Додаток В

до п.п. 3.6

**(Ф \_\_- \_\_\_)**

**Міністерство освіти і науки України**

**Національний авіаційний університет**

**НАВЧАЛЬНО-НАУКОВИЙ ЮРИДИЧНИЙ ІНСТИТУТ**

**Кафедра КОНСТИТУЦІЙНОГО І АДМІНІСТРАТИВНОГО ПРАВА**

**Конспект лекцій**

**з дисципліни**

**«Правова Інформатика»**

### Спеціальність: 081 «Право»

### Спеціалізація: «Правознавство»

Укладач: Гусар О.А. к.ю.н., доцент кафедри конституційного і

адміністративного права

Конспект лекцій розглянутий та схвалений

на засіданні кафедри конституційного і

адміністративного права

Протокол № \_\_\_\_ від «\_\_\_»\_\_\_\_\_20\_\_р.

Завідувач кафедри Пивовар Ю.І.

Продовження Додатку В

**Лекція № 1**

**Тема 1. Правова інформатика як галузь загальної інформатики і прикладна юридична наука**. **Предмет, мета та система вивчення дисципліни «Правова інформатика»**

**План лекції**

Інформатика як наука. Правова інформатика в системі інформаційних знань. Співвідношення правової інформатики і інших юридичних наук. Завдання та система правової інформатики як науки, її місце в системі наукових знань. Основні поняття правової інформатики. Правова інформатика як навчальна дисципліна.

**Література**

1. Дзьобань О.П. Філософія інформаційного права : світоглядні й загальнотеоретичні засади: монографія / О.П. Дзьобань. – Х.: Майдан, 2013. – 360 с.

2. Дзьобань О.П. Проблеми захисту національних інтересів України у сфері державної безпеки в умовах геополітичних трансформацій ХХІ сторіччя : монографія / О.П. Дзьобань, В.Я. Настюк, В.В. Бєлєвцева. – Х.: Право, 2013. – 296 с.

3. Настюк В.Я. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення : монографія / В.Я. Настюк, В.В. Бєлєвцева. – К-Х.: Право, 2013. – 128 с. – (Наук. зб. “Академічні правові дослідження”). Дод. до журн. “Право України”. – Вип. № 28.

4. Пилипчук В.Г. Інформаційне суспільство: філософсько-правовий вимір**:** монографія **/** В.Г. Пилипчук, О.П. Дзьобань. – К., 2013. – 292 с.

5. Інформаційне право та правова інформатика у сфері захисту персональних даних / В.Брижко, М.Гуцалюк, В.Цимбалюк, М.Швець; За ред. д.е.н., професора, члена-кореспондента Академії правових наук України М.Швеця. – К.: НДЦПІ АПрН України, 2005. – 451 с.

6. Чубукова С.Г., Элькин В.Д. Основы правовой информатики (юридические и математические вопросы информатики): Учебное пособие / Под ред. проф. М.М. Рассолова. – М.: Юридическая фирма «КОНТРАКТ», 2004. – 252 с.

**Зміст лекції**

Еволюція співвідношення знань у галузі інформатики та вдачі, та й самих понять "інформатика" і "право", має досить тривалу історію. У всякому разі, історія юридичної науки, що вивчає цю проблему, бере свій початок з того часу, коли поняття "кібернетика" було повернуто в сферу наукової дискусії, тобто з кінця 1950-х рр. Протягом наступних 20-30 років правова наука була захоплена кібернетичними проблемами юриспруденції. У вузах, у тому числі юридичних, знайомство з інформатикою та обчислювальною технікою відбулося в 1960-х рр., Коли в нашій країні було розпочато серійне виробництво ЕОМ. Тоді ж у Київському та Московському університетах для студентів-юристів читався курс з основ правової кібернетики. Так почалося вивчення інформатики в юриспруденції.

В цей же час використання інформаційних методів і математичних засобів інформатики і кібернетики в правовій системі сформувало самостійні напрямки юридичної науки - ***правову кібернетику,*** а пізніше на її основі і ***правову інформатику.*** Основні дослідження велися переважно за наступними напрямками використання інформаційних знань у юриспруденції:

1) використання кібернетичних засобів в пошуку правової інформації та правотворчої діяльності. Розгляд права як тексту, а норми права як елементарної частинки руху правової інформації привело до розуміння інформаційної функції права;

2) застосування методів і науково-технічних засобів інформатики для обробки статистичної інформації суспільно-правового характеру;

3) використання досягнень інформатики в криміналістиці і судових експертизах. Використання кількісних методів при проведенні судових експертиз;

4) інформаційне забезпечення юридичної діяльності: судових і правоохоронних органів;

5) впровадження елементів програмування в юриспруденції: алгоритми кримінальної кваліфікації та проблеми складу злочину, конструктивні особливості правознавства. У цій же площині вивчаються і проблеми моделювання і формування юридичних конструкцій.

У названих напрямках проявляється вплив інформатики на юридичну дійсність, правотворчість і юридичну діяльність, на юриспруденцію в цілому. Закономірності такого впливу формують предмет правової інформатики як науки і навчальної дисципліни.

З іншого боку, коеволюція інформації та права проявляється у впливі права на інформаційну діяльність, на інформаційні відносини, на інформаційну сферу в цілому.

Роль правової системи тут проявляється насамперед у ***забезпеченні:***

• формування прав та інтересів суб'єктів інформаційної сфери (забезпечувальна функція права);

• правового регулювання інформаційних процесів (регулятивна функція вдачі);

• правового захисту нрав і інтересів суб'єктів інформаційної сфери (правоохоронна функція);

• розвитку право-інформаційної культури (виховна функція);

• попередження інформаційних правопорушень (превентивна функція).

Всі ці функції є змістом нової галузі системи - ***інформаційного права.***

Таким чином, проблеми взаємодії інформації та права знаходять вираження у співвідношенні правової інформатики та інформаційного права, а також дозволяються у межах їх еволюції і закономірностей, тобто різних формах стійкого взаємозв'язку і взаємозалежності названих двох явищ.

Якщо інформатика впливає на правознавство та забезпечує юридичну сферу за допомогою специфічних засобів (інформаційних засобів і технологій), то право забезпечує інформаційні процеси та інформаційні відносини за допомогою властивих тільки праву правових засобів та інструментів.

# Правова інформатика як наука і навчальна дисципліна

Як відомо, предметом будь-якої науки є закономірності явищ, тобто виявлення та аналіз найбільш стійких зв'язків і взаємозалежностей між ними, а також пошук шляхів вирішення наукових проблем у тій чи іншого різновиду природної і штучної системах.

Правова інформатика займається дослідженням закономірностей природи і структури правової інформації, а також вирішенням наукових проблем формування, обробки, зберігання та використання інформації в правовій системі. Метою правової інформатики як навчальної дисципліни є вивчення ***найбільш загальних знань*** про природу і існування правової інформації, про інформаційні процесах і формах її обороту, а також набуття досвіду її формування та використання за допомогою засобів обчислювальної техніки та інформаційних технологій.

Таким чином, різниця між наукою та навчальною дисципліною "правова інформатика" полягає в ***рівні пізнання*** проблем правової інформації. Перший рівень пізнання (навчальна дисципліна) зводиться до вивчення основних відомостей про предмет. Більш глибокі знання про проблеми і закономірностях, узагальнення та пошук їх вирішення є ***предметом*** науки.

Як міждисциплінарна область наукових знань правова інформатика є прикладною наукою і поки не досягла високого рівня розвитку. Однак вона має велике практичне значення в юридичній діяльності.

