

**Київський національний торговельно-економічний університет**

**Кафедра міжнародного, цивільного та комерційного права**

**ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА**

на тему:

**ОХОРОНА ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ**

студента 2 курсу, 6 м групи,  
спеціальності 081 «Право»,  
спеціалізації  
«Цивільне право і процес»

Селищева Кирила Костянтиновича

Науковий керівник

к.ю.н.

Коренюк Ольга Олександрівна

Гарант освітньої програми

д.ю.н.

Примак Володимир Дмитрович

**Київ-2020**

**ЗМІСТ**

<b>ВСТУП</b> .....	3
<b>РОЗДІЛ 1 ТЕОРЕТИКО-ПРАВОВІ АСПЕКТИ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ</b>	
1.1. Поняття та ознаки інформації з обмеженим доступом.....	7
1.2. Цивільно-правова охорона окремих видів інформації з обмеженим доступом.....	12
1.3. Особливості охорони комерційної таємниці як виду конфіденційної інформації.....	20
<b>РОЗДІЛ 2 ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ</b>	
2.1. Цивільно-правовий захист інформації з обмеженим доступом.....	27
2.2. Міжнародний досвід охорони інформації з обмеженим доступом.....	37
<b>ВИСНОВКИ ТА ПРОПОЗИЦІЇ</b> .....	47
<b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ</b> .....	50

## ВСТУП

**Актуальність теми дослідження.** Протягом багатьох років необхідність обмеження доступу до певних видів інформації призвело к створенню правових конструкцій для охорони інтересів суспільства, держави, приватних осіб.

Суспільство ХХІ століття все більше розвивається як інформаційне, для якого характерне збільшення обсягів інформації, передача та поширення її, проте існує інформація, розголошення чи оприлюднення якої може завдати шкоди окремим суб'єктам цього суспільства.

Фундамент інформаційної безпеки в Україні становить розмежування інформації на два види: загальнодоступної та інформації з обмеженим доступом.

В Україні стає проблема створення адекватної нинішнім реаліям системи законодавства, що регулює охорону інформації з обмеженим доступом, адже вона має особливе, обмежене коло користувачів, не призначена для широкого розповсюдження і у зв'язку з цим підлягає правовій охороні від несанкціонованого доступу.

Разом із тим, враховуючи інтеграційні прагнення України співпрацювати з Європейським Союзом, потреба в гармонізації національного законодавства у сфері захисту персональних даних відповідно до стандартів Європейського Союзу, вивчення міжнародного досвіду охорони інформації з обмеженим доступом актуально для України.

Вище написане зумовлює актуальність проблематики, необхідність додаткового дослідження вказаних питань з охорони інформації з обмеженим доступом, а відтак вибір теми випускної кваліфікаційної роботи, її об'єкт, предмет, мету і задачі.

Певні аспекти цивільно-правового регулювання, а також питання охорони інформації з обмеженим доступом висвітлені в працях таких правознавців, як В.М. Бем [54], В.В. Головченко [58], О.В. Гронь [61], С.С. Єсімов [63], О.В. Кохановська [66], Д.В. Коц [67], О.О. Кулініч [68], І.І. Саліхов [78]. Також окремі аспекти, зокрема адміністративно-правові, досліджували у своїх працях

вітчизняні вчених-юристи, такі як: Н.В. Нетеса [72], Т.І. Обуховська [73], Н.О. Попова [76], А.В. Тунік [82], О.О. Шарабурина [85] та інші.

Проте аналіз наукових досліджень з цієї проблематики дає змогу дійти висновку, що хоча в юридичній науці і сформоване загальне уявлення про інформацію з обмеженим доступом, разом з тим, недостатньо уваги приділяється заходам щодо забезпечення збереження різних видів інформації з обмеженим доступом. Немає єдиної точки зору і щодо вдосконалення правової охорони окремих видів інформації з обмеженим доступом.

**Мета дослідження.** Автор випускної кваліфікаційної роботи ставив за мету на основі комплексного аналізу вітчизняного та зарубіжного законодавства у сфері охорони інформації з обмеженим доступом прийти до висновків теоретичного характеру та створити певні пропозиції щодо нормативного регулювання окремих видів інформації з обмеженим доступом та вдосконаленням процесу цивільно-правової охорони цієї інформації.

Для досягнення поставленої мети було сформульовано такі основні завдання:

- дослідити поняття інформації з обмеженим доступом;
- виявити ознаки інформації з обмеженим доступом;
- проаналізувати специфіку цивільно-правової охорони окремих видів інформації з обмеженим доступом;
- дослідити особливості охорони комерційної таємниці як виду конфіденційної інформації;
- розробити пропозиції щодо цивільно-правового захисту інформації з обмеженим доступом;
- вивчити досвід інших держав, зокрема держав Європейського Союзу (Італії, Франції, Португалії, Німеччини, Австрії, Латвії, Фінляндії) та США, щодо охорони інформації з обмеженим доступом.

**Об'єктом дослідження** є суспільні відносини, які виникають в процесі одержання, використання, поширення, зберігання та захисту інформації з обмеженим доступом.

**Предметом дослідження** в роботі є охорона інформації з обмеженим доступом.

**Методами дослідження** стали логічний, формально-юридичний, інтерпретації, діалектичний, системно-функціональний, порівняльно-правовий та інші методи.

При виконанні кваліфікаційної роботи був використаний логічний метод, застосування якого дозволило отримати нове юридичне знання про природу та структуру інформації з обмеженим доступом (параграф 1.1.); формально-юридичний, який включає в себе прийоми опису і аналізу правових норм, правовідносин та інших юридичних категорій та використовується, зокрема при аналізі нормативно-правової бази України (параграф 1.1.; 1.2.; 1.3.); інтерпретації (тлумачення) (параграф 1.2.); діалектичний (параграф 1.3.); системно-функціональний (параграф 2.1.); порівняльно-правовий метод, який застосовувався при порівнянні вітчизняного та зарубіжного законодавства у сфері охорони інформації з обмеженим доступом (параграф 2.2.).

**Наукова новизна** полягає у комплексному дослідженні інституту охорони інформації з обмеженим доступом.

Певні теоретичні та практичні результати дослідження знайшли відображення в науковій статті «Правове регулювання інформації з обмеженим доступом в Україні та країнах Європейського Союзу», що опублікована у збірнику наукових статей «Цивільне та комерційне право : виклики сьогодення». К.: Київ. нац. торг.-екон. ун-т, 2020. С. 200-208.

**Практичне значення** цього дослідження визначається пропозиціями щодо внесення змін в чинне законодавство України з метою вдосконалення правової охорони інформації з обмеженим доступом, закріплення в законодавстві нового поняття «інформація з обмеженим доступом», прийняття окремого Закону, щодо захисту персональних даних неповнолітніх осіб. Зібраний матеріал і узагальнення можуть бути використані для підготовки узагальнюючих праць, при підготовці лекційних занять та спецкурсів у вищих навчальних закладах.

**Структура випускної кваліфікаційної роботи** відображає логіку і послідовність наукового дослідження та зумовлена його предметом і метою. Робота складається з анотації, змісту, вступу, двох розділів, висновків, пропозицій та списку використаних джерел. Загальний зміст роботи викладений на 63 сторінці, з них 49 сторінок основного тексту. Список використаних джерел складає 100 найменувань.

## РОЗДІЛ 1

### ТЕОРЕТИКО-ПРАВОВІ АСПЕКТИ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

#### 1.1. Поняття та ознаки інформації з обмеженим доступом

Перш ніж говорити про інформацію з обмеженим доступом, як один із видів інформації, що може одержуватись, використовуватись, поширюватись, зберігатись та захищатись з метою реалізації прав, свобод і законних інтересів громадян, за доцільне вбачається дослідити також і саме поняття інформації.

Цивільний кодекс України закріпив дефініцію «інформація», як дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (стаття 200) [45]. Аналогічне визначення можна знайти у ст. 1 Закону України «Про інформацію» [29].

В сучасному світі інформація може виступати, наприклад, як засіб реалізації конституційних прав і свобод, як товар у процесах її створення, як об'єкт права власності тощо.

Наведене визначення поняття «інформація» дає підстави для виділення таких ознак: 1) інформація – це відомості про події та явища, що відбуваються у державі або у навколишньому природному середовищі; інформація – це дані, які можуть зберігатися в будь-якій формі й вигляді; інформація є об'єктом цивільних прав і належить до категорії нематеріальних благ; інформація – це відомості, які є документованими або публічно оголошеними.

Інформація як об'єкт цивільних прав може «вільно відчужуватися або переходити від однієї особи до іншої в порядку правонаступництва чи спадкування або іншим чином, якщо вони не вилучені з цивільного обороту або не обмежені в обороті (стаття 178 Цивільного кодексу України) [45]. Проте на практиці важко встановити, чи вилучено інформацію з цивільного обороту, а от з інформацією, обмеженою в обороті, легше, такою може вважатися інформація з обмеженим доступом.

Закон України «Про інформацію» за порядком доступу поділяє інформацію на відкриту та інформацію з обмеженим доступом [29].

В законодавстві України немає чіткого формулювання поняття «інформація з обмеженим доступом», проте визначення цього поняття ми можемо знайти в окремих міжнародних двосторонніх угодах між Україною та Європейським Союзом, а саме: в Угоді між Кабінетом Міністрів України та Урядом Словацької Республіки про взаємну охорону інформації з обмеженим доступом [42], Угоді між Україною та Угорською Республікою про взаємну охорону інформації з обмеженим доступом [43], Угоді між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону інформації з обмеженим доступом [40], Угоді між Кабінетом Міністрів України та Урядом Румунії про взаємну охорону інформації з обмеженим доступом [41] тощо.

У науковій сфері існують доктринальні визначення досліджуваного нами поняття інформації з обмеженим доступом, проте, як зазначають В. Ліпкан і Л. Капінус, вони практично відсутні навіть у спеціалізованих працях, предметом яких є безпосередньо інформація з обмеженим доступом [70, с. 46].

Досліджуючи інформацію з обмеженим доступом як предмет цивільно-правового регулювання, О.О. Кулініч розглядає таку інформацію як відомості, дані і знання, що мають особливу цінність для осіб, у володінні яких знаходяться, та щодо яких уживаються заходи, спрямовані на обмеження вільного доступу третіх осіб, поширення яких може заподіяти істотну шкоду зацікавленим особам (власникам чи добросовісним користувачам) [68, с. 8].

З наукової позиції вченого-цивіліста І.І. Саліхова інформація з обмеженим доступом як об'єкт цивільних прав – це здатні бути предметом майнових чи особистих немайнових відносин, відомі лише певному колу осіб і наділені в силу цього особливою цінністю відомості, дані та знання, по відношенню до яких володільцем здійснюються заходи, спрямовані на обмеження вільного доступу третіх осіб, поширення яких може завдати істотної шкоди зацікавленим особам [78].



О.О. Шарабурина дає визначення інформації з обмеженим доступом, як відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, доступ до яких обмежений відповідно до законодавства України, та здійснюється спеціальними уповноваженими суб'єктами адміністративно-правових відносин виключно для захисту визначеного законом інтересу, в межах встановленої мети, для запобігання завдання такому інтересу істотної шкоди, спричиненої розкриттям відомостей [87].

В.Ю. Баскакова трактує термін інформація з обмеженим, як інформацію, відомості та/або дані якої можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, доступ до яких обмежено відповідно до законодавства України її власником чи добросовісним користувачем (суб'єктом владних повноважень, фізичною або юридичною особою) у зв'язку з її особливою цінністю для них на законних підставах [53].

Ми погоджуємося з думкою, що О.О. Шарабурина та В.Ю. Баскаков визначають дефініцію «інформація з обмеженим доступом» з точки зору адміністративно-правового режиму, тому що в наведених науковцями визначеннях увага зосереджується на певних матеріальних носіях, на відміну від О.О. Кулініч, яка дає визначення дефініції нам з точки цивільно-правового і увага зосереджується вже на самому визначенні сутності поняття «інформації з обмеженим доступом».

Аналізуючи визначення поняття інформації з обмеженим доступом, які розглядають різні науковці в області юриспруденції, не залишимо без уваги думку Д.В. Коц про те, що інформація з обмеженим доступом – це відомості та/або дані, які збережені на матеріальних носіях чи відображені в електронному вигляді, які є в законному володінні юридичної особи, фізичної особи, суб'єкта владних повноважень, доступ до яких обмежено таким володільцем відповідно до закону в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав конкретної фізичної особи, інших

людей, юридичних осіб, для запобігання розголошенню інформації, одержаної конфіденційно, для підтримання авторитету і неупередженості правосуддя, та які містяться в документах суб'єктів владних повноважень, одночасно становлячи внутрівідомчу службову кореспонденцію, пов'язану з розробкою напряму діяльності таких суб'єктів або здійсненням ними контрольних, наглядових функцій, процесом прийняття рішень, а також ті, що зібрані в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, шкода від розголошення яких може бути спричинена особі, суспільству і державі, та переважатиме суспільний інтерес в їх отриманні [67, с. 110].

Незважаючи на те, що визначення поняття «інформація з обмеженим доступом» не лаконічно сформульоване науковцем та обтяжене великим смисловим перенавантаженням, проте, воно має цивільно-правовий підхід. З іншої сторони, поняття детально конкретизує у яких суб'єктів може перебувати ці відомості або дані.

Нарешті, з нашої точки зору, інформація з обмеженим доступом – сукупність відомостей, даних, знань, які відтворені на фізичних предметах (флеш-накопичувачах, комп'ютерах та ін.) і можуть запам'ятовувати та зберігати інформацію та мають особливу цінність для окремих суб'єктів-володільців цієї інформації, ризик витоку такої інформації загрожує зробити істотну шкоду цим суб'єктам.

