідальність тягне за собою накладення штрафів та позбавлення права обіймати певні посади обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання; 3) схилення (схиляння) до розголошення комерційної таємниці, а саме спонукання особи, якій були довірені у

встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків відомості, що відповідно до закону становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання; 4) неправомірне використання комерційної таємниці, тобто впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи неправомірно здобутих відомостей, що становлять відповідно до закону комерційну таємницю, чи займатися певною діяльністю на строк до трьох років.

Ст. 231 КК України – за умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого їх використання, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду банку.

Ст. 232 КК України – за умисне розголошення комерційної таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди банку [19].

З аналізу норм кримінального законодавства можна виділити три групи злочинних посягань на відомості, що становлять комерційну таємницю 1) незаконне збирання відомостей, що становлять комерційну; 2) незаконне використання таких відомостей; 3) умисне розголошення такої інформації.

Незаконне збирання відомостей може виявлятися у:

– викраденні відповідної інформації чи об'єктів, що її містять, з приміщень, де вони зберігалися. Така крадіжка може бути як відкритою, так і завуальованою, коли справжні предмети посягання (документи, вироби, що містять комерційну таємницю) викрадаються разом із іншими і в такий спосіб створюється хибне уявлення про дійсні цілі злочинців;

– таємному проникненні злочинця до приміщення й копіювання інформації паперовим чи електронним способом;

– підкупі співробітника підприємства, який мав чи має законний доступ до інформації. Працівник за певні матеріальні чи інші блага копіює інформацію та передає її замовникові. Якщо людина вже звільнилася або на сьогодні не має законного доступу, але інформація, якою вона володіла раніше, ще не втратила комерційної привабливості, то вона її просто повідомляє;

– підкупі посередників у переговорах, які володіють певною інформацією;

– незаконному отриманні інформації у співробітників правоохоронних або контролюючих органів, яким вона стала відома внаслідок виконання ними службових обов'язків;

– погрозах фізичним насильством над особою чи її близькими родичами, якій інформація була довірена в результаті виконання її трудових обов'язків;

– шантажі працівника, який знаходиться на «гачку» внаслідок певних життєвих обставин;

– впровадженні свого агента в штат підприємства під виглядом звичайного співробітника;

– вербуванні діючого працівника або спонуканні до розголошення звільненого із застосуванням мотивів етнічної, расової, релігійної близькості, бажанням помститися керівникові за незаконне звільнення, переведення на іншу роботу, зняття з посади;

– використанні різних технічних пристроїв, що фіксують і передають

інформацію. За допомогою спеціальної техніки здійснюється прослуховування приміщень або зняття інформації з каналів зв'язку Для цього застосовуються радіозакладки, мікрофони направленої дії, пристрої для зняття інформації з вікон за допомогою лазерних промінів, апаратура для виявлення й розшифровування електромагнітного випромінювання від офісної техніки, мініатюрні фото - та відеокамери. Таку техніку можуть встановлювати або використовувати як спеціально підготовлені особи, так і завербовані співробітники підприємства;

– проникненні в комп'ютерні мережі. Для цього злочинці застосовують спеціальні комп'ютерні програми, які дозволяють відшуковувати необхідні дані та копіювати їх.

Незаконним використанням комерційної таємниці є впровадження у виробництво або врахування під час планування чи здійснення господарської діяльності без дозволу власника чи уповноваженої на те особи таких відомостей. Зокрема, незаконне використання може мати такі форми:

– пред'явлення майнових або інших вимог до власника комерційної таємниці за повернення або нерозголошення відповідних відомостей. Такі вимоги можуть стосуватися повернення на роботу, призначення на вищу посаду, звільнення іншого працівника, надання послуг тощо;

– продаж інформації третім особам;

– обмін інформації, що становить комерційну таємницю, на іншу або матеріальні цінності;

– корегування своїх дій при укладанні договорів з власником такої таємниці.

Розголошення може здійснюватися усно, письмово, із використанням засобів зв'язку й масової інформації, комп'ютерних мереж та ін. Розголошення вчиняють особи, яким ця інформація стала відома внаслідок професійної або службової діяльності. Це можуть бути як працівники самого підприємства, установи, організації, так і співробітники правоохоронних чи контролюючих органів, які отримали цю інформацію, користуючись своїм службовим становищем, але не для виконання своїх функцій, а для передавання конкурентам чи використання в інших протиправних цілях, наприклад, різних видів шантажу щодо здійснення чи нездійснення певних дій за нерозголошення комерційної таємниці.