**Лекція № 2**

**Тема 2. Об’єкт та предмет правової інформатики.**

**План лекції**

Предмет правової інформатики. Об’єкти правової інформатики. Поняття організаційно-правового ресурсу. Інформаційно-правове поле. Соціально-правова інформація в структурі правового регулювання

**Література**

1. Правова інформатика. / М.Швець, В. Брижко, Л.Задорожня, Ю.Клімашевська, В.Фурашев, В.Хахановський, В.Цимбалюк та ін. – У 2-х т. – К.: Парлам. вид-во, 2005. – Т. 1. – 416 с.
2. Цимбалюк В. С. Інформаційне право (основи теорії і практики). — К.: «Освіта України», 2010. – 388 с.
3. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє / В.Фурашев, Д.Ланде, О.Григор’єв, О.Фурашев. – К.: “Інжиніринг” 2005. – 164 с.

**Зміст лекції**

Сьогодні досягнення інформатики знаходять широке застосування практично у всіх областях людської діяльності. У кожній області наукового знання інформатика заломлюється в прикладне напрям, заснований на використанні особливостей інформаційних процесів і властивості конкретних видів інформації, що циркулюють в даній області. Це призвело до виникнення прикладної інформатики - економічної, соціальної, правової і т.д.

Природно, що кожне з прикладних напрямків інформатики має в своєму арсеналі весь набір засобів і методів загальної інформатики в цілому. Однак особливість інформаційної роботи в конкретних видах діяльності призводить до необхідності використання специфіки досліджуваної інформації та інформаційних процесів і, отже, розвитку загальної теорії з використанням цих особливостей.

Виходячи з цього, правова інформатика, по-перше - один з напрямків інформатики, а по-друге - наука, що досліджує право і правову систему суспільства з інформаційних позицій. З цієї точки зору правову інформатику можна розглядати і як прикладної юридичної науки.

Мабуть, не викликає сумнівів виключно плідний вплив інформатики як науки на розвиток і практичне застосування сучасних інформаційних технологій в самих різних напрямках науки і практики. У зв'язку з цим становлення правової інформатики як науки, що вивчає інформацію, інформаційні процеси та інформаційні системи в праві (або в правовій системі) в Росії на початку XXI ст., На порозі переходу до інформаційного суспільства - важливий фактор вдосконалення діяльності в області права.

У розвиток правової інформатики значний внесок внесли російські вчені: Ю. М. Батурін, І. Л. Бачило, А. Б. Венгеров, Н. В. Вітрук, О. А. Гаврилов, В. Б. Ісаков, Д. А. Керімов, В. Кнапп, В. А. Копилов, В. Н. Кудрявцев, Ю. В. Кудрявцев, А. В. Морозов, С. С. Москвін, Н. С. Польовий, Μ. М. Розсолів, А. Д. Урсул, В. М. Хургин, С. М. Шахрай, А. Р. Шляхов та ін.

За літературними даними відомий цілий ряд підходів до визначення змісту поняття правової інформатики та її предмета. Багато в чому це визначалося неоднозначністю трактування поняття загальної інформатики, про яку говорилося раніше. Розглянемо найбільш поширені серед цих підходів.

Н. С. Польовий і А. Р. Шляхов розглядали правову інформатику як один із напрямів науки кібернетики. Предметом цього напряму є закономірності освіти, сприйняття, зберігання, обробки і видачі соціально-правової інформації з метою підвищення ефективності організаційної взаємодії керуючих і керованих систем в правовій сфері суспільства [[1]](http://stud.com.ua/72705/informatika/ponyattya_pravovoyi_informatiki" \l "srcannot_1) .

Ю. М. Батурін в правовій інформатиці виділяє три складових: технічну сторону інформаційного права і програмне забезпечення правових задач; спеціалізовані юридичні системи і прийняття юридичних рішень за допомогою ЕОМ; основи теорії інформації стосовно правової матерії [[2]](http://stud.com.ua/72705/informatika/ponyattya_pravovoyi_informatiki#srcannot_2) .

Особливий інтерес, на наш погляд, представляє точка зору А. Б. Венгерова, який пов'язує предмет правової інформатики з "інформаційної концепцією права, тобто вченням про інформаційну природу права", а інформаційно-правову діяльність розглядає як повое напрямок в юридичній роботі [[3]](http://stud.com.ua/72705/informatika/ponyattya_pravovoyi_informatiki#srcannot_3) .

Розвиваючи ці положення, Μ. М. Розсолів і В. Д. Ель- киї визначають правову інформатику як "прикладну науку, що вивчає проблеми збору, сприйняття, реєстрації зберігання, обробки та використання соціально-правового інформації в правовій системі суспільства і її підсистемах, як специфічних правових інформаційних утвореннях" [[4]](http://stud.com.ua/72705/informatika/ponyattya_pravovoyi_informatiki#srcannot_4) . Дані автори відзначають, що правова інформатика, маючи своє коріння в теорії держави і права та загальної, "великий інформатики", підходить до права і до всіх областей юридичної діяльності з самостійних позицій, що значно відрізняються від підходу до них з боку інших юридичних наук; вона досліджує загальні і конкретні інформаційні проблеми і завдання в сфері права та правових механізмів [[5]](http://stud.com.ua/72705/informatika/ponyattya_pravovoyi_informatiki#srcannot_5) . Зазначені автори вперше звернули увагу на значущість підходу до визначення інформатики, запропонованого Ф. Е. темників.

О. А. Гаврилов, погоджуючись із запропонованим Н. С. Польовим визначенням, розглядає правову інформатику як "міждисциплінарну галузь знань про закономірності й особливості інформаційних процесів у сфері юридичної діяльності, про їх автоматизації, про принципи побудови та методиках використання автоматизованих інформаційних систем, створюваних для вдосконалення і підвищення ефективності юридичної діяльності та вирішення правових задач на базі комплексного використання теорії та методології правових наук засобів і методів математики, інформатики і логіки " [[6]](http://stud.com.ua/72705/informatika/ponyattya_pravovoyi_informatiki#srcannot_6) .

Аналіз цих які суперечать одна одній підходів, дозволяє виділити, на наш погляд, два найбільш важливі напрямки заломлення загальної інформатики в правовій сфері.

Перший напрям пов'язаний з дослідженням правової системи суспільства, її підсистем, соціально-правової інформації тощо як специфічних інформаційних правових утворень. Будь-яка правова система - система правових норм, система юридичних органів, правові механізми з точки зору протікають в них процесів, пошуку, збору, передачі, систематизації, сприйняття і обробки інформації є інформаційними системами. І отже, закони функціонування цих систем і що протікають в них інформаційні процеси підкоряються законам інформатики і можуть бути досліджені за допомогою методів, розроблених даною наукою. Метою даної роботи є вдосконалення всієї правової системи па основі створення ефективної системи інформаційного забезпечення юридичної діяльності.

Другий напрямок має бути обов'язково пов'язане з урахуванням правових особливостей, досліджуваних об'єктів, явищ і процесів. З одного боку, це залежить від того, що право і правова система відіграють важливу роль у формуванні та розвитку єдиного інформаційного простору держави та виступають в якості необхідних компонентів інформаційних технологій і забезпечення інформаційних систем. З іншого боку, особливості соціально-правового інформації (в першу чергу нормативної), особливості протікання багатьох інформаційних процесів в юридичних утвореннях, пов'язані з регулятивної функцією права, особливості функціонування правових інформаційних систем повинні обов'язково враховуватися при конструюванні методів дослідження правової інформатики. Таким чином, дослідження в правовій інформатиці повинні враховувати як інформаційні, так і правові сторони досліджуваних об'єктів, явищ і процесів.

З огляду на сказане, *правову інформатику* можна визначити як науку, що вивчає структуру і властивості інформації, закономірності розвитку інформаційних процесів, інформаційних технологій та інформаційних систем в правовій сфері, на основі дослідження правових особливостей досліджуваних об'єктів, явищ і процесів.

З даного визначення відразу видно, що об'єктами вивчення в правовій інформатиці є *інформація, інформаційні процеси, інформаційні технології та інформаційні системи,* що функціонують в правовій сфері.