Розглянувши поняття «інформації з обмеженим доступом», які наводять вчені-цивілісти та вчені-адміністративісти у своїх наукових працях необхідно перейти к розгляду ознак інформації з обмеженим доступом.

З вищенаведених визначень інформація з обмеженим доступом повинна мати наступні ознаки:

- 1) надання такої інформації третім особам або допуск до неї можливий лише у випадку проведення певної процедури;
- 2) володільць інформації вживає заходи з її захисту;
- 3) отримання інформації з обмеженим доступом пов'язане, як правило, з виконанням службових або професійних обов'язків;

4) інформація вилучена із вільного обігу на підставі закону [71, с. 47].

У свою чергу, О. Курман дотримується думки, що до ознак інформації з обмеженим доступом можна віднести: 1) певний суб'єктний склад і зміст; 2) застосування заходів, що обмежують вільний доступ третіх осіб до інформаційного ресурсу; 3) відповідність інформаційного ресурсу вимогам законодавства [69].

До ознак інформації з обмеженим доступом в ході цивілістично-правових досліджень можна вважати наступні: 1) зміст інформації з обмеженим доступом складають знання, повідомлення, відомості про соціальну форму руху матерії і про всі інші її форми у тій мірі, у якій вони використовуються суспільством, державою; 2) відомості, що складають зміст інформації з обмеженим доступом, за своєю сутністю ідеальні (нематеріальні); 3) інформація з обмеженим доступом є самостійним об'єктом правового регулювання, що не залежить від конкретної форми її матеріального носія; 4) інформація з обмеженим доступом не є загальнодоступною; 5) інформація з обмеженим доступом відома і використовується чітко визначеним колом осіб; 6) суб'єкт інформації вживає заходів, що спрямовані на обмеження вільного доступу третіх осіб до інформації; 7) інформація з обмеженим доступом має особливу соціальну цінність у силу її дійсної або потенційної невідомості третім особам. Поширення такої інформації може спричинити заподіяння істотної шкоди зацікавленим особам; 8) зміст інформації з обмеженим доступом відповідає обмеженням, установленим законодавством [68].

Принагідно також згадати окремі класифікуючі ознаки таємної, конфіденційної та службової інформації, які мають свої складники.

До таких класифікуючих ознак слід віднести: 1) ознаки конфіденційної інформації: а) ідентифікує фізичну особу; б) доступ до неї обмежено фізичною або юридичною особою, крім суб'єкта владних повноважень; в) поширення відбувається винятково за згодою фізичної або юридичної особи; 2) ознаки таємної інформації: а) розголошення може завдати шкоди особі, суспільству і державі; б) обмеження доступу здійснюється винятково в інтересах національної

безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; в) шкода від оприлюднення стосується суспільного інтересу в її отриманні; 3) ознаки службової інформації: а) міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, пов'язану з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; б) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці [67, с. 108-109].

Дослідивши загальні та спеціальні-класифікуючі ознаки, вважаємо, що інформація з обмеженим доступом характеризується наступними ознаками:

- 1) може виступати об'єктом інтелектуальної власності;
- 2) захисту підлягає лише задокументована інформація (відтворена на фізичних носіях);
- 3) зміст інформації з обмеженим доступом, має особливу цінність;
- 4) здатність інформації впливати на діяльність володільця цієї інформації, як з позитивного боку, так і з негативного;
- 5) інформація зафіксована у вигляді тексту, за допомогою аудіо на звуковому носії, або відео.

## **1.2. Цивільно-правова охорона окремих видів інформації з обмеженим доступом**

Віднесення інформації до категорії з обмеженим доступом розуміється як установлений правовими нормами порядок визначення важливості відомостей і необхідність їх виокремлення із загальнодоступної інформації, встановлення

обмежень доступу до них з метою запобігання негативним наслідкам для особи, суспільства, держави у разі витоку або розголошення цих відомостей.

Основою правового регулювання охорони та обмеження доступу до інформації в Україні є норми ч. 2. ст. 32 Конституції України [1], згідно з якими не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини, та норми ч. 3 ст. 34 Конституції України [1], якими передбачено можливість обмеження свободи інформації на основі закону в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Правова регламентація охорони інформації з обмеженим доступом в Україні визначається, зокрема, Законом України «Про інформацію» (в редакції від 21.12.2019 р.) [29], «Про доступ до публічної інформації» (в редакції від 01.12.2019 р.) [24] та «Про захист персональних даних» (в редакції від 04.03.2020 р.) [28].

Закон України «Про інформацію» регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [29]. Закон України «Про доступ до публічної інформації» визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес [24]. Закон України «Про захист персональних даних» регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних [28].

Як зазначає В.Т. Савицький, особливість місця цих законів у системі спеціальних законів з правового регулювання інформаційної сфери визначається тим, що саме в них вибудовується класифікація інформації, формулюється понятійно-термінологічний апарат, закріплюються норми, що визначають правовий статус видів інформації, режим роботи з ними, особливості доступу та обмеження доступу до певних видів інформації тощо [77, с. 119].

Існують також інші закони, що визначають правовий режим певних видів інформації з обмеженим доступом: Закони України «Про банки і банківську діяльність» [21], «Про адвокатуру та адвокатську діяльність» [20], «Про рахункову палату» [35], «Про страхування» [37].

Відповідно до статті 7 Закону України «Про доступ до публічної інформації» конфіденційною є інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [24]. Таким чином, можна погодитись, що основними ознаками такої інформації є: 1) наявність документованої форми; 2) неприпустимість віднесення до конфіденційної інформації загальнодоступних відомостей; 3) особлива значущість конфіденційної інформації; 4) наявність засобів охорони й захисту конфіденційної інформації – юрисдикційних, неюрисдикційних; 5) обмеженість доступу до конфіденційної інформації та обмежений міжвідомчий обмін конфіденційною інформацією [60, с. 193].

За суб'єктами конфіденційну інформацію можна поділити на таку, яка перебуває у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідною особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом [24]. Віднесення інформації до категорії конфіденційної є реалізацією повноважень власника, тобто права власності як абсолютного [85, с. 324]. Закон України «Про доступ до публічної інформації» встановлює, що розпорядники інформації, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою

осіб, які обмежили доступ до інформації, а за відсутності такої згоди – лише в інтересах національної безпеки, економічного добробуту та прав людини [24].

Варто звернути увагу, що Постановою Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційну таємницю» від 09.08.1993 № 611 визначено перелік інформації, що не становить комерційну таємницю, а саме: 1) установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами; 2) інформація за всіма встановленими формами державної звітності; 3) дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів; 4) відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць; 5) документи про сплату податків і обов'язкових платежів; 6) інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків; 7) документи про платоспроможність; 8) відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю; 9) відомості, що відповідно до чинного законодавства підлягають оголошенню [34].

На нашу думку, не потрібно на законодавчому рівні Постановою Кабінету Міністрів України створювати «рамковий» перелік відомостей, що не становить комерційну таємницю, можливо, точніше було б прийняти навпаки Постанову з переліком відомостей, що повинні становити комерційну таємницю та відповідно до неї додаток про порядок доступу до відомостей комерційної таємниці. Визначення такого чіткого переліку буде перешкоджати по суті праву фізичних та юридичних осіб визначати яку саму інформацію вони хочуть віднести до комерційної таємниці.

Своєрідним підвидом конфіденційної інформації можна вважати комерційну таємницю, тобто інформацію, яка згідно статті 505 Цивільного кодексу України, 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 зазвичай 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 [45].

Усі види інформації, які можуть вважатися комерційною таємницею, умовно можна розділити на дві групи: технічна інформація, до якої 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 і комерційна інформація, до якої належать віднесено умови контрактів, дані про постачальників і покупців, інформацію про переговори, маркетингові дослідження. [65, с. 9]

Об'єкти інтелектуальної власності, щодо яких отримано патенти або авторські свідоцтва, до складу комерційної таємниці зараховувати немає потреби, оскільки подібні об'єкти охороняються відповідним законодавством, зокрема Законом України «Про охорону прав на винаходи і корисні моделі» [31], «Про авторське право і суміжні права» [19], «Про охорону прав на промислові зразки» [33], «Про охорону прав на знаки для товарів і послуг» [32].

Заходи з охорони комерційної таємниці викладені у Главі 46 Цивільного Кодексу України. При цьому слід розрізняти основні та додаткові заходи. Основні, які вказані у ст. 505 і 506 Цивільного кодексу України [45] та застосовуються незалежно від того, чи був укладений будь-який договір про ознайомлення інших осіб з комерційною таємницею. Це, перш за все, визначення комерційної таємниці і самого загального переліку інформації, яка складає комерційну таємницю, а також нанесення на матеріальні носії (документи), які містять комерційну таємницю грифу «Комерційна таємниця» із вказівкою володільця цієї інформації. Ці заходи доповнюють один одного, вони можуть застосовуватись як у сукупності, так і окремо: з правової точки зору достатньо, якщо буде застосований хоча б один із цих заходів. Такі заходи застосовуються на практиці в українському законодавстві і при реалізації інформаційних прав.



Додаткові заходи, які актуальні при укладенні такого договору, тобто відносяться до випадків договірною ознайомлення з комерційною таємницею чи договірним її використанням [66].

Бажано привернути увагу на особливий вид інформації з обмеженим доступом, такий як інсайдерська інформація. Відповідно до ч.1 ст. 44 Закону України «Про цінні папери та фондовий ринок» під інсайдерською інформацією слід розуміти будь-яку неоприлюднену інформацію про емітента, його цінні папери або правочини щодо них [38]. Інсайдерська інформація може міститись як у бухгалтерських, фінансових, установчих документах, договорах, звітах, так і в усній формі. В Україні спроби цивільно-правово врегулювати охорони інсайдерської інформації хоч і є, проте вони безсистемні та не відображають реальної ситуації, а тому не встигають за вимогами бізнесу і часу.

Ще одним видом конфіденційної інформації є персональні дані.

Закон України «Про захист персональних даних» у статті 2 визначає персональні дані про особу як будь-які відомості чи сукупність відомостей (інформації) про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [28].

Правове регулювання відносин із захисту персональних даних в Україні є Конституція України (ст. 3, 28, 30, 31, 32, 34, 35, 41, 54, 55, 64) [1], Закон України «Про захист персональних даних» [28], Закон України «Про інформацію» [29], документи у сфері захисту персональних даних, прийняті Уповноваженим Верховної Ради України з прав людини [18] та нормативно-правових актах Європейського Союзу, ратифікованих Україною, як Загальна декларація прав людини [5], Міжнародний пакт про громадянські та політичні права [10], Конвенція про захист прав людини і основоположних свобод [9], Конвенція Ради Європи №108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [8], Додатковий протокол до Конвенції Ради Європи №108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних» [4] тощо.

Відповідно до ст. 11 Закону України «Про інформацію» до конфіденційної інформації про фізичну особу, належать, зокрема, дані про національність, дата та місце народження, адреса, місце проживання та перебування, освіта, стан здоров'я, сімейний стан, релігійні переконання, матеріальний стан, професія, доходи та інша інформація про сфери життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Ці відомості не можуть бути використані без письмової згоди суб'єкта персональних даних, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [29].

Про це детально роз'яснює Конституційний Суд України у своєму Рішенні від 20.01.2012 р. № 2-рп/2012, що лише фізична особа, якої стосується конфіденційна інформація, відповідно до конституційного та законодавчого регулювання права особи на збирання, зберігання, використання та поширення конфіденційної інформації має право вільно, на власний розсуд визначати порядок ознайомлення з нею інших осіб, держави та органів місцевого самоврядування, а також право на збереження її у таємниці. Потрібно наголосити, що Конституційний Суд України у Рішенні вважає, що перелік даних про особу, які визнаються як конфіденційна інформація, не є вичерпним. [51].

Наступним видом інформації з обмеженим доступом є таємна. Таємна інформація регулюється Законом України «Про доступ до публічної інформації» [24]. Таємною є інформація з обмеженим доступом, яка має вищий, порівняно з іншими категоріями утаємниченої інформації, ступінь захисту, оскільки її розголошення однозначно спричинить завдання шкоди певній особі, суспільству, державі [84]. Відповідно до статті 8 Закону України «Про доступ до публічної інформації» таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю [24].

Таємна інформація може виступати об'єктом цивільних відносин, тому що вона недоступна широкому колу осіб, наприклад, адвокатська таємниця доступна

тільки клієнту та адвокату; може бути предметом панування суб'єкта правовідносин та здатна задовольняти майнові та особисто немайнові потреби приватних осіб.

Банківська таємниця є одним із самостійних видів таємниць, що охороняються Законом України «Про банки і банківську діяльність» [21].

Основними суб'єктами права на банківську таємницю є її власники та утримувачі, проте, у Законі України «Про банки і банківську діяльність» чітко не визначено, хто є власником банківської таємниці, а хто утримувачем [21]. Власником банківською таємниці може виступати клієнт банку, тобто фізична або юридична особа, яка в процесі співпраці з банківською установою надала їй відомості, що можуть становити банківську таємницю. Утримувач, службова особа банку, яка отримує відомості, що становлять банківську таємницю.

Банківською таємницею, зокрема, є: 1) відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України; 2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди; 3) фінансово-економічний стан клієнтів; 4) системи охорони банку та клієнтів; 5) інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності; 6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація; 7) інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню; 8) коди, що використовуються банками для захисту інформації; 9) інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, отримана під час оцінки її кредитоспроможності [75, с. 126].