ГЛОСАРІЙ

Аналіз документопотоків – шлях до вивчення та раціоналізації існуючої системи управління організації.

Безпека – такий стан суб’єкта, при якому ймовірність зміни властивих цьому суб’єкту якостей та параметрів його зовнішнього середовища незначна, менше певного інтервалу.

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

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 державною таємницею і підлягають охороні державою.

Державний експерт з питань таємниць – фізична особа, що здійснює відповідно віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування.

Джерела інформації – носії інформації у вигляді документів та інших матеріальних об'єктів, що зберігають інформацію, а також повідомлення засобів масової інформації, публічні виступи.

Довідково-інформаційний фонд – це сукупність упорядкованих первинних документів і довідково-пошукового апарату, призначених для задоволення інформаційних потреб.

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

Документообіг – це рух службових документів в установі від дати їх створення чи одержання до завершення виконання або надсилання.

Доступ до комерційної таємниці – це письмова санкція власника підприємства або уповноваженої ним особи на ознайомлення або роботу з конкретними відомостями, що складають комерційну таємницю, співробітників підприємства та представників сторонніх організацій (під представниками сторонніх організацій слід розуміти співробітників органів державної влади і управління, аудиторських структур, українських та зарубіжних партнерів, клієнтів, контрагентів, конкурентів).

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

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

Економічна безпека – це універсальна категорія, яка відбиває захищеність суб'єктів соціально-економічних відносин на всіх рівнях, починаючи з держави і закінчуючи кожним її громадянином. Категорія економічної безпеки характеризує динамічну рівновагу економічної системи в часі, яка досягається в процесі її розвитку і адаптації до дій внутрішніх і зовнішніх чинників.

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

Засіб захисту – засіб, застосування якого виключає або знижує дію на одного або кількох працівників небезпечних і (або) шкідливих виробничих чинників.

Захист прав – сукупність дозволених законом певних дій, прийомів, способів, що використовуються особою, право якої порушено або може бути порушено чи оспорюється самостійно або шляхом звернення до компетентних органів державної влади, з метою відновлення порушеного (оспорюваного) права, припинення правопорушення чи запобігання вчиненню правопорушення та відшкодування спричиненої шкоди.

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

Зміст документопотоку – це склад документів, включених до нього, та склад інформації, зафіксованої в цих документах.

Інформація – це нематеріальне немайнове благо особливого роду, яке нерозривно пов’язане з життям, з його виникненням і закінченням, яке проявляється як особисте немайнове благо, як результат впливу на людину та інших суб’єктів та об’єктів права, як результат інтелектуальної творчої діяльності і як відомості про осіб, події та явища, предмети, об’єкти і процеси незалежно від форми їхнього представлення.

Інформаційні ресурси науково-технічної інформації – це систематизоване зібрання науково-технічної літератури і документації (книги, брошури, періодичні видання, патентна документація,нормативно-технічна документація, промислові каталоги,конструкторська документація, звітна науково-технічна документація з науково-дослідних і дослідно-конструкторських робіт, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксовані на паперових чи інших носіях.

Інструкція з діловодства – це правовий акт, що встановлює технологію створення або одержання документів, їхньої обробки, збереження і використання в поточній діяльності підприємства.

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

Конкуренція – процес управління суб'єктом своїми конкурентними перевагами для того, щоб перемогти або досягти інших цілей в боротьбі з конкурентами за задоволення об'єктивних чи суб'єктивних потреб в рамках законодавства або в природних умовах.

Комерційна таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Конфіденційна інформація:- відомості, якими володіють, користуються або розпоряджаються окремі фізичні чи юридичні особи і які поширюються за їх бажанням відповідно до передбачених ними умов;- є власністю держави і перебуває в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ до неї.

Конфіденційне діловодство здійснюється шляхом вирішення комплексу організаційно-правових, інженерно-технічних, криптографічних та оперативно-пошукових заходів, спрямованих на запобігання розголошення інформації з обмеженим доступом та втратами її матеріальних носіїв.

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

Міжоб'єктні служби безпеки – служби, які, як правило, спеціалізуються або на чисто режимно-охоронних послугах (охорона будівель, споруд, транспорту, окремих працівників підприємств, установ, членів їх сімей тощо), або на суто економічних, правових чи консультаційних.

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

Науково-інформаційна діяльність – це сукупність дій, спрямованих на задоволення потреб громадян, юридичних осіб і держави у науково-технічній інформації, що полягає в її збиранні, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні.