Основними напрямками вивчення *інформації* в правовій системі як об'єкта правової інформатики повинні бути:

• визначення і гармонійне поєднання загальних властивостей соціальної інформації та специфічних властивостей правової інформації (особливо нормативно-правової інформації);

• класифікація соціальної інформації, що циркулює в правовій системі;

• дослідження проблем оцінки кількості і якості правової інформації;

• аналіз ролі інформації в прийнятті юридичних рішень і т.п.

*Інформаційні процеси* в правовій системі - це процеси збору, виробництва, поширення, перетворення, пошуку, отримання, передачі та споживання інформації. Правова інформатика одночасно і у взаємозв'язку вивчає природно-наукову сутність цих процесів з урахуванням юридичних властивостей інформації та інформаційних об'єктів. Метою вивчення є, з одного боку, необхідність ефективної організації інформаційних процесів у всіх видах юридичної діяльності, а з іншого - вивчення їх особливостей, необхідно для грамотного правового регулювання тих суспільних, до виникнення яких призводять розглядаються інформаційні процеси.

*Інформаційні технології* та *інформаційні системи,* що створюються на базі використання сучасних інформаційних технологій, довгий час розглядалися правової інформатикою тільки з точки зору ефективної організації юридичної діяльності. Однак останнім часом проблема правового регулювання суспільних відносин, об'єктами яких є інформаційні технології та системи, актуально стоїть перед галузевими юридичними науками (особливо перед інформаційним правом).

У Федеральному законі від 27 липня 2006 № 149-ФЗ "Про інформацію, інформаційні технології і про захист інформації" (далі - Закон про інформацію) дані основні поняття інформаційного законодавства.

Так, під *інформацією* розуміються відомості (повідомлення, дані) незалежно від форми їх подання.

*Інформаційні технології* визначені як процеси, методи пошуку, збору, зберігання, обробки, надання, поширення інформації та способи здійснення таких процесів і методів.

*Інформаційна система -* це сукупність міститься в базах даних інформації і забезпечують її обробку інформаційних технологій і технічних засобів.

Очевидно, що інформація - це складне багатогранне і всеосяжне явище. І, природно, окремі сторони, грані його є предметом дослідження дуже багатьох наук, які хоча і існують самостійно, однак розвиваються в нерозривній єдності, доповнюючи і збагачуючи один одного, - кібернетики, семіотики, когнітивної психології, математики, технічних наук, теорії інформації і ін.

Юристу знання правової інформатики дозволяє підвищити свій професійний рівень. Сьогодні лавинні потоки соціально-правової інформації, що обрушуються на юриста, настійно вимагають від нього володіння сучасними інформаційними технологіями - довідковими правовими системами, юридичними експертними системами, сучасними програмними та технічними засобами захисту інформації, електронного підпису, інформаційними технологіями, що лежать в основі функціонування сучасних комп'ютерних мереж і глобальної мережі Інтернет, і т.п.

Але для юриста знання інформаційних технологій - це не тільки інструмент в його практичній діяльності. Інформація, інформаційні процеси, інформаційні системи сьогодні є об'єктами правовідносин

і предметом вивчення галузевих правових наук. В активно формується інформаційному законодавстві юристам необхідно провести правове регулювання нових суспільних відносин, що складаються з приводу таких об'єктів, як інформація, інформаційні системи, інформаційні технології, комп'ютерні мережі. Для грамотного, повного правового регулювання необхідно чітке розуміння істоти даних інформаційних об'єктів, їх особливостей і принципів функціонування, всього того, що вже побудовано і обґрунтовано в теорії інформатики та правової інформатики. З цієї точки зору правова інформатика для юриста - це джерело знань, необхідних йому для вирішення професійних завдань.

Нарешті, інформатика дає в руки юристу додаткові методи дослідження. Більшість правових явищ, по суті, є інформаційними системами, тобто системами, заснованими на процесах створення, зберігання, поширення і обробки інформації. Механізми правотворчості, правового регулювання, правопорядку, правової культури, правового виховання та ін. Є інформаційними утвореннями. Всебічне вивчення таких явищ і процесів неможливо без використання тих методів і засобів, які розроблені в інформатиці та правової інформатики.

В даний час вже можна говорити про зміст "інформаційної метрики в області права" [[7]](http://stud.com.ua/72705/informatika/ponyattya_pravovoyi_informatiki#srcannot_7) , куди насамперед включаються різноманітні розділи сучасної математики і кібернетики: структурні заходи інформації (геометрична міра, комбінаторна міра, аддитивная міра і ін.); статистичні заходи інформації (ймовірність і інформація, поняття ентропії, ентропія ансамблю, кількість інформації і т.д.); семантичні заходи інформації (змістовність інформації, доцільність інформації, динамічна ентропія ін.); дискретизація і кодування інформації; дослідження операцій (поняття теорії дослідження операцій, інформація, що вводиться в моделі дослідження операцій, рішення задач в разі відсутності повної інформації й т.д.) і інші галузі знань. До складу "інформаційної метрики" повинні увійти також конкретні схеми оптимізації функціонування правових інформаційних утворень, до яких можна віднести:

1) окремі інформаційні елементи правових утворень е допомогою програмно-логічних методів. Ця схема заснована, але суті, на ідеях системного аналізу, програмування, алгоритмізації і математичної логіки, за допомогою яких представляється можливим вивчити деякі "константи" правової інформатики - програми роботи з правовою інформацією в фірмах, компаніях, банках, масиви і логіку правових повідомлень на підприємствах і в організаціях, алгоритми вирішення юридичних завдань в області інформаційного обслуговування правоохоронних органів та інші проблеми;

2) функціональні значення правових інформаційних утворень, що залежать від структури і цілей останніх. Ця схема оптимізації заснована на теорії ймовірностей, математичній статистиці та теорії дослідження операцій. Тут розглядаються акти ймовірного поведінки правових інформаційних утворень, операції у сфері управління останніми, інформація, що вводиться в юридичні моделі, підходи до вирішення завдань масового інформаційного обслуговування в механізмах законності, правопорядку, профілактики конкретних злочинів і інші проблеми;

3) функціонування правових інформаційних утворень на основі використання математичної теорії інформації, теорії графів, теорії множин, розпізнавання образів і ін. За цією схемою здійснюється оптимізація інформаційного забезпечення приватних актів правового регулювання, оптимізація розробки і прийняття законів, здійснення прокурорських перевірок, розслідування злочинів, оцінки ефективності правоохоронної діяльності тощо

**Лекція № 3**

**Тема3. Огляд законодавства у сфері інформації і інформатизації**

**План лекції**

Основні положення та особливості застосування законів України «Про електронні документи та електронний документообіг» і «Про електронний цифровий підпис». Електронні документи. Електронний документообіг. принципи електронного документообігу. Зберігання електронних документів та архіви електронних документів. Юридична значимість електронного цифрового підпису. Механізм електронного цифрового підпису.

Міжнародні правові документи в галузі інформаційного суспільства і права.

Шенгенська Інформаційна Система (SIS). Конвенція Європолу. Огляд інформаційного законодавства США, Великобританії, ФРН, РФ. Шенгенська Інформаційна Система (SIS). Конвенція Європолу. Закон США «Про захист комп'ютерної інформації».