Інформація про банки чи клієнтів, що збирається під час проведення банківського та валютного нагляду, становить банківську таємницю.

Поряд з банківською варто звернути увагу і на професійну таємницю: до них належить інформація, яка перебуває у володінні приватних суб'єктів, але на відміну від конфіденційної інформації, випадки віднесення певної інформації до професійної таємниці значно чіткіше регламентуються законодавчими актами,

зокрема, такими, як Закон України «Про адвокатуру та адвокатську діяльність» [20], Закон України «Про страхування» [37], Закон України «Про свободу совісті та релігійні організації» [36], Закон України «Про рахункову палату» [35], тому суб'єкт не може відносити до професійної таємниці будь-яку інформацію суто на власний розсуд.

В Україні налічується близько двадцяти видів професійної таємної інформації в залежності від професійної сфери діяльності. Наприклад, правовий режим журналістської таємниці встановлюється в Законі України «Про друковані засоби масової інформації (пресу) в Україні» [25]. Закон гарантує журналісту збереження таємниці авторства та джерел інформації, за винятком випадків, коли ці таємниці обнародуються на вимогу суду. Редакція та журналісти зобов'язані задовольняти прохання осіб, які надають інформацію щодо їх авторства або збереження таємниці авторства.

Правовий режим нотаріальної таємниці встановлюється Законом України «Про нотаріат» [30]. Нотаріус зобов'язаний зберігати в таємниці відомості, які стали відомі у зв'язку із професійною діяльністю.

Відповідно до Закону України «Основи законодавства України про охорону здоров'я» [17] до відомостей, які охороняються у правовому режимі лікарської таємниці, відносять інформацію, що стосується стану здоров'я, діагнозу, відомостей, отриманих при обстеженні та лікуванні, в т.ч. про самий факт звернення особи в медичний заклад.

Правовий режим таємниці усиновлення визначена ст. 226 Сімейного кодексу України [39], так як збереження таємниці усиновлення є запорукою успішного входження дитини в сім'ю на правах рідної.

### **1.3. Особливості охорони комерційної таємниці як виду конфіденційної інформації**

В сучасних умовах жорсткої конкуренції кожен розуміє як важливо зберігати і надійно охороняти інформацію, яка має комерційну цінність, адже її

втрата може призвести до різного роду збитків, а деколи навіть до банкрутства [83, с. 94].

Комерційна таємниця охоплює як інтереси суб'єктів господарювання, так і держави, і без відповідної системи правил та заходів, встановлених державою, неможливе існування цього інституту, а отже – й існування самої добросовісної конкуренції, добросовісних методів конкурентної боротьби. Адже конкуренція корисна для суспільства, коли вона вільна, чесна, добросовісна.

Ми вже зазначали вище, що сучасне законодавче визначення комерційної таємниці міститься в Цивільному кодексі України в статті 505 [45]. Зокрема п.1 ст. 36 Господарського кодексу України дає визначення комерційної таємниці, як відомостей, пов'язаних 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 [16].

Незважаючи на те, що інституту комерційної таємниці було приділено дуже багато уваги з боку науковців, ми вважаємо, що необхідно більш детально зупинитись на розкритті інституту охорони комерційної таємниці, тому що в Україні тільки починає зароджуватися механізм правової охорони цього інституту.

Авторське визначення поняття комерційної таємниці запропонувала О. Сергеева, яке вона сформулювала на основі аналізу досвіду західноєвропейських та американських правників. Як зазначає науковець, під комерційною таємницею слід розуміти інформацію конфіденційного характеру, яка безпосередньо пов'язана з підприємницькою діяльністю суб'єктів права на цю діяльність, як промислового (індустріального), так і торговельного характеру, або з діяльністю з надання послуг, що має реальну або потенційну економічну цінність та надає перевагу у конкурентній боротьбі через її невизначеність, а за розголошення якої настає юридична відповідальність та існує особливий режим її охорони [79, с. 17].

Е.Я. Соловйов вважає, що комерційна таємниця — це економічні інтереси та відомості про різні сфери виробничо-господарської, управлінської, науково-технічної, фінансової діяльності фірми, що навмисно приховуються з комерційних міркувань і охорона яких обумовлена інтересами конкуренції та можливою загрозою економічної діяльності фірми. Комерційна таємниця виникає тоді, коли вона є інтересом для комерції, Тоді як А.А. Фатьянов, вивчаючи сутність таємниць, надає визначення комерційної таємниці як науково-технічної, комерційної, організаційної та іншої інформації, що використовується в підприємницькій діяльності та має реальну або потенційну економічну цінність. [81, с. 307-308]

Для того щоб ми розуміли, яку інформацію відносити до комерційної таємниці, необхідно визначити ознаки.

За даними М.В. Ситницького, відомості, які можуть бути віднесені до комерційної таємниці, повинні мати наступні ознаки: 1) не містити державної таємниці; 2) не наносити шкоди інтересам суспільства; 3) відноситись до виробничої діяльності підприємства; 4) мати дієву або потенційну комерційну цінність та створювати переваги у конкурентній боротьбі; 5) мати обмеження у доступі [80, с. 264].

У свою чергу, Н.О. Попова розділяє ознаки комерційної таємниці на три групи: 1) ознаки, що стосуються властивостей об'єкту. Нематеріальність: комерційній таємниці властиві всі ознаки матеріального об'єкту – можливість одночасного використання різними особами, відсутність фізичної амортизації; має значення зміст нематеріального результату інтелектуальної діяльності, тобто сама інформація, яка становить комерційну таємницю, а не форма її зовнішнього представлення (на відміну від авторського права). Відповідно, об'єкт, який має цінність в силу своєї сутності, а не форми, може бути створений повторно, незалежно від першого, іншою особою. Тому для встановлення правової охорони необхідні спеціальні заходи з відокремлення об'єкту; 2) ознаки комерційної таємниці, що властиві їй, обумовлюють наступні умови надання об'єкту правової охорони: відсутність загальновідомості, потреби реєстрації об'єкту та його

оборотоздатність; 3) необмеженість строку захисту комерційної таємниці. Право особи на комерційну таємницю зберігається на весь час існування фактичної монополії цієї особи на інформацію, яка її складає, а також за наявності передбачених законом умов охорони. Комерційній таємниці властива також універсальність порівняно з іншими об'єктами виключних прав [76, с. 365].

До комерційної таємниці не потрібно відносити значну кількість відомостей, адже це може призвести до втрати клієнтів і зниження прибутку, оскільки умови ринку потребують постійних клієнтів, широкої інформації про діяльність підприємства.

На практиці комерційною таємницею підприємства можуть вважатися деякі аспекти його діяльності: формування цінової політики, рівень прибутку та плани розвитку підприємства, дані про контрагентів та укладені договори, маркетингові дослідження та аналітичні огляди ринку, власні розробки та винаходи, на які не оформлені патенти.

Суб'єктами права власності на комерційну таємницю, відповідно до діючого законодавства, є громадяни України, іноземці, підприємства усіх форм власності, установи, які здійснюють свою діяльність відповідно до законодавства України і визначають інформацію, яка становить їх комерційну таємницю.

Статтею 420 Цивільного кодексу України визначено, що комерційна таємниця є одним з об'єктів інтелектуальної власності [45]. Відповідно, майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не встановлено договором. Отже, право власності на комерційну таємницю виникає з моменту її класифікації у визначеному законом порядку і діє до закінчення терміну її засекречення або відчуження у встановленому законодавством порядку.

Як зазначає Н.Г. Карпенко [64], загальновизнаним є положення про те, що до комерційної таємниці не слід відносити фундаментальні наукові дослідження, оскільки вони не приносять прибутку. Якщо ж ці дослідження набувають прикладного значення, вони можуть класифікуватись в якості комерційної таємниці.

У певних випадках науково-технічну інформацію та ділову інформацію до якої відносяться професійні знання підприємця і працівника, технологічні знання фахівця і пропозиції зацікавлених суб'єктів відносно стану справ на ринку, недоцільно класифікувати як комерційну таємницю через великі матеріальні витрати на її захист, труднощі проведення охоронних заходів, а також у зв'язку з її використанням в рекламній діяльності, або для підвищення іміджу підприємства, так як до ділової інформації відносяться

З правової точки зору комерційна таємниця є засобом захисту від недобросовісної конкуренції в рамках реалізації права на інтелектуальну власність. Це загально визнане у світі положення впливає також із змісту пункту VIII статті 2 Конвенції про заснування Всесвітньої організації інтелектуальної власності 1967 року, що утверджувала Всесвітню організацію інтелектуальної власності [7].

Так порушенням комерційної таємниці вважаються:

- 1) необґрунтована відмова від надання відповідної інформації;
- 2) надання інформації, що не відповідає дійсності;
- 3) умисне приховування інформації;
- 4) розголошення державної або іншої таємниці, що охороняється законом, особою, яка повинна зберігати цю таємницю;
- 5) порушення порядку збереження.

Відповідно до ст. 162 Господарського кодексу України [16], суб'єкт господарювання, що є володільцем технічної, організаційної або іншої комерційної інформації, має право на захист від незаконного використання цієї інформації третіми особами, за умов, що ця інформація має комерційну цінність у зв'язку з тим, що вона невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а володільць інформації вживає належних заходів до охорони її конфіденційності. Строк правової охорони комерційної таємниці обмежується часом дії сукупності зазначених у частині першій цієї статті умов. Особа, яка протиправно використовує комерційну інформацію, що належить суб'єкту господарювання, зобов'язана відшкодувати завдані йому



такими діями збитки відповідно до закону. Особа, яка самостійно і добросовісно одержала інформацію, що є комерційною таємницею, має право використовувати цю інформацію на свій розсуд.

В інформаційному листі «Про деякі питання практики застосування господарськими судами законодавства про інформацію» від 28.03.2007 № 01-8/184 Вищого Господарського Суду України [49] згідно п.14 надається роз'яснення, що за порушення майнових прав інтелектуальної власності на комерційну таємницю чи право на «ноу-хау», зокрема, шляхом добування протиправним способом чужої комерційної інформації, розголошення її без згоди особи, уповноваженої на те, чи схилення до її розголошення або використання чужої комерційної інформації без згоди уповноваженої особи, власник цієї інформації має право на відшкодування завданих майнової та моральної шкоди відповідно до правил статей 1166 та 1167 Цивільного кодексу (435-15) [45]. Така цивільна відповідальність може наставати і в разі вчинення дій, зазначених у главі 4 Закону України «Про захист від недобросовісної конкуренції» (236/96-ВР) [27]. Проте не може бути застосовано відповідальності за збирання, розголошення чи використання відомостей, які не можуть належати до кола комерційної таємниці згідно з приписами постанови Кабінету Міністрів України від 09.08.1993 № 611 (911-93-п) «Про перелік відомостей, що не становлять комерційної таємниці» [34].

Юридична особа, яка зазнала втрати немайнового характеру, тобто була спричинена немайна шкода, має право на відшкодування моральної шкоди. Відповідно до п. 4 Постанови Пленуму Верховного Суду України від 25 травня 2001 № 5 «Про внесення змін та доповнень до постанови Пленуму Верховного Суду України від 31 березня 1995р. № 4 «Про судову практику в справах про відшкодування моральної (немайнової) шкоди» [47] під немайновою шкодою, заподіяною юридичній особі, слід розуміти втрати немайнового характеру, що настали у зв'язку з приниженням її ділової репутації, посяганням на фірмове найменування, товарний знак, виробничу марку, розголошенням комерційної

таємниці, а також вчиненням дій, спрямованих на зниження престижу чи підірив довіри до її діяльності.

Разом із терміном «комерційна таємниця» часто використовують і такий термін, як «ноу-хау».

Відповідно до п. 5 ч. 1 ст. 1 Закону України «Про державне регулювання діяльності у сфері трансферу технологій» [23] «ноу-хау» — це технічна, організаційна або комерційна інформація, що отримана завдяки досвіду та випробуванням технології та її складових, яка: не є загальновідомою чи легкодоступною на день укладення договору про трансфер технологій; є істотною, тобто важливою та корисною для виробництва продукції, технологічного процесу та/або надання послуг; є визначеною, тобто описаною достатньо вичерпно, щоб можливо було перевірити її відповідність критеріям незагальновідомості та істотності.

Існує питання щодо співвідношення понять «ноу-хау» та «комерційної таємниці». Так, на сьогоднішній день не існує єдиної думки стосовно цього приводу. Деякі вчені відносять «ноу-хау» до структури комерційної таємниці, як її елемент, інші ж натомість відокремлюють її.

Ноу-хау по своїй правовій природі — частина комерційної таємниці, що являє собою рішення у сфері техніки й технологій, які є результатом інтелектуальної або творчої діяльності людини та має практичне застосування. Саме така інформація може позначатися і як інформація, що становить комерційну таємницю, і як ноу-хау її володільця.

Досліджуючи спільні ознаки понять «ноу-хау» та комерційної таємниці, М.В. Нетеса визначає наступні: 1) результат інтелектуальної діяльності завжди має нематеріальний характер; 2) відсутність вільного доступу третіх осіб; 3) незагальновідомість інформації, що визначає її комерційну цінність; 4) конфіденційність інформації, яка складає її зміст; 5) відсутність вимоги абсолютної секретності [72, с. 146].

## РОЗДІЛ 2

# ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

### 2.1. Цивільно-правовий захист інформації з обмеженим доступом

Однією із нагальних проблем сьогодні є захист інформації з обмеженим доступом.