Невизнання права – це дії учасника цивільного правовідношення, який несе юридичний обов'язок перед уповноваженою особою, які спрямовані на заперечення в цілому або у певній частині суб'єктивного права іншого учасника цивільного правовідношення, внаслідок якого уповноважена особа позбавлена можливості реалізувати своє право.

Неправомірним збиранням комерційної таємниці – добування протиправним способом відомостей, що відповідно до законодавства України становлять комерційну таємницю, якщо це завдало чи могло завдати шкоди суб'єкту господарювання (підприємцю).

Неправомірним використанням комерційної таємниці – впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи неправомірно здобутих відомостей, що становлять відповідно до законодавства України комерційну таємницю.

Ноу-хау – відомості про рішення у будь-яких сферах практичної діяльності (техніці, економіці, організації тощо), що допускає практичне використання та є придатним для участі в економічному обігу в силу невідомості та недоступності невизначеному колу осіб.

Номенклатура справ (далі – НС) – це обов'язковий для кожної юридичної особи систематизований перелік назв справ, що формуються у діловодстві із зазначенням строків зберігання.

Організація документообігу – загальні засади організації документообігу підприємства, констатують категорію підприємства залежно від обсягу документообігу, визначають форму організації діловодства (централізована, децентралізована, змішана), порядок реєстрації і обліку документів, створення інформаційно-пошукових систем.

Оспорювання – це такий стан цивільного правовідношення, при якому між учасниками існує спір з приводу наявності чи відсутності суб'єктивного права у сторін, а також приналежності такого права певній особі. Оспорюване право ще не порушене, але виникає невизначеність у праві, зумовлена поведінкою другої сторони щодо уповноваженого.

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

Порушенням права на інформацію – такий стан суб'єктивного права, при якому воно зазнало протиправного впливу з боку правопорушника, внаслідок якого суб'єктивне право уповноваженої особи зазнало зменшення або ліквідації як такого. Порушення права пов'язане з позбавленням його носія можливості здійснити, реалізувати своє право повністю або частково.

Режим секретності – встановлений згідно з вимогами Закону «Про державну таємницю» та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці.

Розголошенням комерційної таємниці – ознайомлення іншої особи без згоди особи, уповноваженої на те, з відомостями, що відповідно до чинного законодавства України становлять комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання (підприємцю).

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

Система охорони державної таємниці – це організована державою сукупність суб'єктів режимно-секретної діяльності, які здійснюють, у межах визначеної законодавством компетенції, охорону державної таємниці для забезпечення національної безпеки України від загрози розголошення (витоку) державної таємниці чи/або втрати матеріальних носіїв секретної інформації в інформаційній сфері.

Схилянням до розголошення комерційної таємниці – спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків відомості, що відповідно до законодавства

України становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання (підприємцю).