**Література**

1. Про доступ до публічної інформації : Закон України від 13.01.11 р. № 2939- VI // Відомості Верховної Ради України. – 2011. – № 32. – С. 1491. – Ст. 314. 15
2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.94 р. №80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. Ст. 286.
3. Про телекомунікації : Закон України від 18.11.03 р. № 1280-IV : за станом на 16.01.12 р. // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.
4. Про Національну програму інформатизації : Закон України від 04.02.98 р. № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27 – 28. – Ст.181.
5. Про Національну систему конфіденційного зв`язку : Закон України від 10.01.02 р. № 2919-ІІІ // Відомості Верховної Ради України. – 2002. – № 15. – Ст. 103.
6. Про затвердження Концепції технічного захисту інформації в Україні : Постанова Кабінету Міністрів України від 08.10.97 р. № 1126 : за станом на 16.01.12 р. – Режим доступу : <http://zakon2.rada.gov.ua>
7. Про Стратегію національної безпеки України : Указ Президента України від 12.02.07 р. № 105/2007 // Офіційний вісник України. – 2007. – № 11. – С. 7. – Ст. 389.
8. Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року “Про невідкладні заходи щодо забезпечення інформаційної безпеки України” : Указ Президента України від 23.04.08 р. № 377/2008 // Офіційний вісник Президента України. – 2008. – № 18. – С. 24. – Ст. 570. 30. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В.П. Горбулін, О.Г. Додонов , Д.В. Ланде. – К. : Інтертехнологія, 2009. –164 с.
9. Правові проблеми протидії новітнім викликам, загрозам і правопорушенням в інформаційній сфері / Савінова Н.А., Стрельбицький М.П. // Правова доктрина України. – 2 том: Публічно-правова доктрина України. – Харків: «Право», 2013. – С. 832 – 861.
10. Проблеми захисту національних інтересів України у сфері державної безпеки в умовах геополітичних трансформацій ХХІ сторіччя : монографія / О.П. Дзьобань, В.Я. Настюк, В.В. Бєлєвцева. – Х.: Право. – 2013. – 296 с.
11. Інформаційно-правове регулювання документованої інформації / Коваленко Л.П. // Інформація і право. – 2013. – № 1(7). – С. 58-63.

**Зміст лекції**

Верховною Радою України були прийняті закони України, які набули чинності, „Про електронні документи та електронний документообіг", „Про електронний цифровий підпис", „Про обов’язковий примірник документів", „Про Національну програму інформатизації", „Про телекомунікації", „Про Національну систему конфіденційного зв’язку", „Про захист інформації в інформаційно-телекомунікаційних системах", тощо.

Закон України „Про електронні документи та електронний документообіг" визначив основні організаційно-правові засади електронного документообігу та використання електронних документів.

Законом встановлено, що електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа, зокрема, електронного цифровий підпису. Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Проте, закон також встановив певні обмеження на застосування електронного документа як оригіналу. Зокрема в електронній формі не може бути створено оригінал свідоцтва про право на спадщину; інший документ, який, згідно із законодавством, може бути створений лише в одному примірнику (поки не буде створено централізованого сховища оригіналів електронних документів).

Електронний цифровий підпис дає змогу підтвердити цілісність електронного документу, тобто його захищеність від несанкціонованого спотворення, руйнування або знищення в процесі руху від відправника до одержувача, та ідентифікувати підписувача.

Правочини здійснені за допомогою накладання на них електронного цифрового підпису та передані адресату в мережі передачі даних мають великий ступень захисту від несанкціонованого доступу, спотворення чи знищення змісту правочину, адже такий підпис отримується за результатом криптографічного перетворення набору електронних даних.

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки), якщо: електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису; під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису; особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Особистий ключ має бути відомий лише його володільцеві. Відкритий ключ доступний всім учасникам електронного документообігу.

Засвідчення чинності відкритого ключа здійснюється шляхом формування сертифіката відкритого ключа – документа, що видається центром сертифікації ключів. Посилений сертифікат відкритого ключа видається акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом.

Сертифікат ключа містить найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру); зазначення, що сертифікат виданий в Україні; унікальний реєстраційний номер сертифіката ключа; основні дані (реквізити) підписувача – власника особистого ключа; дату і час початку та закінчення строку чинності сертифіката; відкритий ключ; найменування криптографічного алгоритму, що використовується власником особистого ключа; інформацію про обмеження використання підпису.

Посилений сертифікат ключа, крім обов’язкових даних, які містяться в сертифікаті ключа, повинен мати ознаку посиленого сертифіката ключа.

Юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом ключа, а також використовувати електронний цифровий підпис без сертифіката ключа.

Розподіл ризиків збитків, що можуть бути заподіяні підписувачам, користувачам та третім особам, які користуються електронними цифровими підписами без сертифіката ключа, визначається суб’єктами правових відносин у сфері послуг електронного цифрового підпису на договірних засадах.

Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа.

Отже, електронний цифровий підпис спрямований на спрощення та прискорення документообігу між суб’єктами господарювання, що, в свою чергу, має зміцнити конкурентоспроможність вітчизняних підприємств, адже пришвидшиться процедура укладення цивільно-правових та господарських договорів, оформлення експортно-імпортних операцій, надання електронних банківських послуг.

Станом на сьогодні, згідно з інформації розміщеній на офіційному веб-сайті центрального засвідчувального органу, акредитацію пройшли три центри сертифікації ключів, тобто система електронного цифрового підпису є повністю структурно укомплектованою для належного функціонування.

Документообіг в державі є системою, що матеріалізує процеси збору, перетворення, зберігання інформації, а також процеси управління: підготовку та прийняття рішень, контроль за їх виконанням.

Поняття „електронне урядування" на сьогодні вже не є цілком невідомим і новим, як це було кілька років тому. Пов’язуючи його з доступом до публічної інформації, можна сказати, що воно є ефективним засобом забезпечення інформування та доступу до інформації фізичними та юридичними особами, а отже, сприяє прозорості та ефективності діяльності влади.

Реалізація ідеї електронного урядування викликає величезний інтерес у всьому світі. США, Великобританія, Швеція, Данія, Норвегія, Латвія, Естонія та багато інших країн уже застосовують або починають застосовувати методи електронного урядування. Зокрема, уряд США надає громадянам різноманітні послуги через мережу Інтернет: видачу ліцензій, сплату штрафів тощо. В Англії реєстрація фірм потребує заповнення через мережу тільки однієї форми.

Позитивні приклади запровадження та функціонування електронних урядів в інших країнах, допоможуть підкреслити реальні переваги цих систем та всебічно реалізувати електронне урядування в Україні.

На сьогодні, в нашій державі існує досить велика кількість норматив­но-правових актів, що регулюють відносини у сфері інформаційних тех­нологій. Проте значна частина з них потребує внесення змін та допов­нень, оскільки тією чи іншою мірою не узгоджується між собою та не в змозі адекват­но вирішувати проблеми, що виникають.

Концепція електронного урядування складається з двох взаємозалежних та водночас самостійних структур. Внутрішня урядова інформаційна інфраструктура, аналог корпоративної мережі, та зовнішня інформаційна інфраструктура, що взаємодіє з громадянами та організаціями. У рамках „електронної держави" інтегруються інформаційні ресурси органів державної влади, а також створюється система он-лайнових послуг.

З метою підвищення ефективності роботи органів державної влади та органів місцевого самоврядування у рамках реалізації завдань (проектів) Національної програми інформатизації передбачається, згідно з інформації розміщеній на веб-сайті Державного департаменту з питань зв’язку та інформатизації, об’єднання існуючих у цих органах інформаційних систем та тих, що будуть розроблятися в єдиний інформаційно-аналітичний комплекс – Інтегровану інформаційно-аналітичну систему органів державної влади та органів місцевого самоврядування України.

Враховуючи різноманітність існуючих систем електронного документообігу в органах державної влади та органах місцевого самоврядування, при розробці та реалізації пілот-проекту системи передбачається створення інтегрованої системи електронного документообігу.

Метою створення такої системи є забезпечення руху документів (укази, постанови, закони, розпорядження, повідомлення, звіти, аналітичні довідки, тощо), скорочення терміну підготовки та прийняття рішень шляхом автоматизації процесів колективного створення та використання документів в органах державної влади.

Проте, правового забезпечення відносин у сфері системи електронного урядування, на сьогодні у формі нормативно-правового акта, який би чітко і всебічно регулював дане питання не має.

31 липня 2000 року Президент України прийняв Указ „Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні". Цим Указом встановлено, що розвиток національної складової інформаційної мережі Інтернет, забезпечення широкого доступу до цієї мережі громадян та юридичних осіб усіх форм власності в Україні, належне представлення в ній національних інформаційних ресурсів є одним з пріоритетних на­прямів державної політики у сфері інформатизації, задоволення консти­туційних прав громадян на інформацію, побудови відкритого демократич­ного суспільства, розвитку підприємництва. Відповідно до даного Указу основними завданнями є забезпечення підтримки розвитку інфраструкту­ри надання інформаційних послуг через мережу Інтернет та розвиток і впровадження сучасних комп’ютерних інформаційних технологій у сис­темі державного управління.