На нашу думку, основними елементами та складовими системи правового захисту інформації з обмеженим доступом є:

- 1) юридичне закріплення інформації з обмеженим доступом, в нормативних документах;
- 2) визначення інформації, яка підлягає захисту;
- 3) якісний підбір осіб, які будуть мати доступ до інформації з обмеженим доступом;
- 4) визначення порядку допуску та доступу до інформації з обмеженим доступом;
- 5) встановлення порядку збереження інформації з обмеженим доступом;
- 6) створення порядку поведінки з інформацією з обмеженим доступом.

Запорукою успішної боротьби з несанкціонованим доступом до інформації з обмеженим доступом є засоби захисту інформації, які використовуються для вирішення різних завдань із захистом інформації з обмеженим доступом, у тому числі попередження витоку і забезпечення безпеки цієї інформації.

Засоби забезпечення захисту інформації з обмеженим доступом можна поділити на групи:

- 1) Група технічних засобів захисту інформації поєднує апаратні і програмні засоби. Основні засоби: резервне копіювання і віддалене зберігання найбільш важливих масивів даних в комп'ютерній системі - на регулярній основі; дублювання і резервування всіх підсистем мереж, які мають значення для збереження даних; створення можливості перерозподіляти ресурси мережі в випадках порушення працездатності окремих елементів; забезпечення можливості

використовувати резервні системи електроживлення; забезпечення безпеки від пожежі або пошкодження обладнання водою; установка програмного забезпечення, яке забезпечує захист баз даних та іншої інформації від несанкціонованого доступу;

2) Організаційні засоби захисту інформації складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу) та організаційно-правових (національні законодавства і правила роботи, встановлені керівництвом конкретного підприємства). Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають широкі можливості модифікації і розвитку. Недоліки організаційних засобів - висока залежність від суб'єктивних факторів, у тому числі від загальної організації роботи із захисту інформації.

Найбільш чітко способи захисту прав на інформацію з обмеженим доступом визначені щодо комерційної таємниці.

Для підприємств одним із способів виживання в економічній боротьбі є забезпечення збереження комерційної таємниці, а тому забезпечення охорони від її розголошення – одне з пріоритетних завдань кожного суб'єкта господарювання.

Інформація, якою володіє підприємство є важливою для комерційного успіху і, одночасно, становить інтерес конкурентів. Наведемо кілька випадків, коли незахищеність комерційної таємниці призводить до негативних наслідків:

1) працівник після звільнення відкрив своє підприємство та почав здійснювати тотожну діяльність з використанням відомостей, отриманих за попереднім місцем роботи;

2) менеджер звільнився з роботи, а з собою забрав базу контактів клієнтської бази. Тепер всі конкуренти телефонують цим клієнтам, пропонуючи нижчі ціни;

3) інженер, який раніше працював на підприємстві, звільнившись, почав реалізовувати ідеї у нового роботодавця, які отримали технічне рішення на

підприємстві з якого звільнився інженер. Як результат – продукт уже не є унікальним.

Що характерно, відомості комерційного характеру є комерційною таємницею чи конфіденційною інформацією лише тоді, коли це підтверджено відповідними документально зафіксованими нормами власника підприємства. І перед тим, як стати до роботи, попередньо працівник обов'язково повинен бути ознайомлений з переліком такої інформації. Якщо не повідомити працівника про те, які саме відомості належать до комерційної таємниці, то, відповідно, він і не буде нести відповідальності за їх розголошення.

Щоб певна інформація належала до комерційної таємниці суб'єкта господарювання, останньому з метою використання своїх прав на комерційну таємницю та захисту від її розголошення необхідно оформити таку інформацію юридично.

Таким чином, необхідно розробити методи охорони, щоб запобігти в подальшому неправомірний комерційної таємниці. Для цього необхідно:

1) розробити на підприємстві положення про комерційну таємницю, в якому вказати наступні положення:

- а) перелік відомостей, що становлять комерційну таємницю;
- б) порядок захисту комерційної таємниці;
- в) механізм забезпечення доступу сторонніх осіб до комерційної інформації;
- г) відповідальність за розголошення відомостей, що становлять комерційну таємницю;
- г) порядок видачі працівникам документів, відомостей, передання інформації, яка становить комерційну таємницю підприємства, контрагентам, клієнтам і державним органам;
- д) правила доступу до інформації, яка є комерційною таємницею;
- е) конкретний строк, на який інформація набуває статусу комерційної таємниці, і порядок виключення інформації із складу комерційної таємниці тощо.

- 2) розробити інструкції щодо дотримання режиму нерозголошення комерційної таємниці;
- 3) розробити угоду про нерозголошення комерційної таємниці.

Положення про комерційну таємницю може стати одним з ефективних шляхів вирішення проблеми охорони конфіденційної інформації. Воно є локальним нормативним актом, який приймається на підприємстві та визначає об'єм інформації, яка становить комерційну таємницю, а також відображує порядок її використання, зберігання та поширення.

Сьогодні все більше на підприємствах з'являються необхідні важелі для того, щоб притягнути до відповідальності або примусити відшкодувати збиток співробітників, які порушили Положення про комерційну таємницю.

Правомірний володілець комерційної таємниці, права якого порушені, може звернутись до суду з цивільним позовом, вибравши один із загальних способів захисту, які передбачені ст. 16 Цивільного кодексу України [45].

Потерпілі від розголошення відомостей, що складають комерційну таємницю, найчастіше вибирають такий цивільно-правовий спосіб захисту, як відшкодування завданих збитків (п. 8 ч. 2 ст. 16 Цивільного кодексу України) [45] та /або компенсація моральної шкоди (п. 9 ч. 2 ст. 16 Цивільного кодексу України) [45], рідше звертаються з позовами про визнання незаконним розголошення відомостей, що становлять комерційну таємницю.

Як зазначено у п. 3 Роз'яснення Президії Вищого арбітражного суду України зі змінами від 01.02.2005р., при вирішенні спорів, пов'язаних з відшкодуванням моральної шкоди слід мати на увазі, що відповідно до статті 440-1 Цивільного кодексу України винна у заподіянні цієї шкоди особа може бути звільнена від обов'язку відшкодування тільки за умови, якщо вона доведе відсутність своєї вини (умислу або необережності). Таким чином, позивач повинен довести лише факт заподіяння йому моральної шкоди відповідачем, а не наявність у цьому вини останнього [48].

Розглядаючи судову практику, можна зробити висновок, що захист комерційної інформації має низький рівень ефективності в Україні в порівнянні з

країнами Європейського Союзу та США. Найбільшими проблемами при розгляді будь-якої справи такої категорії є питання доказів і доказування факту розголошення комерційної таємниці, визначення реального розміру нанесеної шкоди та притягнення працівника до матеріальної відповідальності.

Наприклад, Постановою Верховного Суду від 28.02.2019 р. у справі № 752/5775/16-ц залишено без задоволення касаційну скаргу у справі про притягнення до відповідальності за привласнення й неправомірне використання у власних цілях комерційної таємниці юридичної особи, оскільки не доведено факт розголошення й не надано доказів порушення відповідачем прав позивача, тобто позивач не довів у суді, що відповідач незаконно використовував комерційну таємницю позивача [46].

Щодо інституту комерційної таємниці, на думку О.О. Кулініч, існує необхідність у вирішенні таких питань, а саме: розроблення механізму здійснення права власності на інформацію, що становить комерційну таємницю; розроблення методу визначення її вартості; розроблення підстав для організаційно-правових заходів із питань захисту комерційної таємниці [68].

Ми в свою чергу підкреслюємо, що на ефективність охорони комерційної таємниці впливає:

- 1) належне документальне оформлення, тому умови про використання та захист комерційної таємниці бажано регулювати в договірному порядку не лише з працівниками, а й учасниками та контрагентами;
- 2) загальність, тобто необхідно відійти від типових «Зобов'язань про нерозголошення комерційної таємниці та конфіденційної інформації компанії», а слід підходити індивідуально і найбільше уваги приділити таким розділам, як перелік комерційної таємниці конкретно на підприємстві;
- 3) відповідальність, тому рекомендуємо прописати конкретну суму штрафу, як міру відповідальності, та розмежувати відповідальність за невиконання умов або вчинення дій, які призвели до розголошення інформації, і які не привели до наслідків у вигляді розголошення, але мали місце.

Потрібно звернути увагу на рівень захисту ноу-хау в Україні, адже він значно нижчий, у порівнянні з захистом інших видів інформації з обмеженим доступом. Таке становище зумовлено, передусім відсутністю спеціального закону, який би створював можливість для захисту «ноу-хау», реєстрації їх в Державному підприємстві «Український інститут інтелектуальної власності» та надання їм правової охорони не тільки засобами боротьби з недобросовісною конкуренцією, а й нормами закону. В законодавстві України не передбачена відповідальність за розголошення ноу-хау. У разі порушення прав на ноу-хау, відповідальність за порушення відбувається за загальними нормами, тобто, стаття 507 Цивільного кодексу України [45]. Захист прав власників ноу-хау можливий за допомогою договору про передачу ноу-хау іншим суб'єктам. Варто зазначити, що комерційна таємниця не може існувати поза підприємством, як тільки вона виходить за його межі та передається іншій особі, її передача здійснюється вже за інститутом ноу-хау. При цьому найчастіше передача прав на використання комерційної таємниці відбувається за ліцензійним договором про передачу ноу-хау.

Актуальним сьогодні залишається питання формування інституту ноу-хау в українському праві і його відмежування від комерційної таємниці.

Основа для вдосконалення правового визначення ноу-хау в Україні становить Угода про партнерство та співробітництво між Україною та Європейським Союзом від 15 червня 1994 року [44].

Так, відповідно до ч. 1 ст. 50 Угоди, «до інтелектуальної, промислової та комерційної власності входить захист нерозкритої інформації стосовно ноу-хау». Втім, ст. 420 Цивільного кодексу України [45] серед переліку об'єктів інтелектуальної власності не містить.

Таким чином, слід доповнити ст. 420 Цивільного кодексу України стосовно зазначення ноу-хау об'єктом інтелектуальної власності, а книгу 4 доповнити розділом щодо прав інтелектуальної власності на ноу-хау.

Чинне законодавство України, як було зазначено вище, не встановлює відповідальності за розголошення ноу-хау. В разі порушення прав захист відбувається відповідно до загальних принципів захисту цивільних прав, в той час



як порушення комерційної таємниці тягне за собою кримінальну, адміністративну і цивільно-правову.

Для чіткого розмежування двох наведених понять слід у главі 46 Цивільного кодексу України закріпити, що відомості, які складають комерційну таємницю, у цивільному обігу виступають, як ноу-хау, одночасно главу 75 Цивільного кодексу України доповнивши нормою про передачу ноу-хау.

Способи охорони банками інформації та відомостей, що становлять банківську таємницю, наведено у розділі 2 Правил зберігання, захисту, використання та розкриття банківської таємниці Постанови правління Національного Банку України № 267 від 14.07.2006р. [26].

Хотілось би зазначити, що серед недоліків правового механізму охорони банківської таємниці слід відзначити наступні: існують недоліки правової охорони банківської таємниці, в т.ч. і прогалин та протиріч у відповідному законодавстві; відсутній нормотворчий та правозастосовний досвід правової охорони банківської таємниці в Україні; латентний характер злочинів у сфері охорони банківської таємниці.

Шляхи подолання проблем правової охорони банківської таємниці ми вбачаємо в наступному: прийнятті відповідного закону, який би систематизував положення стосовно охорони банківської таємниці, її законодавчого визначення та гарантій захисту; визначенні на законодавчому рівні правових засад одержання, використання, поширення, зберігання та охорони інформації, яка становить банківську таємницю, з метою забезпечення прав фізичних та юридичних осіб на володіння, користування та розпорядження такою інформацією; систематизуванні законодавства у сфері охорони банківської інформації, розробленні єдиного підходу до охорони банківської таємниці та до визначення понятійного апарату в цій сфері.

Серед напрямів вдосконалення правового механізму захисту банківської таємниці слід відзначити наступні:

- 1) процес роботи банківських установ з персональними даними має врегульовуватися не лише шляхом прийняття локальних процедурних документів,

а й на державному рівні (зокрема, шляхом прийняття відповідного спільного документу Національним банком України та Державною службою України з питань захисту персональних даних).

2) вважаємо, що до законодавства України слід внести положення, які би покладали обов'язок зберігати і на такі фінансові установи, як: кредитні спілки; лізингові компанії; ломбарди; страхові компанії; довірчі товариства; установи накопичувального пенсійного забезпечення; інвестиційні фонди і компанії.

3) необхідно ухвалити підзаконний нормативно-правовий акт, у якому б визначалися більш детально вимоги до тексту запиту, порядку його складання, направлення, а також встановлювалася б відповідальність за перевищення працівниками Міністерства фінансів своїх повноважень при реалізації вказаного права, або передбачити ці вимоги у Законі «Про банки і банківську діяльність» [21].

Перейдемо до розгляду захисту персональних даних. Незважаючи на значну кількість нормативно-правових актів у цій сфері, якість правового забезпечення та правореалізації є незадовільною. Так, Конституція України має ряд обмежень діяльності, що пов'язана з інформаційними даними про особу та конфіденційною інформацією щодо особистого життя людини, хоча механізму, спроможного реалізовувати конституційні гарантії на практиці, не існує.