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

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

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

Технічні засоби захисту – це технічні пристрої і (або) технологічні розробки, призначені для створення технологічної перешкоди порушенню авторського права і (або) суміжних прав при сприйнятті і (або) копіюванні захищених (закодованих) записів у фонограмах (відеограмах) і передачах організацій мовлення чи для контролю доступу до використання об'єктів авторського права і суміжних прав.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Конституція України // Відомості Верховної Ради України. – 1996. – №30. – Ст.141.
2. Господарський кодекс України // Відомості Верховної Ради України. –2003 – №18-22, – Ст.144.
3. Науково-практичний коментар Господарського кодексу України / За заг. ред. В.К.Мамутова. – К.: Юрінком Інтер, 2004. – 688 с.
4. Науково-практичний коментар Господарського кодексу України / Кол. авт.: Г. Л. Знаменський, В. В. Хахулін, В. С. Щербина та ін.; За заг. ред. В. К. Матузова. – К.: Юрінком Інтер, 2004. – 688 с.
5. Цивільний кодекс України. // Офіційний вісник України. – 2003. – № 11. – С. 461.
6. Науково-практичний коментар Цивільного кодексу України: У 2 т. / За відповід. ред. О. В. Дзери (кер. авт. кол.), Н. С. Кузнєцової, В. В. Луця. – К.: Юрінком Інтер, 2005. – Т. І. – 832 с.
7. Науково-практичний коментар Цивільного кодексу України / За ред. В.М. Коссака. – К.: Істина, 2004. – 976 с.
8. Цивільний процесуальний кодекс України від 18.03.2004 р. № 1618-IV // Відомості Верховної Ради. – 2004. - N 40-41, 42. - ст. 492.
9. Кримінальний кодекс України // Офіційний Вісник України. – 2001. – №21. – Ст. 920.
10. Кодекс України про адміністративні правопорушення // Відомості Верховної Ради Української РСР. – 1984. Додаток до №51. – Ст. 1122. Із змінами і доповненнями станом на 1 квітня 2002р. – Х.: Одисей, – 2002.
11. Кодекс адміністративного судочинства України від 06.07.2005 р. № 2747-IV // Відомості Верховної Ради. – 2005. - N 35-36, N 37. - ст. 446.
12. Про інформацію: Закон України в редакції Закону від 13.01.2011 р. № 2938-VI // Відомості Верховної Ради України. 2011. № 32. Ст.313.
13. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України № 537–V від 09.01.2007 р. // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.
14. Про захист від недобросовісної конкуренції : Закон України від 7 червня 1996 р. №236 // Відомості Верховної Ради України. 1996. №36. Ст. 164.
15. Про авторське та суміжні права: Закон України від 17.07.2001р. // Відомості Верховної Ради України. – 2001. – №13. – Ст.64.
16. Про державну таємницю: Закон України від 21.01.94р. // Відомості Верховної Ради України. – 1994. – №16. – Ст.93.
17. Про службу безпеки України: Закон України № 2229-XII від 25.03.1992 р. // Відомості Верховної Ради України. – 1992. – N 27. – ст. 382.
18. Про колективні договори й угоди: Закон України № 3356-XII від 1.07.1993 р. // Відомості Верховної Ради України. – 1993. – N 36. – ст. 361.
19. Про перелік відомостей, що не становлять комерційної таємниці: Постанова Кабінету Міністрів України № 611 від 9.08.1993 р. // Зібрання постанов Уряду України, 1993, N 12, ст. 269
20. Звід відомостей, що становлять державну таємницю України. Затверджений наказом Голови Служби безпеки України від 1.03.01 р. № 52 // zakon.rada.gov.ua.

21. Концепція технічного захисту інформації в Україні: Затв. Постановою Кабінету Міністрів України від 8 жовтня 1997 р. № 1126.

22. Положення про технічний захист інформації в Україні: Затв. Указом Президента України від 27 вересня 1999 р. № 1229/99.

23. Про затвердження Положення про контроль за функціонуванням системи технічного захисту інформації: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації служби безпеки України від 22.12.99 № 61.

24. Про затвердження Інструкції про порядок забезпечення режиму безпеки, що повинен бути створений на підприємствах, установах та організаціях, які здійснюють підприємницьку діяльність у галузі криптографічного захисту конфіденційної інформації, що є власністю держави: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації служби безпеки України від 22.10.99 № 45.

25. Про затвердження Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації служби безпеки України від 30.11.99 № 53.

26. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави: Затв. Постановою Кабінету Міністрів України від 27.11.98 № 1893.

27. Положення про режимно-секретні органи в міністерствах, відомствах, Уряді Автономної Республіки Крим, місцевих органах державної виконавчої влади, виконкомах Рад, на підприємствах, в установах і організаціях: Затв. Постановою Кабінету Міністрів України від 04.08.95 № 609.

28. Про затвердження Інструкції щодо умов і правил здійснення діяльності у галузі технічного захисту інформації та контролю за їх дотриманням: Наказ Державної служби безпеки України з питань технічного захисту інформації від 23.05.94 № 46.

29. Інструкція про умови і правила провадження підприємницької діяльності (ліцензійні умови), пов’язаної з розробленням, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації, та контроль за їх дотриманням: Затв. наказом Ліцензійної палати України та Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 17.11.98 № 104/81.

Додаткова

1. Андрощук Г. Правова охорона комерційної таємниці в країнах Європейського Союзу // Теорія і практика інтелектуальної власності. 2012. №5. С. 26-36.

2. Андрощук Г.А., Крайнев П.П. Экономическая безопасность предприятия: защита коммерческой тайны / Г.А. Андрощук, П.П. Крайнев. – К., Издательский Дом «Ин Юре», 2000. – 400 с.

3. Алексеев С. В. Правовое регулирование предпринимательской деятельности / С.В. Алексеев // Учеб. пособие для вузов. – М.: ЮНИТИ-ДАНА, Закон и право, 2004. – 502 с. – (Серия «Dura lex, sed lex»).

4. Білоусов В.М. Інститут комерційної таємниці в законодавстві України: поняття і шляхи вдосконалення / В.М. Білоусов //Часопис Київського університету права, 2009 – №1.