Серед інших нормативно-правових актів, які регулюють правовідноси­ни у сфері інформатизації, а саме щодо питань електронного урядування, важливим документом є Постанова Кабінету Міністрів України від 4 січня 2002 року за № 3 „Про по­рядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади". Відповідно до зазначеного Порядку оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади здійснюється з метою підвищення ефективності та прозорості діяльності цих органів шляхом впровадження та викорис­тання сучасних інформаційних технологій для надання інформаційних та інших послуг громадськості, забезпечення її впливу на процеси, що відбу­ваються у державі. Оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади здійснюється шляхом:

* розміщення і періодичного оновлення міністерствами, іншими цен­тральними та місцевими органами виконавчої влади інформації відповід­но до вимог цього Порядку на власних веб-сайтах;
* створення Єдиного веб-порталу Кабінету Міністрів України, призначеного для інтеграції веб-сайтів органів виконавчої влади та розмі­щення інформаційних ресурсів відповідно до потреб громадян.

З метою вирішення питань, які стосуються проблематики запровадження в Україні системи електронного урядування, 24 лютого 2003 № 208 року було прийнято Постанову Кабінету Міністрів України „Про заходи щодо створення електронної інформаційної системи „Електронний уряд".

Відповідно до Постанови передбачається створити належні нормативно-правові засади функціонування системи „Електронний уряд", забезпе­чити умови для більш швидкого та доступного надання інформаційних послуг громадянам та юридичним особам шляхом використання електронної інформаційної системи „Електронний уряд", яка забезпечує: взаємодію органів виконавчої влади між собою, з громадянами та юридични­ми особами на основі сучасних інформаційних технологій, інтегрувати державні електронні інформаційні ресурси і системи в Єдиний веб-портал органів виконавчої влади.

Таким чином, проаналізувавши хід подій у сфері інформаційних правовідносин та інформатизації, зокрема, впровадження системи електронного документування в Україні, різно­манітні документи та матеріали, можна зробити висновок, що у цьому напрямку здійснюються певні заходи. Можливо, не настільки інтенсивно, як в інших державах, але можна стверджувати, що через деякий час Украї­на, за умови системної правової та практичної розбудови системи електронного документування, також буде характеризуватися неабиякими здобутками у цій сфері.

## Про електронний цифровий підпис

Цей Закон визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису.

Дія цього Закону не поширюється на відносини, що виникають під час використання інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису.

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Законом, застосовуються правила міжнародного договору.

* ***електронний підпис*** - дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;
* ***електронний цифровий підпис*** - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;
* ***засіб електронного цифрового підпису*** - програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;
* особистий ключ - параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;
* відкритий ключ - параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;
* засвідчення чинності відкритого ключа - процедура формування сертифіката відкритого ключа;
* сертифікат відкритого ключа (далі - сертифікат ключа) - документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача;
* посилений сертифікат відкритого ключа (далі - посилений сертифікат ключа) - сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом;
* підписувач - особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа;
* послуги електронного цифрового підпису - надання у користування засобів електронного цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксуваннячасу,консультаціїтаіншіпослуги,визначені цим Законом;

***Суб'єктами правових відносин усферіпослуг електронного цифрового підпису є:***

* підписувач;
* користувач;
* центр сертифікації ключів;
* акредитований центр сертифікації ключів;
* центральний засвідчувальний орган;
* засвідчувальний центр органу виконавчої влади або іншого державного органу (далі - засвідчувальний центр);
* контролюючий орган.

Електронний цифровий підписзаправовимстатусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

* електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;
* під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;
* особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

***Електронний підпис не може бути визнаний недійсним лише через те,що він має електронну форму або не грунтується напосиленому сертифікаті ключа.***

Електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб,яка здійснюється з використанням електронних документів.

Електронний цифровий підпис використовується фізичними та юридичними особами-суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів,встановленого законом для вчинення правочинів у письмовій формі.

Нотаріальні дії із засвідчення справжності електронного цифрового підпису на електронних документах вчиняються відповідно до порядку, встановленого законом.

#### *Особливості застосування електронного цифрового підпису*

Органи державної влади,органимісцевого самоврядування, підприємства, установи та організації державної форми власності для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа.

Інші юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом ключа, сформованим центром сертифікації ключів,а також використовувати електронний цифровий підпис без сертифіката ключа.

Розподіл ризиків збитків, що можуть бути заподіяні підписувачам, користувачам та третім особам,які користуються електронними цифровими підписами без сертифіката ключа, визначається суб'єктами правових відносин у сфері послуг електронного цифрового підпису на договірних засадах.

Захист прав споживачів послуг електронного цифрового підпису, а також механізм реалізації захисту цих прав регулюються цим Законом та Законом України "Про захист прав споживачів".

У випадках, коли відповідно до законодавства необхідне засвідчення дійсності підпису на документах та відповідності копій документів оригіналам печаткою, на електронний документ накладається ще один електронний цифровий підпис юридичної особи, спеціально призначений для таких цілей.

Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності визначається Кабінетом Міністрів України.

Порядок застосування цифрового підпису в банківській діяльності визначається Національним банком України.

Сертифікат ключа містить такі обов'язкові дані:

* найменування тареквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);
* зазначення, що сертифікат виданий в Україні;
* унікальний реєстраційний номер сертифіката ключа;
* основні дані (реквізити) підписувача - власника особистого ключа;
* дату і час початку та закінчення строку чинності сертифіката;
* відкритий ключ;
* найменування криптографічного алгоритму, що використовується власником особистого ключа;
* інформацію про обмеження використання підпису.

Посилений сертифікат ключа, крім обов'язковихданих, які містяться в сертифікаті ключа, повинен мати ознаку посиленого сертифіката ключа.

Інші дані можуть вноситися у посилений сертифікат ключа на вимогу його власника.

#### Права та обов'язки підписувача

Підписувач має право:

* вимагати скасування,блокування або поновлення свого сертифіката ключа;
* оскаржити дії чи бездіяльність центру сертифікаціїключіву судовому порядку.

Підписувач зобов'язаний:

* зберігати особистий ключ у таємниці;
* надавати центру сертифікації ключів дані згідно з вимогами статті 6 цього Закону для засвідчення чинності відкритого ключа;
* своєчасно надавати центру сертифікації ключів інформацію про зміну даних, відображених у сертифікаті ключа.

#### *Центр сертифікації ключів.*Центром сертифікації ключів може бути юридична особа незалежно від форми власності або фізична особа,яка є суб'єктом підприємницької діяльності, що надає послуги електронного цифрового підпису та засвідчила свій відкритий ключ у центральному засвідчувальному органі або засвідчувальному центрі з дотриманням вимог статті 6 цього Закону.

Обслуговування фізичнихта юридичних осіб здійснюється центром сертифікації ключів на договірних засадах.

Центр сертифікації ключів має право:

* надавати послугиелектронногоцифровогопідпису та обслуговувати сертифікати ключів;
* отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування сертифіката ключа безпосередньо у юридичної або фізичної особи чи у її уповноваженого представника.

Центр сертифікації ключів зобов'язаний:

* забезпечувати захист інформації в автоматизованих системах відповідно до законодавства;
* забезпечувати захист персональних даних, отриманих від підписувача, згідно з законодавством;
* встановлювати під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу;
* своєчасно скасовувати,блокувати та поновлювати сертифікати ключів у випадках, передбачених цим Законом;
* своєчасно попереджувати підписувача та додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання електронного цифрового підпису, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку центру сертифікації ключів;
* перевіряти законність звернень про скасування,блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;
* цілодобово прийматизаявипроскасування,блокування та поновлення сертифікатів ключів;
* вести електронний перелік чинних,скасованих і блокованих сертифікатів ключів;
* забезпечувати цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали;
* забезпечувати зберігання сформованих сертифікатів ключів протягом строку,передбаченого законодавством для зберігання відповідних документів на папері;
* надавати консультації з питань,пов'язаних з електронним цифровим підписом.