Законом України «Про захист персональних даних» встановлено положення про те, що обробка персональних даних може здійснюватись тільки відповідно до мети обробки, яка була сформульована при отриманні у суб'єкта персональних даних згоди на обробку даних. Кожного разу при зміні мети використання персональних даних, власник бази персональних даних зобов'язаний повторно звернутись до суб'єкта персональних даних за отриманням згоди на використання його персональних даних для нової мети. Однак, у Законі відсутні норми, які б деталізували і конкретизували його застосування для окремих категорій суб'єктів (страхові компанії, медичні установи, банки тощо) [82].

Збирання, зберігання використання та поширення конфіденційної інформації про особу без її згоди державою, органами місцевого самоврядування,

юридичними або фізичними особами визнається втручанням в її особисте та сімейне життя, яке допускається винятково, у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [86]. Пункт 20 Постанови Пленуму ВСУ №1 від 27.02.2009 акцентує увагу на тому, що судам слід ураховувати положення ч. 11 ст. 30 Закону України «Про інформацію», в якій зазначено, що інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист, що відповідає практиці застосування ЄСПЛ ст. 8 Конвенції [50].

Отже, перед тим як, персональна інформація про фізичну особу буде оброблятися, в тому числі поширюватися, відповідно до статті 11 Закону України «Про захист персональних даних» [28], необхідно отримати згоду або дозвіл від цієї особи на обробку її персональних даних. Проте сьогодні в умовах пандемії COVID-19 є виняток, що на період карантину та протягом 30 днів з дня його відміни дозволяється обробка персональних даних без згоди особи – їх власника. Дозволяється обробка даних, що стосуються стану здоров'я, місця госпіталізації або самоізоляції, прізвища, ім'я, по батькові, дати народження, місця проживання, роботи (навчання). Обробка дозволяється з метою протидії поширенню коронавірусної хвороби (COVID-19) [22].

Проблемним моментом, що потребує надійної системи захисту персональних даних в процесі їх обробки, є розміщення їх в мережі Інтернет. Оскільки персональні дані кожного з нас чи то медичного, чи фінансового характеру, не кажучи вже про ті, що ми використовуємо у своїх візитках, є або можуть бути об'єктом використання в автоматизованій системі обробки. Ми, користуючись Інтернетом, там залишаємо велику кількість своїх персональних даних. І використання наших даних нічим не обмежене і не врегульоване, тобто фактично такі дані залишаються не захищеними. І вони безперешкодно можуть використовуватись з метою впливу на наш вибір, чи то економічний, чи то

політичний - будь-який, можуть впливати на наші переконання і думки або використовуватись якимось іншим чином.

Перспективами вдосконалення найбільш «слабкої ланки» в системі обробки персональних даних – захисту – є: юридичне супроводження захисту персональних даних у мережі Internet, оскільки ця незахищеність сьогодні стає вагомим важелем впливу на діяльність суб'єктів персональних даних; чітка фіксація відповідальності володільців персональних даних у випадках, коли ці дані стають загальновідомими (через санкції, притягнення до відповідальності та інші) [61, с. 106-107].

Пропонуємо також вивести в окремий закон захист персональних даних неповнолітніх, тому що це більш вразливі дані. Діти потребують особливого захисту в питанні персональних даних, оскільки вони можуть бути менш обізнаними про відповідні ризики, наслідки та гарантії, а також про свої права щодо опрацювання персональних даних. В таких випадках необхідно отримувати згоду від тих осіб (наприклад, батьків, опікунів чи усиновителів), які повністю усвідомлюють значення дій та наслідків, які можуть статися під час обробки даних.

Представимо структуру Закону України «Про захист персональних даних неповнолітніх осіб»:

*Стаття 1. Сфера дії Закону.*

*Стаття 2. Визначення термінів.*

*Стаття 3. Законодавство України про захист персональних даних.*

*Стаття 4. Вимоги до обробки даних неповнолітніх осіб.*

*Стаття 5. Спеціальні вимоги до обробки даних неповнолітніх осіб.*

*Стаття 6. Обробка медичних даних неповнолітніх осіб.*

*Стаття 7. Суб'єкти, які мають право розпоряджатися персональними даними неповнолітніх осіб.*

*Стаття 8. Порядок зберігання персональних даних неповнолітніх осіб.*

*Стаття 9. Контроль за дотриманням законодавства про захист персональних даних неповнолітніх осіб.*

*Стаття 10. Забезпечення захисту персональних даних неповнолітніх осіб.*

*Стаття 11. Відповідальність за розголошення та розкриття даних неповнолітніх осіб.*

*Стаття 12. Прикінцеві положення.*

Що стосується професійних таємниць, то зараз окремі види інформації, яка становить професійну таємницю, регулюються правовими нормами різних галузей законодавства. Ці норми не завжди взаємоузгоджені та розпорошені по багатьох нормативно-правових актах, їх кількість має об'єктивну тенденцію до збільшення, оскільки зростає кількість напрямів та видів професійної діяльності. На нашу думку, потрібно згрупувати всі професійні таємниці в окремий закон.

## **2.2. Міжнародний досвід охорони інформації з обмеженим доступом**

Враховуючи інтеграційні прагнення України на сучасному етапі її розвитку, доцільно буде дослідити міжнародний досвід та досвід Європейського Союзу щодо правового регулювання відносин, пов'язаних із створенням, збиранням, зберіганням, використанням, поширенням та охороною інформації з обмеженим доступом.

Для Європейського Союзу, як унікального міжнародного утворення зі спільними інституціями держав-членів, першим пріоритетом є забезпечення власної інформаційної безпеки, внаслідок поширення та розвитку світового інформаційного простору.

Кожна демократична держава з метою забезпечення інформаційної безпеки формує спеціальну систему законів щодо захисту інформації, яка має спеціальний статус з обмеженим доступом. Наприклад, в усіх країнах-членах Європейського Союзу існують закони про обмеження доступу до певних видів інформації та їх охорону в контексті цивільного права, зокрема, в Чехії – Порядок доступу до інформації; в Естонії – Акт про суспільну інформацію; в Литві – Закон про умови передання інформації громадськості; в Латвії – Закон про свободу інформації [56, с. 130]. Аналогічно, в США правову основу забезпечення інформаційної

безпеки, завдяки якій можна скласти уявлення про загальну державну політику Сполучених Штатів Америки у сфері охорони інформації з обмеженим доступом, як пише О. Бусол [55, с. 93], становлять наступні закони: «Про охорону особистих таємниць» [89], «Про таємницю» (1974 р.) [97], «Про право на фінансову таємницю» (1978 р.) [98], «Про доступ до інформації про діяльність ЦРУ» (1984 р.) [74], «Про безпеку комп'ютерних систем» (1987 р.) [95], «Про свободу інформації» (1967 р.) [96].

В країнах Європейського Союзу, закони щодо регулювання доступу до інформації встановлюють рівень обмеження в залежності від того, який збиток може виникнути в результаті несанкціонованого доступу до такої інформації.

В цьому контексті варто звернути увагу на правове регулювання відносин щодо охорони комерційної таємниці і секретів виробництва в Європейському Союзі, як підвиду інформації, яка має обмежений доступ, адже на рівні Європейського Союзу законодавство про охорону окремих видів інформації з обмеженим доступом, як то комерційної таємниці, ноу-хау (секретів виробництва) не уніфіковано. Серед інших країн-членів Європейського Союзу тільки в Швеції прийнятий закон, повністю присвячений охороні секретів виробництва [52]. В інших країнах Європейського Союзу секрети виробництва та охорона комерційної таємниці регулюються окремими положеннями чи застосовуються загальні норми законодавства.

Охоронюваним результатом інтелектуальної діяльності комерційна таємниця (секрет виробництва) вважається в Італії, Великобританії, Латвії, Румунії, Словаччині, Словенії, Фінляндії, Франції.

В Німеччині та Австрії норми, що стосуються комерційної таємниці, зосереджені в законодавстві про недобросовісну конкуренцію, тоді як в Португалії охорона секретів виробництва міститься в Кодексі промислової власності, в якому прописано, що за розголошення секретів виробництва особою з використанням її службового становища кримінальним кодексом встановлюється відповідальність, до того ж при розголошенні секретів виробництва власник також має право вимагати відшкодування збитків. Аналогічно в Італії норми про

секрети виробництва містяться в Кодексі промислової власності. Також в Польщі основним нормативним актом, який регулює секрети виробництва, є Закон про недобросовісну конкуренцію, в якому прописані такі методи захисту, як припинення подальшої незаконної діяльності; усунення наслідків порушення; стягнення збитків або доходів порушника; публічне визнання відповідачем провини. В Румунії секретам виробництва присвячений Закон про протидію недобросовісної конкуренції, за яку передбачена цивільно-правова і кримінальна відповідальність за незаконні дії. У Франції захист ноу-хау встановлений Кодексом інтелектуальної власності, в якому прописано, що працівник за розголошення виробничого секрету може бути притягнутий до відповідальності у вигляді відшкодування збитків чи розірвання трудового договору [52].

Як зазначає Г. О. Андрощук, правова система Європейського Союзу надає охорону інформації, що становить комерційну таємницю, як охорону «ноу-хау», яка міститься в Європейській патентній конвенції. Патентне право Європейського Союзу створює додаткові стимули щодо використання режиму комерційної таємниці для охорони конфіденційної інформації, тому що в Європі патентна заявка оприлюднюється до видачі патенту, що надає конкурентам достатньо часу, щоб скопіювати технологію [52].

Необхідно зупинитися на Першій Директиві Ради 68/151/ЄЕС від 09.03.1968р. [12] щодо координації заходів безпеки, які для захисту інтересів членів та інших країн вимагаються країнами-членами від компаній у розумінні частини другої ст. 58 Договору з метою забезпечення рівнозначності таких заходів усередині Співтовариства [62, с. 88]. Статтею 2 Директиви визначено мінімальний перелік документів, які підлягають обов'язковому розкриттю (інакше кажучи, які не можна віднести до комерційної таємниці) [12].

У США охорона комерційної таємниці спочатку регулювалась загальним правом окремих штатів, проте сьогодні в більшості юрисдикцій США комерційна таємниця охороняється законами [59, с. 89]. 42 штати та Округ Колумбія прийняли ту чи іншу версію Уніфікованого Закону про комерційну таємницю (Uniform Trade Secrets Act) 1979 р. [99]. У Каліфорнії положення Закону включені

в Цивільний кодекс. Законодавчі положення доповнюються договірним захистом, який виступає додатковим [62, с. 20].

Потреба в міжнародній охороні прав інтелектуальної власності щороку тільки зростає, через недобросовісну конкуренцію. Основною міжнародною угодою, що регулює питання охорони прав, є Паризька конвенція 1883 року з охорони промислової власності [11]. Головною метою конвенції є саме створення пільгових умов для патентування винаходів, промислових зразків, реєстрації товарних знаків фірмами, організаціями і громадянами одних держав в інших.

Міжнародне-правове регулювання охорони персональних даних вперше знайшли своє закріплення, як складова права на приватність, в наступних міжнародних договорах з прав людини: Міжнародний Пакт про громадянські та політичні права 1966р. [10] та Конвенція про права дитини 1989р. [6]. Згідно статті 17 Міжнародного Пакту про громадянські та політичні права: «1. Ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію. 2. Кожна людина має право на захист закону від такого втручання чи таких посягань» [10].

В рамках ОЕСР було впроваджено «Керівні принципи зі захисту недоторканності приватного життя і транскордонних потоків персональних даних» (англ. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) [94], схвалені Рекомендацією Ради ОЕСР від 23 вересня 1980 р., нова редакція яких була ухвалена у 2013 р. Т.І. Обуховська відмічає, що дотримання принципів згідно документа ОЕСР на національному рівні передбачає такі обов'язки для держав-членів ОЕСР: прийняти належні національні закони; заохочувати і підтримувати саморегулювання шляхом прийняття кодексів поведінки/поводження або інших правил; забезпечити наявність розумних механізмів реалізації індивідуальних прав; застосувати необхідні санкції та інші засоби захисту персональних даних на випадок невиконання заходів, що



передбачені зазначеними принципами; забезпечити недискримінаційне ставлення до суб'єктів даних [73, с. 98].

Найбільш важливе питання в політиці інформаційної безпеки країн Європейського Союзу є охорона персональних даних, в якому вони керуються Генеральним регламентом про захист персональних даних 2016/679 (The General Data Protection Regulation 2016/679), який захищає фундаментальні права і свободи фізичних осіб, зокрема, їх право на захист персональних даних, а також встановлює нові вимоги щодо захисту персональних даних, які є обов'язковими для застосування у всіх державах-членах Європейського Союзу [13].

Регламентом Європейського Парламенту та Ради №45/2001 від 18.12.2000 р. про захист прав приватних осіб засновано новий незалежний інститут Європейського Уповноваженого (омбудсмена) із захисту персональних даних, основним завданням якого є забезпечення захисту персональних даних усіма союзними органами та інститутами [58].

До того, як був прийнятий Генеральний регламент про захист персональних даних 2016/679 [13], Європейський Союз досить тривало керувався положенням Директиви 95/46/ЄС «Про захист фізичних осіб у зв'язку з обробкою персональних даних і вільного обігу таких даних» [2]. Цей документ одночасно декларував бажання вільного руху інформації між державами-членами Європейського Союзу та забезпечував гарантії захисту основних прав громадян, які мають право на захист персональних даних та їх захист від третіх осіб. Директива зобов'язувала країну, яка входить до Європейського Союзу, прийняти свій власний закон про захист приватних відомостей.

Охорона персональних даних в Європейському Союзі забезпечується також Директивою 97/66/ЄС Європейського парламенту та Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі», якою закріплено конфіденційність зв'язку [3]. Впровадження в телекомунікаційних мережах нових цифрових систем в країнах-членах Європейського Союзу зумовлює певні вимоги щодо захисту інформації з

обмеженим доступом, тобто персональних даних користувачів та невторчання в особисте життя користувача.