5. Беспянска Г. Методологія і методика раціоналізації діловодства // Секретар-референт. – 2007. – № 12 (декабрь) – С. 9-13.

6. Беспянска Г. Раціоналізація документообігу на підприємстві // Секретар-референт. – 2007. – № 10 (октябрь) – С. 21-25.

7. Беспянска Г. Розроблення Інструкції з організації роботи з документами, що містять комерційну таємницю / Г. Беспянска // Секретар-референт. – 2007. – № 9 (сентябрь) – С. 9-116.

8. Бибик С.П., Сюта Г.Н. Ділові документи та правові папери / С.П. Бибик – Харків: ФОЛІО; 2006..

9. Безклубий І. А. Банківські правочини: цивільно-правові проблеми: Монографія. – К.: Видавничо-поліграфічний центр "Київський університет", 2005. – 378 с.

10. Вінник О.М. Господарське право: Курс лекцій / О.М Вінник // К.: Атіка, 2004. – 624 с.

11. Гончар И. Режим коммерческой тайны / И. Гончар // Юридическая практика. – 2005. - № 40 (406).

12. Глухівський Л. Державна таємниця та охорона прав на винаходи / Л. Глухівський //Інтелектуальна власність. – 2005. - № 9. – С. 21-23.

13. Демушкин А.С. Документы и тайна. Государственная. Личная (персональные данные). Почтово–телеграфные отправления. Религиозная. Следствия и судопроизводства. Свидетельская. Безопасности участников правосудия. Адвокатская. Служебная. Аудиторская. Записи актов гражданского состояния. Профессиональная. Врачебная. Нотариальная. Журналистская. Коммерческая. Банковская. Производства (ноу–хау) : [научное издание] / А.С. Демушкин. – М.: ООО «Городец-издат», 2003. – 396 с.

14 Дрейс Ю. О. Функціонування системи охорони державної таємниці в україні: організаційно-правова структура, принципи та завдання // Безпека інформації. 2014. Т. 20. № 2. С. 176-184.

15. Дудоров О.О. Злочини у сфері господарської діяльності: кримінально-правова характеристика: Монографія. – К.: Юридична практика, 2003. – 924 с.

16. Загорецька О. Особливості роботи з документами, що містять комерційну таємницю підприємства // Довідник кадровика. 2011. № 09(111). С.40-46.

17. Зайцева-Калаур І. В. Інформаційне право: навчальний посібник.– Тернопіль: ФО-П Шпак В.Б., 2017.– 227 с.

18. Капіца Ю.М. Проблеми правової охорони комерційної таємниці, ноу-хау та конфіденційної інформації в праві України // Реферативний огляд діючого законодавства України та практики його застосування / Регіональний центр АПН України. – К., 2000. – С.175-199.

19. Климчук С. Проведення порівняльного аналізу законодавства у сфері інформації з обмеженим доступом України та країн_членів НАТО / С. Климчук // Юридичний радник. – 2006. – № 11. – С. 9–16.

20. Козлов С.С., Тимошенко В. А. Коментар до Закону від 21 липня 1993 р. № 5485-1 «Про державну таємницю». - М.: ТОВ «Нова правова культура», 2006 р.

21. Кормич Б.А. Інформаційна безпека: організаційно-правові основи / Б.А. Кормич Навч. посібник.– К.: Кондор, 2004.– 384 с.

22. Костюк В. Л., Бонтлаб В. В. Проблемні питання застосування положень щодо комерційної таємниці в трудовому договорі / // Бюлетень Міністерства юстиції України. – 2005. - № 2 (40). – С. 46 – 52.

23. Кохановська О.В. Інформація як нематеріальне благо та захист інформаційних прав згідно з Цивільним кодексом України / О.В. Кохановська // Вісник Верховного суду України. – 2005. – № 11. – С. 37–44.

24. Курман О. В. Типізація способів учинення злочинних посягань на відомості, що становлять комерційну або банківську таємницю / Теорія та практика судової експертизи і криміналістики. Випуск 10. 2010. С. 62-68.

25. Мірошник Ю. Державна таємниця як складова забезпечення національної безпеки України / Ю. Мірошник // Право України. – 2004. - № 9. – С. 32 – 34.

26. Нелін О. І., Низенко Е. І., Панфілов В. М. Роль недержавних служб безпеки в захисті економічних інтересів підприємництв / О.І. Нелін // К.: Поліграф-Сервіс, 2001.