Зберігання особистих ключів підписувачів та ознайомлення з ними в центрі сертифікації ключів забороняються.

**Засвідчувальний центр**

Кабінет Міністрів України за необхідності визначає засвідчувальний центрцентрального органу виконавчої влади для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи центрів сертифікації ключів, які надають послуги електронного цифрового підпису цьому органу і підпорядкованим йому підприємствам, установам та організаціям.

Інші державні органи за необхідності,за погодженням з Кабінетом Міністрів України, визначають свої засвідчувальні центри, призначені для виконання функцій, зазначених у частині першій цієї статті.

Засвідчувальний центр по відношенню до групи центрів сертифікації ключів, зазначених у частині першій цієї статті, має ті ж функції і повноваження, що й центральний засвідчувальний орган стосовно центрів сертифікації ключів.

Засвідчувальний центр відповідає вимогам, встановленим законодавством для акредитованого центру сертифікації ключів.

Засвідчувальний центр реєструється,засвідчує свій відкритий ключ і акредитується у центральному засвідчувальному органі.

Положення про засвідчувальний центрцентрального органу виконавчої влади затверджується Кабінетом Міністрів України.

#### Центральний засвідчувальний орган

Центральний засвідчувальнийорган визначається Кабінетом Міністрів України.

Центральний засвідчувальний орган:

* формує і видає посилені сертифікати ключів засвідчувальним центрам та центрам сертифікації ключів з дотриманням вимог статті 6 цього Закону;
* блокує, скасовує та поновлює посилені сертифікати ключів засвідчувальних центрів та центрів сертифікації ключів у випадках, передбачених цим Законом;
* веде електронні реєстри чинних,блокованих та скасованих посилених сертифікатів ключів засвідчувальних центрів та центрів сертифікації ключів;
* веде акредитацію центрів сертифікації ключів,отримує та перевіряє інформацію, необхідну для їх акредитації;
* забезпечує цілодобово доступ засвідчувальних центрів та центрів сертифікації ключів до посилених сертифікатів ключів та відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали;
* зберігає посилені сертифікати ключів засвідчувальних центрів та центрів сертифікації ключів;
* надає засвідчувальним центрам та центрам сертифікації ключів консультації з питань,пов'язаних з використанням електронного цифрового підпису.

Центральний засвідчувальний органв і дповідає вимогам, встановленим законодавством для акредитованого центру сертифікації ключів.

Положення про центральний засвідчувальний орган затверджується Кабінетом Міністрів України.

#### Контролюючий орган

Функції контролюючого органу здійснює спеціально уповноважений центральний орган виконавчої влади у сфері криптографічного захисту інформації.

Контролюючий орган перевіряє дотримання вимог цього Закону центральним засвідчувальним органом, засвідчувальними центрами та центрами сертифікації ключів.

У разі невиконання або неналежного виконання обов'язків та виявлення порушень вимог, встановлених законодавством для центру сертифікації ключів, засвідчувального центру, контролюючий орган дає розпорядження центральному засвідчувальному органу про негайне вжиття заходів, передбачених законом.

#### Скасування, блокування та поновлення посиленого сертифіката ключа

Акредитований центр сертифікації ключів негайно скасовує сформований ним посилений сертифікат ключа у разі:

* закінчення строку чинності сертифіката ключа;
* подання заяви власника ключа або його уповноваженого представника;
* припинення діяльності юридичної особи - власника ключа;
* смерті фізичної особи- власника ключа або оголошення його померлим за рішенням суду;
* визнання власника ключа недієздатним за рішенням суду;
* надання власником ключа недостовірних даних;
* компрометації особистого ключа.

Центральний засвідчувальний орган негайно скасовує посилений сертифікат ключа центру сертифікації ключів, засвідчувального центру у разі:

* припинення діяльності з надання послуг електронного цифрового підпису;
* компрометації особистого ключа.

Центральний засвідчувальний орган,засвідчувальний центр, акредитований центр сертифікації ключів негайно блокують посилений сертифікат ключа:

* у разі подання заяви власника ключа або його уповноваженого представника;
* за рішенням суду, що набрало законної сили;
* у разі компрометації особистого ключа.

Скасування і блокування посиленого сертифіката ключа набирає чинності з моменту внесення до реєстру чинних, скасованих і блокованих посилених сертифікатів і з зазначенням дати та часу здійснення цієї операції.

Центральний засвідчувальний орган,засвідчувальний центр, акредитований центр сертифікації ключів негайно повідомляють про скасування або блокування посиленого сертифіката ключа його власника.

Блокований посилений сертифікат ключа поновлюється:

* у разі подання заяви власника ключа або його уповноваженого представника;
* за рішенням суду, що набрало законної сили;
* у разі встановлення недостовірності даних про компрометацію особистого ключа.

#### Припинення діяльності центру сертифікації ключів

Центр сертифікації ключів припиняє свою діяльність відповідно до законодавства.

Про рішення щодо припинення діяльності центр сертифікації ключів повідомляє підписувачів за три місяці,якщо інші строки не визначено законодавством. Підписувачі мають право обирати за власним бажанням будь-який центр сертифікації ключів для подальшого обслуговування, якщо інше непередбачено законодавством. Після повідомлення про припинення діяльності центр сертифікації ключів не має права видавати нові сертифікати ключів.

Усі сертифікати ключів,що були видані центром сертифікації ключів, після припинення його діяльності скасовуються.

Центр сертифікації ключів, що повідомив про припинення своєї діяльності, зобов'язаний забезпечити захист прав споживачів шляхом повернення грошей за послуги, що неможуть надаватися в подальшому, якщо вони були попередньо оплачені.

Акредитований центр сертифікації ключів додатково повідомляє про рішення щодо припинення діяльності центральний засвідчувальний орган або відповідний засвідчувальний центр.

Акредитований центр сертифікації ключів протягом доби, визначеної як дата припинення його діяльності, передає посилені сертифікати ключів, відповідні реєстри посилених сертифікатів ключів та документовану інформацію, яка підлягає обов'язковій передачі, відповідному засвідчувальному центру або центральному засвідчувальному органу.

Порядок передачі акредитованим центром сертифікації ключів посилених сертифікатів ключів, відповідних реєстрів посилених сертифікатів ключів та документованої інформації, яка підлягає обов'язковій передачі, встановлюється Кабінетом Міністрів України.

**Лекція № 4**

**Тема 4. Інформаційне суспільство і правова інформатика. Правовий сегмент інформаційного простору. Інформаційне середовище.**

**План лекції**

Поняття інформаційного суспільства. Інформаційні правовідносини. Концепція інформаційного суспільства З. Бжезинского, Э. Тоффлера. Глобальне інформаційне суспільство. Проблеми інформаційного суспільства. Роль та місце правової інформатики у побудові інформаційного суспільства.

Співвідношення понять «інформаційний простір» і «інформаційне середовище». Рівні інформаційного середовища. Властивості види та функції інформаційного середовища. Єдиний інформаційний простір. Інформаційний простір України. Правовий сегмент інформаційного простору.