Слід звернути увагу ще на такі нормативно-правові акти в Європейській системі законодавства про захист персональних даних: Конвенція Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28.01.1981 р. [8], у якій вперше викладено ключові принципи обробки персональних даних, права особи у зв'язку з обробкою її персональних даних, базові норми щодо транскордонної передачі даних та Додатковий протокол до конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 08.11.2001 р. [4], в якому деталізовані положення Конвенції в частині, що стосується транскордонної передачі даних, та містить нові положення щодо необхідності створення Сторонами Конвенції наглядового органу, який би здійснював контроль за додержанням законодавства про захист персональних даних [54, с. 16].

У Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» передбачено, що персональні дані мають зберігатися та використовуватися у визначених та законних цілях, бути точними та поновлюваними, допускати ідентифікацію фізичної особи [8]. Персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство країни не забезпечує відповідних гарантій [73].

Інститут охорони персональних даних в Європейському Союзі ґрунтується на принципах: законності персональних даних (застосування принципу законності в рішенні ЄСПЛ у справі «Ротару проти Румунії») [15]; визначеності мети обробки персональних даних; принципі адекватності, відповідності та ненадмірності (застосування принципу в рішенні ЄСПЛ у справі «Гардель проти Франції») [14]; достовірності та точності; чесності обробки персональних даних [54].

Зупинимося докладніше на практиці Європейського Суду з прав людини у сфері охорони персональних даних та наведемо декілька прикладів:

1) «K.H. and Others v. Slovakia» (заява № 32881/04, рішення від 06/11/2009) [90] - Ненадання лікарнею заявникам копій їх медичної документації. Порухення. Заявниці у позові стверджували про те, що їхні права, закріплені у ч. 1 ст. 6, ст. 8 та 13 Конвенції, були порушені через невиконання національними органами влади свого обов'язку щодо забезпечення доступу заявниць до копій їхньої медичної документації [9]. Основним контраргументом уряду проти вимоги позивачеві було те, що надання можливості фотокопій медичних документів дозволить зловживати інформацією вказаною на них, а надана судами можливість робити виписки, не розкриваючи іншу інформацію, яка не стосується предмета провадження у справі. Проте, ЄСПЛ у своєму рішенні зазначив наступне: «Суд дотримується думки, що такий позитивний обов'язок повинен бути розширений, зокрема у справах, подібних до тієї, що є предметом цього розгляду, коли йдеться про персональні дані, щоб уможливити виготовлення копій документів з персональними даними». За результатом розгляду справи, суд дійшов до висновку, порушені норми ч.1 ст. 6, ст. 8 Конвенції [9]. Відповідно до цього рішення персональні дані фізичної особи зазначені на документах можуть слугувати як доказ у суді для з'ясування всіх обставин. Вище наведене рішення ЄСПЛ є яскравим прикладом перешкоджання доступу фізичних осіб, дані яких опрацьовуються, до власних персональних даних в даному випадку це медичні документи;

2) «L.H. v. Latvia» (заява № 52019/07, рішення від 29/04/2014) [92] – Збір інформації контролюючим органом із метою оцінки якості наданої пацієнту медичної допомоги лікарнею. Відсутність легітимної мети збору персональних даних. Надмірний об'єм зібраної інформації. Неврахування інтересів пацієнта. Порухення. Щодо законності збору інформації про стан здоров'я заявниці Інспекцією, Інспекція мала право на збір інформації за зверненням установи (не лише за скаргами, як то наголошував заявник). Досліджуючи питання необхідності збору інформації щодо заявниці ЄСПЛ зазначив про таке: збір

інформації розпочався через сім років після надання медичних послуг, відтак сумнівно, що він здійснювався «в цілях лікування або організації надання медичних послуг». Відтак, втручання не було законним і не містило достатніх гарантій проти свавілля. Заявника не повідомляли, що на прикладі його справи здійснюється оцінка надання допомоги (так стверджував Уряд, натомість заявник говорив, що єдина мета – це надання доказів у справі). Жодних рекомендацій лікарні не надавали за результатами перевірки. Звіт стосувався дій одного з лікарів і був наданий якраз під час судового провадження щодо лікарні. Втручання не було законним і не містило достатніх гарантій проти свавілля.

3) «Z. v. Finland» (заява № 22009/93, рішення від 25/02/1997) [100] – Недостатність строків, впродовж яких обмежувався доступ до рішення суду, що містив чутливу інформацію про заявницю. У справі було порушено використання медичних даних позивачки (вона була ВІЛ-позитивною особою і ця інформація належить до «чутливих даних»), під час кримінального провадження проти її чоловіка (також ВІЛ-позитивного), обвинуваченого в убивстві та свідомому підданню ризику зараження жінок вірусом імунодефіциту. Було розголошені «чутливі дані» позивачки під час судових засідань, а пізніше у засобах масової інформації, тому що спочатку лікарі позивачки були змушені свідчити щодо її стану здоров'я, а згодом правоохоронні органи вилучили медичні документи позивачки із закладів охорони здоров'я (біологічні тести). Суд вирішив, що порушення права на приватність (за ст. 8 Європейської конвенції з прав людини [9]) щодо свідчення в суді чи вилучення даних правоохоронними органами не відбулося; однак загальне оприлюднення даних позивачки, як і публікація імені та прізвища позивачки, включно з її діагнозом у рішенні Апеляційного суду міста Хельсінкі порушують її право на приватність, вирішив справу на користь позивачки;

4) «S. and Marper v. The United Kingdom» (заяви № 30562/04 і 30566/04, рішення від 04/12/2008) [93] – Законність збору та зберігання працівниками поліції відбитків пальців, профілів та зразків ДНК затриманих, підозрюваних тощо. Посилаючись на статтю 8 Конвенції [9], заявники скаржились до Суду на

зберігання їхніх відбитків пальців, зразків клітин та профілів ДНК згідно з пунктом 1А статті 64 Акту про поліцію та докази у кримінальних справах 1984 року. Суд прийшов к висновку, щодо відсутності достатньо чіткої мети збору інформації, відсутності необхідності у зборі такого великого об'єму даних у порівнянні з отримуваними перевагами, неврахування індивідуальних обставин осіб, чії дані зберігалися. Отже, у справі було допущено порушення вимог статті 8 Конвенції про захист прав людини і основоположних свобод (рішення прийнято одноголосно) [9].

У країнах Європейського Союзу для того, щоб не було випадків розкрадання персональних даних громадян, комерційної таємниці та іншої секретної інформації в кіберпросторі, значна увага приділяється також проблемам кібербезпеки. Вона спрямована на збереження доступності та цілісності мереж, а також конфіденційної інформації. 13 вересня 2017 р. Європейська комісія представила документ під назвою «Стійкість, стримування та захист: створення сильної кібербезпеки для ЄС», в якому зазначено, що невживання заходів по забезпеченню кібербезпеки є великим ризиком витоку інформації з обмеженим доступом, яка становить комерційну таємницю, персональну інформацію та іншу вкрай секретну інформацію, розголошення якої може вплинути на безпеку країн Європейського Союзу [57, с. 31].

Якщо в державах-членах Європейського Союзу створений досить розгалужений інституційний механізм із охорони персональних даних, то в Україні інститут охорони персональних даних є досить молодим у правовому значенні та потребує подальшого удосконалення та розвитку.

За даними С.С. Єсімова, у Бельгії банківська таємниця визначена як професійна таємниця. Її порушення не передбачає кримінального покарання, а тільки цивільно-правове. Водночас бельгійське законодавство встановлює окремі гарантії нерозголошення банківської інформації третім особам (зокрема, податковим органам), які нівелюються винятками, встановленими окремими законами [63, с. 51].

Італія сформувала національне законодавство щодо банківської таємниці на підставі директив Європейського Союзу та існуючих у банківській системі традицій та адміністративної практики судів і численних правил, встановлених банками [63, с. 52].

В Іспанії Закон “Про банки” покладає на банки обов’язок зберігати в таємниці дані і операції своїх клієнтів, прирівнюючи банківську таємницю до таємниці особистого та сімейного життя [91]. Механізм забезпечення банківської таємниці ґрунтується на підставі укладених контрактів із введенням положень, сформованих на практиці до вступу у законну силу Закону “Про банки” [91].

Португалія декретом № 298, прийнятим у 1992 р., визначила банківську таємницю як професійне зобов’язання працівників фінансових установ, які надають послуги на постійній або тимчасовій основі, не публікувати або використовувати інформацію, що стосується діяльності кредитних інститутів та їх взаємовідносин з клієнтами. Імена клієнтів, рахунки і рух за рахунками знаходяться під захистом професійної таємниці. Закон передбачає розкриття інформації третім особам, зокрема правоохоронним органам [88].

Отже, кожна країна з розглянутих має окремий нормативно-правовий акт, який чітко регулює охорону банківської таємниці.

## ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Здійснивши дослідження охорони інформації з обмеженим доступом на підставі викладеного в випускній кваліфікаційній роботі матеріалу, можна зробити такі висновки:

1. Встановлено, що інформація з обмеженим доступом як об'єкт цивільно-правових відносин - це здатні бути предметом майнових чи особистих немайнових відносин, відомі лише певному колу осіб і наділені в силу цього особливою цінністю відомості, дані та знання, по відношенню до яких володільцем здійснюються заходи, спрямовані на обмеження вільного доступу третіх осіб, поширення яких може завдати істотної шкоди зацікавленим особам.

Інформація з обмеженим доступом є одним із видів інформації, яка призначена для певного кола суб'єктів і складають знання, що мають особливу цінність та щодо яких уживаються заходи, спрямовані на обмеження вільного доступу третіх осіб, поширення яких може заподіяти істотну шкоду володільцю інформації.

2. Виявлено, що інформація з обмеженим доступом повинна мати наступні ознаки: 1) зміст інформації з обмеженим доступом складають знання, повідомлення, відомості про соціальну форму руху матерії і про всі інші її форми у тій мірі, у якій вони використовуються суспільством, державою; 2) відомості, що складають зміст інформації з обмеженим доступом, за своєю сутністю ідеальні (нематеріальні); 3) інформація з обмеженим доступом є самостійним об'єктом правового регулювання, що не залежить від конкретної форми її матеріального носія; 4) інформація з обмеженим доступом не є загальнодоступною; 5) може виступати об'єктом інтелектуальної власності; 6) захисту підлягає лише задокументована інформація (відтворена на фізичних носіях).

3. Обґрунтовано, що кожен вид інформації з обмеженим доступом має свої особливості цивільно-правової охорони в залежності від суб'єкта відносин, що виникають з приводу інформації та вимог чинного законодавства, що висуваються до обігу певного виду інформації.

4. Аргументовано, що секретність певної інформації може сприяти досягненню максимального прибутку, а комерційну таємницю доцільно охороняти як ті відомості підприємства, які дозволяють підвищити конкурентоспроможність його товарів та послуг на ринку. Заходи з охорони комерційної таємниці викладені у Главі 46 ЦК України.

5. Обґрунтовано, що для забезпечення ефективного контролю та визначення санкціонованого механізму доступу до інформації з обмеженим доступом виникає потреба у прийнятті окремого Закону «Про порядок доступу та захист інформації з обмеженим доступом», в якому будуть окремо висвітлюватися питання надання доступу, використання інформації з обмеженим доступом, контрзаходи від несанкціонованого доступу до інформації, види інформації з обмеженим доступом та інше

6. В умовах адаптації українського законодавства до законодавства Європейського Союзу, Україна має привести національне законодавство стосовно правового регулювання щодо охорони інформації з обмеженим доступом у відповідність з міжнародними стандартами Європейського Союзу.

З метою удосконалення чинного законодавства України з питань охорони інформації з обмеженим доступом пропонується внести наступні **зміни та доповнення** до нормативно-правових актів України, а саме:

- закріпити в Законі України «Про інформацію» поняття інформація з обмеженим доступом, виклавши його в наступній редакції: «інформація з обмеженим доступом – сукупність відомостей, даних, знань, які відтворені на фізичних предметах (флеш-накопичувачах, комп'ютерах та ін.) або в хмарних сховищах, що можуть запам'ятовувати та зберігати інформацію, та мають особливу цінність для окремих суб'єктів-володільців цієї інформації, ризик витоку такої інформації загрожує завдати істотної шкоди цим суб'єктам;
- доповнити перелік об'єктів права інтелектуальної власності, закріплений у ст. 420 Цивільного кодексу України, таким об'єктом, як ноу-хау;
- викласти назву глави 46 книги 4 Цивільного кодексу України в такій редакції: «Право інтелектуальної власності на комерційну таємницю та ноу-хау»;



- доповнити частину 6 статті 6 Закону України «Про захист персональних даних» абзацом такого змісту: «З метою запобігання епідемічним та іншим інфекційним хворобам, а також масовим неінфекційним захворюванням (отруєнням) і боротьби з ними, дозволяється обробка персональних даних без згоди суб'єкта персональних даних, якщо дії або бездіяльність суб'єкта персональних даних спричинили або завідомо могли спричинити поширення цих захворювань. Дозволяється обробка даних, що стосуються стану здоров'я, місця госпіталізації або самоізоляції, прізвища, ім'я, по батькові, дати народження, місця проживання, роботи (навчання)».

- прийняти окремий Закон України «Про захист персональних даних неповнолітніх осіб», структура якого запропонована в роботі.