27. Низенко Е. І. Організаційно-правове забезпечення, формування та реалізація державної політики в сфері безпеки підприємництва // Зб. наук. праць. — К.: Приватне право і підприємництво, 2003.

28. Низенко Э. И. Обеспечение безопасности предпринимательской деятельности: Учеб. пособие. — К.: МАУП, 2003. — 123 с.

29. Нікіфоров Г.К., Нікіфоров С.С. Підприємництво та правовий захист комерційної таємниці / Навч.-практ. посіб. Для вищих навч. закл. – К.: Олан, 2001. – 208 с.

30. Ніколаєва Т. Конфіденційна інформація / Т. Ніколаєва // Юридичний вісник України. – 2004. - № 37.

31. Носік Ю. Міжнародно-правова охорона комерційної таємниці / Ю. Носік // Право України. – 2004. - № 11. – С. 131-135.

32. Носік Ю.В. Підстави виникнення, зміни та припинення прав на комерційну таємницю в Україні / Ю.В. Носік // Бюлетень Міністерства юстиції України. – 2006. – № 1. – С. 86-94.

33. Носік Ю.В. Юридичне значення ознак комерційної таємниці// Приватно-правовий метод регулювання суспільних відносин: стан та перспективи розвитку: Збірник тез Міжнародної наукової конференції студентів та аспірантів (25-26 листопада 2005 року). – Київ – Хмельницький: Видавництво Хмельницького університету управління та права, 2005.

34. Пастернак М. С. Процедура віднесення інформації до державної таємниці // Інформаційна безпека людини, суспільства, держави. 2012. №1 (8). С.88-93.

35. Пашков А. С. Система охорони державної таємниці та її роль в забезпеченні інформаційної безпеки // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Вип. №22. 2009. С. 168- 171.

36. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю (аналіз складів злочинів). Автореф. дис. ... канд. юр. наук: 12.00.08 / Національна юридична академія України імені Ярослава Мудрого. – Харків, 2002. – 15 с.

37. Самойлова О.С. Конфіденційна інформація, що є власністю держави, як різновид інформації з обмеженим доступом: актуальні проблеми сучасної науки в дослідженнях молодих учених: зб. наук. праць / О.С. Самойлова. – Х.: Вид_во Нац. ун_ту внутр. справ, 2003. – С. 84–92.

38. Самойлова О.С. Кримінально_правова характеристика передачі або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави: дис. … канд. юрид. наук: 12.00.08 / Самойлова О.С. – К., 2006. – 18 с.

39. Сляднева А. Определение понятия коммерческой тайны субъекта хозяйствования // Підприємництво, господарство і право. – 2004. - № 9. – С. 40 – 43.

40. Сляднєва Г. О. Комерційна таємниця як вид інформації / Г.О. Следнєва // Актуальні проблеми держави і права. – Одеса: Одеська національна юридична академія, Юридична література. – 2003. – Вип. 18. – С. 624-629.

41. Сляднєва Г.О. Поняття та ознаки комерційної таємниці суб'єкта господарювання // Актуальні проблеми держави і права. – Одеса: Одеська національна юридична академія, Юридична література. – 2003. – Вип. 21. – С. 307 – 311.

42. Сляднєва Г.О. Специфіка комерційної таємниці суб'єкта господарювання та її відокремлення від інших видів таємниць / Г.О. Следнєва // Вісник Хмельницького інституту регіонального управління та права. – 2004. - № 3. – С. 126-130.

43. Стенюков М.В. ЗРАЗКИ ДОКУМЕНТІВ з діловодства (керівництво до складання) – М.: "Видавництво ПРІОР", 2002. – 144 с.

44. Харченко В. Комерційна таємниця: проблеми охорони за кримінальним законодавством України та напрямки її вдосконалення / В. Харченко // Теорія і практика інтелектуальної власності. – 2008.– № 6.– С.42-53.

45. Франчук С. Як організувати захист комерційної таємниці та конфіденційної інформації на підприємстві // Юридична газета. URL: http://www.yur-gazeta.com/article/1326/

46. Чікін С., Черненко В. Управління комерційною таємницею на підприємстві: дії організаційного, технічного та психологічного характеру / С. Чікін, В. Черненко // Теорія і практика інтелектуальної власності. – 2011.– №5.– 56-64.

47. Чікін С., Черненко В. Комерційна таємниця як об'єкт управління на підприємстві / С. Чікін, В. Черненко // Теорія і практика інтелектуальної власності. – 2011.– №4.– 56-61.