**Література**

1. Правова інформатика. / М.Швець, В. Брижко, Л.Задорожня, Ю.Клімашевська, В.Фурашев, В.Хахановський, В.Цимбалюк та ін. – У 2-х т. – К.: Парлам. вид-во, 2005. – Т. 1. – 416 с.
2. Цимбалюк В. С. Інформаційне право (основи теорії і практики). — К.: «Освіта України», 2010. – 388 с.
3. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє / В.Фурашев, Д.Ланде, О.Григор’єв, О.Фурашев. – К.: “Інжиніринг” 2005. – 164 с.
4. Пономаренко В. С., Журавльова І. В., Туманов В. В. Основи захисту інформації. Навчальний посібник. — Харків: Вид. ХДЕУ, 2003. — 176 с.
5. Рубанець О.М. Інформаційне суспільство: когнітивний креатин постнекласичних досліджень [Текст]: монографія / О.М.Рубанець.– К.: ПАРАПАН, 2006.– 420с.
6. Саркисян Д.Б. Международное сотрудничество по формированию глобального информационного общества [Текст] / Д.Б.Саркисян // Научно-техническая информация. Серия "Организация и методика информационной работы".– 2007.– №9.– С.26-33.

**Зміст лекції**

В історії розвитку цивілізації, нерозривно пов'язаної з процесом накопичення знань, багато дослідників відзначають кілька етапів, обумовлених кардинальними змінами в сфері обробки інформації. Наслідком цих змін стали важливі якісні перетворення людського суспільства. До числа таких змін зазвичай відносять появу писемності, перехід до друкарства і використання електрики, винахід радіозв'язку і електронних обчислювальних машин і, нарешті, формування і розвиток глобальних інформаційно-телекомунікаційних мереж.

Кожен з етапів визначили деякі якісні зміни в можливостях використання інформації:

1) можливість фіксації знань на матеріальному носії і передачі знань від покоління до поколінь;

2) можливість активного поширення інформації, її тиражування (середина XVI ст.);

3) використання телеграфу, телефону, радіо, що дозволяють оперативно передавати і накопичувати інформацію (кінець XIX ст.);

4) створення комп'ютерів, комп'ютерних мереж, систем передачі даних (інформаційні комунікації).

Останній період розвитку інформаційних технологій (70-і рр. XX ст.) Характеризують три фундаментальні інновації:

- Перехід від механічних та електричних засобів перетворення інформації до електронних;

- Мініатюризація всіх вузлів, пристроїв, приладів, машин;

- Створення програмно-керованих пристроїв і процесів.

На перший план висувається нова галузь - інформаційна індустрія, пов'язана з виробництвом технічних засобів, методів, технологій для поширення нових знань.

Найважливішими складовими інформаційної індустрії стають всі види інформаційних технологій, особливо телекомунікації. Інформаційні та телекомунікаційні технології активно розвиваються і проникають в усі сфери діяльності - економіку, бізнес, освіту.

Бурхливий розвиток комп'ютерної техніки та інформаційних технологій стимулювало розвиток суспільства, побудованого на використанні інформації та знань і отримав назву інформаційного суспільства.

В останні десятиліття відбулися принципово важливі масові позитивні зміни практично у всіх сферах життя і діяльності людини, які визначаються бурхливим зростанням інформаційних ресурсів і застосуванням інформаційних технологій. Прогрес комп'ютерних інформаційних технологій, комунікаційних систем, електронних засобів масової інформації тощо зачіпає вже сьогодні життєві інтереси кожної конкретної людини.

Відповідно до концепції 3. Бжезинського, Д. Белла, О. Тоффлера, що підтримується і іншими зарубіжними вченими, інформаційне суспільство - це різновид постіндустріального суспільства. При розгляді розвитку суспільства як "зміну ступенів", прибічники цієї концепції інформаційного суспільства пов'язують його становлення з домінуванням "четвертого", інформаційного сектору економіки, який йде за трьома відомими секторами - сільським господарством, промисловістю та економікою послуг. При цьому вони стверджують, що капітал і праця є основою індустріального суспільства, поступаються місцем інформації і знань в інформаційному суспільстві.

Можна відзначити, що в деяких публікаціях підкреслюється "пріоритет інформаційних ресурсів" в інформаційному суспільстві. Вважаємо, що це - небезпечна помилка. Повчальним і загальнодоступним доказом існування такої небезпеки є сюжет відомого науково-фантастичного оповідання. Опинившись в далекому минулому (коли не було необхідних матеріалів і енергетичних ресурсів), наш сучасник, який володів великими знаннями, виявився абсолютно безпорадним, був визнаний обманщиком і страчений. У зв'язку з цим особливого звучання набуває висловлювання одного з основоположників інформатики Ф. Е. Темнікова про необхідність для успішного розвитку суспільства збалансованого використання трьох видів ресурсів - матеріальних, енергетичних та інформаційних.

Існують різні критерії визначення факту переходу суспільства до інформаційної стадії. Так, наприклад, в якості критерію оцінки переходу суспільства до постіндустріальної і далі до інформаційної стадії розвитку може служити відсоток населення, зайнятого в сфері послуг. Якщо в суспільстві більш 50% населення зайнято в сфері послуг, наступила постіндустріальна фаза. Якщо в суспільстві більш 50% населення зайнято в сфері інформаційних послуг, то суспільство стало інформаційним. Згідно з цим критерієм США, наприклад, вступили в постіндустріальний період свого розвитку в 1956 р (штат Каліфорнія подолав цей рубіж ще в 1910 р), а інформаційним суспільством США стали в 1974 р

Однак інформаційне суспільство - суспільство особливе, не відоме історії. Перелічимо основні *особливості і характеристики*[[1]](http://stud.com.ua/72703/informatika/teoretichni_osnovi_pravovoyi_informatiki" \l "srcannot_1) інформаційного суспільства:

• вирішена проблема інформаційної кризи, в тому числі інформаційного кризи науки, тобто дозволено протиріччя між "інформаційною лавиною" і "інформаційним голодом";

• забезпечений пріоритет інформації в порівнянні з іншими ресурсами;

• головною формою розвитку є інформаційна економіка;

• в основу суспільства закладені автоматизовані генерація, зберігання, обробка і використання знань за допомогою новітньої інформаційної техніки і технології;

• інформаційні технології набули глобального характеру, охопивши всі сфери соціальної діяльності людини;

• забезпечено інформаційне єдність всієї людської цивілізації.

*Небезпечні тенденції* інформатизації:

• зростаючий вплив на суспільство засобів масової інформації;

• зростаючі можливості проникнення в приватне життя громадян або організацій за допомогою використання інформаційних технологій;

• усложняющаяся проблема відбору якісної і достовірної інформації;

• збільшення розриву між розробниками і споживачами інформаційних технологій до стратегічно небезпечної величини;

• посилення проблеми адаптації частини людей до середовища інформаційного суспільства.

22 липня 2000 року на о. Окінава Великобританія, Німеччина, Італія, Канада, Росія, США, Франція і Японія прийняли Хартію Глобального інформаційного суспільства . У цій Хартії встановлюються основні принципи входження держав в таке суспільство і проголошуються основні положення, які країни "вісімки" будуть узгоджено застосовувати, а також можуть застосовувати всі інші країни світу. Хартія є найважливішим документом, покликаним організувати та активізувати діяльність країн і урядів на шляху активного формування глобального інформаційного суспільства.

У 1998 році Генеральна Асамблея ООН вирішила провести Всесвітній Саміт з питань інформаційного суспільства. Саміт був проведений в два етапи - в Женеві (2003) і Тунісі (2005).

10-12 грудня 2003 року уперше в історії керівники 175 країн світу зібралися в Женеві для обговорення глобальних проблем інформаційного суспільства. Прийняті на Саміті документи відбили сучасне бачення основних гуманітарних проблем інформаційного суспільства - в філософських, соціально-політичних, соціологічних, культурологічних, технологічних аспектах .

У роботі Саміту в Тунісі (16-18 листопада 2005 року) взяли участь 174 країни, близько 19,5 тис. Учасників, 46 глав держав і віце-президентів, 197 міністрів / заступників міністрів. Були представлені всі основні рушійні сили розвитку інформаційного суспільства - держава, бізнес, громадянське суспільство, організації  .

Існуючі господарські системи інтегруються в економіку знань. Перехід від індустріального до постіндустріального суспільства істотно підсилює роль інтелектуальних чинників виробництва.