Зазначені пропозиції можуть бути імплементовані до законодавства.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996 № 30. Ст. 141.
2. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» : Директива від 24.10.1995 р. № 994\_242. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 24.10.1995. URL: [https://zakon.rada.gov.ua/laws/show/994\\_242](https://zakon.rada.gov.ua/laws/show/994_242) (дата звернення: 15.09.2020).
3. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» : Директива від 15.12.1997 р. № 994\_243. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 15.12.1997. URL: [https://zakon.rada.gov.ua/laws/show/994\\_243](https://zakon.rada.gov.ua/laws/show/994_243) (дата звернення: 15.09.2020).
4. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 08.11.2001 р. № ETS N 181. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 06.07.2010. URL: [https://zakon.rada.gov.ua/laws/show/994\\_363#Text](https://zakon.rada.gov.ua/laws/show/994_363#Text) (дата звернення: 14.09.2020).
5. Загальна декларація прав людини (рос/укр) : Декларація від 10.12.1948 р. *Законодавство України* : база даних / Верхов. Рада України. URL: [https://zakon.rada.gov.ua/laws/show/995\\_015#Text](https://zakon.rada.gov.ua/laws/show/995_015#Text) (дата звернення: 03.10.2020).
6. Конвенція ООН про права дитини від 20.11.1989р. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 20.11.2014. URL: [https://zakon.rada.gov.ua/laws/show/995\\_021#Text](https://zakon.rada.gov.ua/laws/show/995_021#Text) (дата звернення: 15.09.2020).
7. Конвенція про заснування Всесвітньої організації інтелектуальної власності : Конвенція від 14.07.1967 № 995\_169. *Законодавство України* : база даних / Верхов. Рада України. Дата набрання чинності для України міжнародного

договору : 26.04.1970. URL: [https://zakon.rada.gov.ua/laws/show/995\\_169#Text](https://zakon.rada.gov.ua/laws/show/995_169#Text) (дата звернення: 19.09.2020).

8. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р. № 108. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 06.07.2010. URL: [https://zakon.rada.gov.ua/laws/show/994\\_326#Text](https://zakon.rada.gov.ua/laws/show/994_326#Text) (дата звернення: 14.09.2020).

9. Конвенція про захист прав і основоположних свобод від 04.11.1950 р. № ETS № 005. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 02.10.2013. URL: [https://zakon.rada.gov.ua/laws/show/995\\_004#Text](https://zakon.rada.gov.ua/laws/show/995_004#Text) (дата звернення: 14.09.2020).

10. Міжнародний пакт про громадянські і політичні права. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 19.10.1973. URL: [https://zakon.rada.gov.ua/laws/show/995\\_043#Text](https://zakon.rada.gov.ua/laws/show/995_043#Text) (дата звернення: 15.09.2020).

11. Паризька конвенція про охорону промислової власності від 20 березня 1883 року (укр/рос) : Конвенція від 20.03.1883 р. *Законодавство України* : база даних / Верхов. Рада України. URL: [https://zakon.rada.gov.ua/laws/show/995\\_123#Text](https://zakon.rada.gov.ua/laws/show/995_123#Text) (дата звернення: 01.10.2020).

12. Перша Директива Ради Європейських Співтовариств № 68/151/ЄЕС Ради : «Про координацію гарантій (застережних заходів), які вимагаються країнами-членами від компаній в рамках контексту другого абзацу Статті 58 Договору для захисту інтересів членів та інших з перспективою зробити такі гарантії однаковими в усьому Співтоваристві» : Директива від 09.03.1968 р. № 994\_453. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 09.03.1968. URL: [https://zakon.rada.gov.ua/laws/show/994\\_453#Text](https://zakon.rada.gov.ua/laws/show/994_453#Text) (дата звернення: 17.09.2020).

13. Регламент Європейського парламенту і ради (ЄС) 2016/679 : Регламент від 27.04.2016 р. № 984\_008-16. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 24.05.2016. URL: [https://zakon.rada.gov.ua/laws/show/984\\_008-16](https://zakon.rada.gov.ua/laws/show/984_008-16) (дата звернення: 15.09.2020).

14. Рішення у справі «Гардель проти Франції» (Gardel v. France), заява № 16428/05, пункт 62, ЄСПЛ 2009 : *European Court of Human Rights* URL: <https://www.legal-tools.org/doc/315a62/pdf/> (дата звернення: 15.09.2020).

15. Рішення у справі «Ротару проти Румунії» (Rotaru v. Romania) [ВП], заява № 28341 /95, п. 43, ЕЧПР 2000-V : *European Court of Human Rights* URL: [https://zakon.rada.gov.ua/laws/show/994\\_363#Text](https://zakon.rada.gov.ua/laws/show/994_363#Text) (дата звернення: 15.09.2020).

16. Господарський кодекс України : Закон України від 16.01.2003 р. № 436-IV. *Відомості Верховної Ради України*. 2003. № 19-20. Ст. 144.

17. Основи законодавства України про охорону здоров'я : Закон України від 19.11.1992 р. № 2801-XII. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 24.07.2020. URL: <https://zakon.rada.gov.ua/laws/show/2801-12#Text> (дата звернення: 15.09.2020).

18. Перелік національного законодавства, щодо захисту персональних даних. *Уповноважений Верховної Ради України з прав людини*. URL: <http://www.ombudsman.gov.ua/ua/page/zpd/zakonodavstvo/naczionalne-zakonodavstvo/> (дата звернення: 14.09.2020).

19. Про авторське право і суміжні права : Закон України від 23.12.1993 р. № 3792-XII. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 04.11.2018. URL: <https://zakon.rada.gov.ua/laws/show/3792-12#Text> (дата звернення: 15.09.2020).

20. Про адвокатуру та адвокатську діяльність : Закон України від 05.07.2012 р. № 5076-VII. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 03.07.2020. URL: <https://zakon.rada.gov.ua/laws/show/5076-17> (дата звернення: 14.09.2020).

21. Про банки і банківську діяльність : Закон України від 07.12.2000 р. № 2121-III. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 03.07.2020. URL: <https://zakon.rada.gov.ua/laws/main/2121-14> (дата звернення: 14.09.2020).

22. Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби

(COVID-19) : Закон України від 13.04.2020 р. № 555-IX. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 18.04.2020. URL: <https://zakon.rada.gov.ua/laws/show/555-20#Text> (дата звернення: 03.10.2020).

23. Про державне регулювання діяльності у сфері трансферу технологій : Закон України від 14.09.2006 р. № 143-V. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 09.12.2015. URL: <https://zakon.rada.gov.ua/laws/show/143-16#Text> (дата звернення: 19.09.2020).

24. Про доступ до публічної інформації : Закон України від 13.01.11 р. № 2939-VI. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 15.08.2020. URL: <https://zakon.rada.gov.ua/laws/main/2939-17> (дата звернення: 14.09.2020).

25. Про друковані засоби масової інформації (пресу) в Україні від 16.11.1992 р., № 2782-XII. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 03.07.2020. URL: <https://zakon.rada.gov.ua/laws/show/2782-12#Text> (дата звернення: 14.09.2020).

26. Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці : Постанова Правління Національного Банку України від 14.07.2006 р. № 267. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 01.04.2020. URL: <https://zakon.rada.gov.ua/laws/show/z0935-06#Text> (дата звернення: 01.10.2020).

27. Про захист від недобросовісної конкуренції : Закон України від 07.06.1996 р. № 236/96-ВР. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 11.12.2019. URL: <https://zakon.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80#Text> (дата звернення: 19.09.2020).

28. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 04.03.2020. URL: <https://zakon.rada.gov.ua/laws/main/2297-17> (дата звернення: 14.09.2020).

29. Про інформацію : Закон України від 02.10.92 р. № 2657-ХІІ. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 16.07.2020. URL: <https://zakon.rada.gov.ua/laws/main/2657-12> (дата звернення: 14.09.2020).

30. Про нотаріат : Закон України від 02.09.1993 р. № 3425-ХІІ. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 08.08.2020. URL: <https://zakon.rada.gov.ua/laws/show/3425-12#Text> (дата звернення: 15.09.2020).

31. Про охорону прав на винаходи і корисні моделі : Закон України від 15.12.1993 р. № 3687-ХІІ. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 16.08.2020. URL: <https://zakon.rada.gov.ua/laws/show/3687-12#Text> (дата звернення: 15.09.2020).

32. Про охорону прав на знаки для товарів і послуг : Закон України від 15.12.1993 р. № 3689-ХІІ. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 16.08.2020. URL: <https://zakon.rada.gov.ua/laws/show/3689-12#Text> (дата звернення: 15.09.2020).

33. Про охорону прав на промислові зразки : Закон України від 15.12.1993 р. № 3688-ХІІ. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 16.08.2020. URL: <https://zakon.rada.gov.ua/laws/show/3688-12#Text> (дата звернення: 15.09.2020).

34. Про перелік відомостей, що не становлять комерційної таємниці : Постанова Кабінету Міністрів України від 09 серпня 1993р. № 611. *Законодавство України* : база даних / Верхов. Рада України. URL: <https://zakon.rada.gov.ua/laws/show/611-93-%D0%BF#Text> (дата звернення: 15.09.2020).

35. Про рахункову палату : Закон України від 02.07.2015 р. № 576-VIII. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 03.07.2020. URL: <https://zakon.rada.gov.ua/laws/show/576-19> (дата звернення: 14.09.2020).

36. Про свободу совісті та релігійні організації : Закон України від 23.04.1991 р. № 988-ХІІ. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 20.11.2020. URL: <https://zakon.rada.gov.ua/laws/show/987-12#Text> (дата звернення: 20.11.2020).

37. Про страхування : Закон України від 07.03.1996 р. № 85/96-ВР. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 03.07.2020. URL: <https://zakon.rada.gov.ua/laws/main/85/96-%D0%B2%D1%80> (дата звернення: 14.09.2020).

38. Про цінні папери та фондовий ринок : Закон України від 23.02.2006 р. № 3480-ІV. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 24.09.2020. URL: <https://zakon.rada.gov.ua/laws/show/3480-15#Text> (дата звернення: 14.11.2020).

39. Сімейний кодекс України : Закон України від 10.01.2002 р. № 2947-ІІІ. *Відомості Верховної Ради України*. 2002. № 21-22. Ст. 135.

40. Угода між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону інформації з обмеженим доступом : Угода від 05.06.2003 р. № 440\_038. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 07.07.2004. URL: [https://zakon.rada.gov.ua/laws/show/440\\_038](https://zakon.rada.gov.ua/laws/show/440_038) (дата звернення: 14.09.2020).

41. Угода між Кабінетом Міністрів України та Урядом Румунії про взаємну охорону інформації з обмеженим доступом : Угода від 22.10.2013 р. № 642\_061. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 01.10.2015. URL: [https://zakon.rada.gov.ua/laws/show/642\\_061](https://zakon.rada.gov.ua/laws/show/642_061) (дата звернення: 14.09.2020).

42. Угода між Кабінетом Міністрів України та Урядом Словацької Республіки про взаємну охорону інформації з обмеженим доступом : Угода від 22.06.2006 р. № 703\_069. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 01.12.2008. URL: [https://zakon.rada.gov.ua/laws/show/703\\_069](https://zakon.rada.gov.ua/laws/show/703_069) (дата звернення: 14.09.2020).

43. Угода між Україною та Угорською Республікою про взаємну охорону інформації з обмеженим доступом : Угода від 15.11.2006 р. № 348\_073. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 06.03.2008. URL: [https://zakon.rada.gov.ua/laws/show/348\\_073](https://zakon.rada.gov.ua/laws/show/348_073) (дата звернення: 14.09.2020).

44. Угода про партнерство і співробітництво між Україною і Європейськими Співтовариствами та їх державами-членами : Угода від 14.06.1994 р. № 998\_012. *Законодавство України* : база даних / Верхов. Рада України. Дата оновлення: 01.09.2017. URL: [https://zakon.rada.gov.ua/laws/show/998\\_012#Text](https://zakon.rada.gov.ua/laws/show/998_012#Text) (дата звернення: 04.10.2020).

45. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435-IV. *Відомості Верховної Ради України*. 2003. № 40-44. Ст. 356. (19).

46. Постанова Верховного Суду від 28.02.2019 р. у справі № 752/5775/16-ц : Постанова Верховного Суду від 28.02.2019 URL: <https://www.uacourt.openregister.info/tsyvilni-spravy-do-01-01-2019-1000/pozovne-provazhennya-1042/spory-pro-pravo-intelektualnoyi-vlasnosti-1057/spory-pro-pravo-intelektualnoyi-vlasnosti-spory-pro-avtorske-pravo-1058?document=67084831> (дата звернення: 17.11.2020).

47. Про внесення змін та доповнень до постанови Пленуму Верховного Суду України від 31 березня 1995 р. N 4 «Про судову практику в справах про відшкодування моральної (немайнової) шкоди» : Постанова Пленуму Верховного Суду України від 25.05.2001 № 5. *Законодавство України* : база даних / Верхов. Рада України. URL: <https://zakon.rada.gov.ua/laws/show/v0005700-01#Text> (дата звернення: 19.09.2020).

48. Про деякі питання практики вирішення спорів, пов'язаних з відшкодуванням моральної шкоди: Роз'яснення Президії Вищого арбітражного суду України від 29.02.1996 р. № 02-5/95. *Збірник рішень та арбітражної практики Вищого арбітражного суду України*. 1996. №2. С. 95-97.

49. Про деякі питання практики застосування господарськими судами законодавства про інформацію : Інформаційний лист Вищого Господарського



Суду України від 28.03.2007 р. № 01-8/184. *Законодавство України* : база даних / Верхов. Рада України. URL: [https://zakon.rada.gov.ua/laws/show/v\\_184600-07#Text](https://zakon.rada.gov.ua/laws/show/v_184600-07#Text) (дата звернення: 19.09.2020).

50. Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи : Постанова Пленуму Верховного Суду України від 27 лютого 2009 року № 1. *Законодавство України* : база даних / Верхов. Рада України. URL: [https://zakon.rada.gov.ua/laws/show/v\\_001700-09#Text](https://zakon.rada.gov.ua/laws/show/v_001700-09#Text) (дата звернення: 01.10.2020).

51. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 р., № 2-рп/2012 *Законодавство України* : база даних / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text> (дата звернення: 14.09.2020).

52. Андрощук Г. О. Правова охорона комерційної таємниці в країнах Європейського Союзу. Теорія і практика інтелектуальної власності. 2012. Вип. 6. С. 49–58. URL: [http://nbuv.gov.ua/UJRN/Triv\\_2012\\_6\\_9](http://nbuv.gov.ua/UJRN/Triv_2012_6_9) (дата звернення: 15.09.2020).

53. Баскаков В. Ю. Захист інформації з обмеженим доступом: розвиток вітчизняного законодавства *GOAL* : стаття Глобальної організації союзницького лідерства за 2011 р. URL: <http://goal-int.org/zaxist-informacii-z-obmezhenim-dostupom-rozvitok-vitchiznyanogo-zakonodavstva/> (дата звернення: 14.09.2020).

54. Бем М. В., Городинський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник / за ред. М. В. Бен. Київ: К.І.С, 2015. 220 с.

55. Бусол О. Ю. Тенденції нормативно-правового забезпечення інформаційної безпеки США. URL: [http://nbuv.gov.ua/UJRN/nprnbuimviv\\_2017\\_46\\_8](http://nbuv.gov.ua/UJRN/nprnbuimviv_2017_46_8) (дата звернення: 15.09.2020).

56. Василенко Д. П. Законодавство провідних країн світу у сфері захисту інформації. *Вісник КДУ імені Михайла Остроградського*. 2010. Вип. 2 (61). Ч. 1. С. 128-132. URL: [http://www.kdu.edu.ua/statti/2010-2-1\(61\)/128.PDF](http://www.kdu.edu.ua/statti/2010-2-1(61)/128.PDF) (дата звернення: 15.09.2020).

57. Войціховський А. В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права*. 2018. Вип. 53. С. 26-37. URL: <http://univd.edu.ua/science-issue/issue/3019> (дата звернення: 15.09.2020).

58. Головченко В. В. Правові основи захисту персональних даних. *Юридична газета online*. : всеукр. щотиж. проф. юр. видання 2018. Вип. 36 (638). URL: <https://yur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnih-danih.html> (дата звернення: 03.04.2020).

59. Гороховська О. В., Семенюк І. С. Захист комерційної таємниці в міжнародному праві та законодавстві зарубіжних країн. URL: [http://nbuv.gov.ua/UJRN/drp\\_2016\\_1\\_18](http://nbuv.gov.ua/UJRN/drp_2016_1_18) (дата звернення: 16.09.2020).

60. Гриценко В. Г. Щодо питання про поняття, ознаки та класифікацію конфіденційної інформації. *Юридичний вісник*. 2014. № 4. С. 191-194. URL: [http://nbuv.gov.ua/UJRN/urid\\_2014\\_4\\_41](http://nbuv.gov.ua/UJRN/urid_2014_4_41) (дата звернення: 14.09.2020).

61. Гронь О. В. Проблеми захисту персональних даних у контексті сучасної комунікації. *Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство*. 2018. № 19(1). С. 102-108.

62. Дорошев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно “Критериев оценки надежных компьютерных систем TCSEC (Trusted Computer Systems Evaluation Criteria)”, США, “Оранжевая книга” / за ред. В. В. Дорошев, В. В. Домарев. Бизнес и безопасность, 1998. № 1. С. 19–21.

63. Єсімов С. С. Банківська таємниця у країнах ЄС та адаптація національного законодавства у контексті інформаційного права.

URL: <http://sphhcj.nuph.edu.ua/index.php/2415-3818/article/view/89907/85318>  
(дата звернення: 17.09.2020).

64. Карпенко Н. Г. Комерційна таємниця – визнання, захист, відповідальність. URL: [http://www.economy.nauka.com.ua/pdf/5\\_2020/67.pdf](http://www.economy.nauka.com.ua/pdf/5_2020/67.pdf) (дата звернення: 19.09.2020).

65. Колобов Л., Колеснікова І. Комерційна таємниця та питання захисту комерційної таємниці URL: <http://pgr-journal.kiev.ua/archive/2016/05/3.pdf> (дата звернення: 15.09.2020).

66. Кохановська О. В. Цивільно-правові проблеми інформаційних відносин в Україні : Дисертація на здобуття наукового ступеня доктора юридичних наук : 12.00.03. цивільне право і цивільний процес; сімейне право; міжнародне приватне право. Київський національний університет імені Тараса Шевченка, Київ, 2006. 531 с.

67. Коц Д. В. Теоретико-правові засади інформації з обмеженим доступом. URL: [https://ela.kpi.ua/bitstream/123456789/32676/1/VPSP2019-2\\_107-111.pdf](https://ela.kpi.ua/bitstream/123456789/32676/1/VPSP2019-2_107-111.pdf) (дата звернення: 14.09.2020).

68. Кулініч О. О. Інформація з обмеженим доступом як об'єкт цивільних прав : автореф. дис. ... канд. юрид. наук : 12.00.03. Одеська нац. юрид. акад. Одеса, 2006. 20 с.

69. Курман О. В. Відомості, що становлять комерційну таємницю, як предмет злочинного посягання. *Право і суспільство*. 2015. № 2. С. 177-181. URL: [http://www.pravoisuspilstvo.org.ua/archive/2015/5\\_2\\_2015/part\\_2/33.pdf](http://www.pravoisuspilstvo.org.ua/archive/2015/5_2_2015/part_2/33.pdf) (дата звернення: 14.09.2020).

70. Ліпкан В. А, Капінус Л. І. Доступ до інформації з обмеженим доступом: Проблеми вироблення уніфікованих дефініцій. *Науково-практичний юридичний журнал «Публічне право»*. Київ, 2013. № 4. С 45–53.

71. Логінова Н. І., Дробожур Р. Р. Правовий захист інформації: навчальний посібник / за ред. Н. І. Логінової. Одеса: Фенікс, 2015. 264 с.

72. Нетеса Н. В., Дубина К. В. «НОУ-ХАУ» як об'єкт права інтелектуальної власності : проблемні питання. URL: <https://www.inter-nauka.com/uploads/public/15916454199270.pdf> (дата звернення: 19.09.2020).
73. Обуховська Т. І. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство. URL: <http://visnyk.academy.gov.ua/wp-content/uploads/2014/05/2014-1-17.pdf> (дата звернення: 16.09.2020).
74. Олійник О. В. Інформаційна безпека США. URL: [http://nbuv.gov.ua/j-pdf/boz\\_2012\\_1\\_33.pdf](http://nbuv.gov.ua/j-pdf/boz_2012_1_33.pdf). (дата звернення: 15.09.2020).
75. Полуніна Л. В. Поняття комерційної таємниці як предмета злочинного посягання. URL: [http://www.jurnaluljuridic.in.ua/archive/2019/2/part\\_2/27.pdf](http://www.jurnaluljuridic.in.ua/archive/2019/2/part_2/27.pdf) (дата звернення: 19.09.2020).
76. Попова Н. О. Поняття комерційної таємниці як об'єкта права інтелектуальної власності в законодавстві України. URL: [http://www.nbuv.gov.ua/j-pdf/FP\\_index.htm\\_2014\\_2\\_64.pdf](http://www.nbuv.gov.ua/j-pdf/FP_index.htm_2014_2_64.pdf) (дата звернення: 17.09.2020).
77. Савицький В. Д. Доступ і обмеження доступу до інформації: забезпечена свобода і застережена небезпека. URL: <http://univer.km.ua/visnyk/1624.pdf> (дата звернення: 14.09.2020).
78. Салихов И. И. Информация с ограниченным доступом как объект гражданских правоотношений : дис. ... канд. юрид. наук : 12.00.03. Казань, 2004. 38 с.
79. Сергеева О. Поняття та ознаки комерційної таємниці. *Підприємництво, господарство і право*. 2001. № 2. С. 16 – 23.
80. Ситницький М. В. Характерні ознаки комерційної таємниці. URL: <https://dspace.uzhnu.edu.ua/jspui/handle/lib/6693> (дата звернення: 17.09.2020).
81. Сляднева Г. О. Поняття та ознаки комерційної таємниці суб'єкта господарювання. *Актуальні проблеми держави і права*. 2003. Вип. 21. С. 307-311.
82. Тунік А. В. Правові основи захисту персональних даних: автореферат дис. ... канд. юрид. наук за спеціальністю 12.00.07. Національний авіаційний університет, Київ, 2012, 229 с.

83. Турук А. О. Историчний аспект формування інституту комерційної таємниці. *Молодий вчений*. 2018. № 4(1). С. 92-95.

84. Федоренко О. О., Керсіцький С. О., Курбатов А. І. Проблемні питання правового регулювання обігу інформації з обмеженим доступом (державна таємниця та службова інформація). *Право та інноваційне суспільство*. 2013. № 1. URL: [http://nbuv.gov.ua/UJRN/pric\\_2013\\_1\\_17](http://nbuv.gov.ua/UJRN/pric_2013_1_17) (дата звернення: 14.09.2020).

85. Шарабурина О. О. Деякі аспекти визначення поняття інформації з обмеженим доступом та її видів у законодавстві України. *Альманах права*. 2011. № 2. С. 322-325. URL: <http://dspace.nbuv.gov.ua/bitstream/handle/123456789/63367/84Sharaburina.pdf?sequence=1> (дата звернення: 14.09.2020).

86. Шарабурина О. О. Проблеми правового захисту персональних даних як відомостей з обмеженим доступом. *Вісник Національного технічного університету України «Київський політехнічний інститут»*. *Політологія. Соціологія. Право*. 2012. № 4. С. 74-78.

87. Шарабурина О. О. Адміністративно-правовий режим інформації з обмеженим доступом : Дисертація на здобуття наукового ступеня кандидата юридичних наук : 12.00.07. адміністративне право і процес; фінансове право; інформаційне право. Київський національний торговельно-економічний університет, Київський Національний економічний університет імені Вадима Гетьмана, Київ, 2019. 201 с.

88. Risk Management. Законодавче регулювання інституту банківської таємниці в ЄС і ряді інших Європейських країн. *Taurus group. Taurus Ltd*. 2015. URL: <http://taurusgroup.eu/ru/about-us/> (дата звернення: 17.09.2020).

89. Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505. Children's Privacy. : *ECFR*. URL: <https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5> (дата звернення: 15.09.2020).

90. K.H. and Others v. Slovakia. App. No. 32881/04, 49 Eur. Ct. H.R. 34 (2009). : *European Court of Human Rights*. URL: <https://www.globalhealthrights.org/wp->

content/uploads/2013/10/K.H. \_and\_Others-Slovakia-2009.pdf (дата звернення: 15.09.2020).

91. Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero. *Jefatura del Estado*. URL: <https://www.boe.es/buscar/act.php?id=BOE-A-2002-22807> (дата звернення: 18.09.2020).

92. L.H. v. Latvia. App. No. 52019/07, Judgment 29.4.2014. Section IV. Article 8. : *European Court of Human Rights*. URL: <http://hudoc.echr.coe.int/eng?i=002-9365> (дата звернення: 15.09.2020).

93. S. & Marper v. U. K., App. Nos. 30562/04 and 30566/04 (Eur. Ct. H.R. Dec. 4, 2008). : *European Court of Human Rights*. URL: <http://hudoc.echr.coe.int/fre?i=001-90051> (дата звернення: 15.09.2020).

94. Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. OECD. 2011. URL: <http://www.oecd.org/sti/ieconomy/48975226.pdf> (дата звернення: 15.09.2020).

95. The Computer Security Act of 1987, Public Law No. 100-235 (H.R. 145), (Jan. 8, 1988) : *EPIC*. URL: <https://epic.org/crypto/csa/csa.html> (дата звернення: 15.09.2020).

96. The Freedom of Information Act (FOIA) Pub.L. 90–23, 81 Stat. 54, enacted June 5, 1967 (originally H.R. 5357 in the 90th Congress) : *National Archives*. URL: <https://www.archives.gov/about/laws/foia.html> (дата звернення: 15.09.2020).

97. The Privacy Act of 1974, as amended, 5 U.S.C. § 552a : *The United States Department of Justice*. URL: <https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf> (дата звернення: 15.09.2020).

98. The Right to Financial Privacy Act of 1978. RFPFA; codified at 12 U.S.C. ch. 35, § 3401 : *FDIC*. URL: <https://www.fdic.gov/regulations/compliance/manual/8/viii-3.1.pdf> (дата звернення: 15.09.2020).

99. Uniform Trade Secrets Act (UTSA), published by the Uniform Law Commission (ULC) in 1979 with 1985 amendments drafted by National Conference of

Commissioners URL: <https://www.wipo.int/edocs/lexdocs/laws/en/us/us034en.pdf>  
(дата звернення: 16.09.2020).

100. Z v. Finland. App. No. 22009/93, 25 Eur. H.R. Rep. 371 (1997). : *European Court of Human Rights*. URL: <http://hudoc.echr.coe.int/rus?i=001-58033> (дата звернення: 15.09.2020).