Міжнародний досвід показує, що високі технології, в тому числі інформаційні та телекомунікаційні, вже стали локомотивом соціально-економічного розвитку багатьох країн світу, а забезпечення гарантованого вільного доступу громадян до інформації - однієї з найважливіших завдань держав.

В рамках державної інформаційної політики закладені основи для вирішення таких завдань, як формування єдиного інформаційного простору і входження України у світовий інформаційний простір, забезпечення інформаційної безпеки особистості, суспільства і держави, формування демократично орієнтованої масової свідомості, становлення галузі інформаційних послуг, формування та розвитку інформаційного права.

Наступним етапом у розвитку людства буде створення нового суспільства - суспільства інформаційного, гуманного, духовного - *інформаційної цивілізації.*

Сучасна наука приходить до висновку, що цивілізація майбутнього перестане бути техногенної, тобто орієнтованої на техніку. Це буде антропогенне цивілізація, народжена мірками і запитами людини. Звідси і нове глобальне світогляд, інша система цінностей, нові уявлення людини про самого себе і своє призначення. З інформаційної цивілізацією пов'язані надії на якісну зміну соціально-історичної долі людства, вдосконалення способу життя мільйонів людей, їх культури, звичаїв і соціальної поведінки.

*Пріоритет особистості* - ось найважливіший моральний принцип інформаційної цивілізації. Ідеалом суспільства третього тисячоліття має бути суспільство людського благополуччя, в якому держава підпорядковане інтересам особистості, що з'явиться головною умовою і гарантом його волі. У центрі цього суспільства - людина зі своїми унікальними здібностями постійного і безмежного розвитку, створення себе як особистості, гармонізації своїх людських відносин, спрямованих на об'єднання всіх в ім'я блага кожного .

З таким стрибкоподібним підвищенням ролі інформації та інформаційних технологій в сучасному суспільстві пов'язане інтенсивний розвиток фундаментальних і прикладних досліджень в області наук, що об'єднуються інтегруючим поняттям "інформація" - інформатики, кібернетики, теорії інформації, Термін "інформатика" виник в 1960-х рр. у Франції для назви області автоматизованої обробки інформації за допомогою електронних обчислювальних машин. Французький термін *informatique*утворений шляхом злиття слів *information* (інформація) і *automatique*(автоматика) і означає "інформаційна автоматика", або "автоматизована переробка інформації".

В кінці 1960-х рр. поняття "інформатика" пов'язувалося не тільки з інформаційною технікою, а й з теорією наукової інформації ( "документалістикою"). Цьому багато в чому сприяв вихід праці А. І. Михайлова, А. І. Чорного і Р. С. Гиляревський "Основи інформатики" (1968) . У цій роботі були детально розглянуті поняття науково-технічної інформації та методи її обробки.

На Міжнародному конгресі в Японії в 1978 р зазначалося, що "поняття інформатики охоплює області, пов'язані з розробкою, створенням, використанням і матеріально-технічним обслуговуванням систем обробки інформації, включаючи машини, устаткування, математичне забезпечення, організаційні аспекти, а також комплекс промислового, комерційного, адміністративного, соціального і політичного впливу".

Важливими стимулами бурхливого розвитку інформатики як науки в нашій країні послужили дві знаменні події: вихід улітку 1982 р монографії академіка В. М. Глушкова "Основи безпаперової інформатики"  і річне загальні збори Академії наук СРСР в березні 1983 року, на якому було прийнято рішення про створення в рамках Академії нового відділення - інформатики, обчислювальної техніки та автоматизації  . Більш того, з цього моменту ідеї інформатики набули поширення не тільки в науці, але також і серед фахівців-практиків, включаючи і юридичну сферу.

Таким чином, з кінця 1980-х рр. в термін "інформатика" позначає не тільки науку, а й напрямок практичної діяльності. Інформатика як галузь народного господарства складається з однорідної сукупності підприємств різних форм господарювання, пов'язаних з виробництвом комп'ютерної техніки, програмних продуктів і розробкою сучасної технології переробки інформації .

З цього моменту все більшої популярності набуває "французький варіант", згідно з яким інформатика трактується як павука про здійснювану переважно за допомогою автоматичних засобів доцільною обробці інформації. А інформація вивчається з точки зору представлення знань і повідомлень в технічних, економічних і соціальних областях.

Очевидним є те, що обчислювальна техніка зараз здатна вирішувати найрізноманітніші проблеми і завдання, пов'язані зі збором, обробкою і використанням будь-якої інформації. І в цьому сенсі дану техніку слід називати інформаційною, а застосовувані технічні засоби - технічними засобами інформатики. Однак задоволення інформаційних потреб суспільства і людини далеко не завжди залежало від прогресу названих засобів.

Інший підхід до проблеми визначення інформатики як науки був запропонований в 1963 р Ф. Е. темників  , який виступив з ідеєю створення загальної науки про інформацію. Він спробував надати поняттю "інформатика" досить широкий зміст: зокрема, запропонував назвати інформатику інтегральної наукою про інформацію взагалі, що складається з трьох основних частин: теорії інформаційних елементів, теорії інформаційних процесів і теорії інформаційних систем. Це був, на наш погляд, перший важливий поворот у долі поняття "інформатика". Він залишався довго лише історичним фактом. Спроба обгрунтувати нове поняття, довести його необхідність нс була успішною і в належній мірі не оцінена в силу того, що публікація була здійснена в мало відомому, спеціальному журналі.

У наступний період також не існувало єдиної думки щодо змісту поняття "інформатика". Для прикладу, наведемо точки зору деяких вчених, які визначали інформатику наступним чином:

• фундаментальна природнича наука, що вивчає проблеми передачі і обробки інформації (А. П. Єршов);

• наука про перетворення інформації, яка базується на обчислювальній техніці. Предметом інформатики є обчислювальна технологія, як соціально-історичний феномен ... склад інформатики - це три нерозривно і істотно пов'язані складові частини: технічні засоби, програмні та алгоритмічні (А. А. Дородніцин);

• якась синтетична дисципліна, яка включає в себе розробку нової технології наукових досліджень і проектування, заснованої на використанні електронно-обчислювальної техніки, і кілька великих наукових дисциплін, пов'язаних з проблемою спілкування з машиною і, нарешті, зі створенням машини (Η. Н. Моїсеєв );

• комплексна наукова і технологічна дисципліна, яка вивчає, перш за все, найважливіші аспекти розробки, проектування, створення, "вбудовування" машинних систем обробки даних, а також їх впливу на життя суспільства (В. С. Михалевич);

• наука про проблеми обробки різних видів інформації, створення нових видів високоефективних ЕОМ, що дозволяє представляти людині широкий спектр інформаційних ресурсів (Е. А. Якубайтіс);

• наука, техніка і застосування машинної обробки, зберігання та передачі інформації (М. Брой);

• наукова дисципліна, що вивчає закономірності отримання, відбору, зберігання, передачі, перетворення і застосування інформації у виробничій, науковій, суспільно-політичній і культурній діяльності людей  ;

• наукова дисципліна, що вивчає структуру і загальні властивості інформації, а також закономірності всіх процесів обміну інформацією при безпосередньому усному і письмовому спілкуванні фахівців до формальних процесів обміну за допомогою різних носіїв інформації  ;

• галузь науки, що вивчає структуру і загальні властивості наукової інформації, а також питання, пов'язані з її збиранням, зберіганням, пошуком, переробкою, перетворенням, поширенням і використанням в різних сферах людської діяльності  ;

• галузь науки, що досліджує властивості і поведінку інформації; сили, що керують потоком інформації; засоби обробки інформації з метою забезпечення її оптимальної доступності та використання *(information science)* .

Якщо взяти до уваги тільки найбільш близькі за сукупністю розглянутих питань підходи, можна запропонувати наступне визначення інформатики.

*Інформатика* - наука, що вивчає структуру і загальні властивості інформації, закономірності розвитку інформаційних процесів, інформаційних технологій та інформаційних систем в різних областях людської діяльності.

З визначення видно, що основними об'єктами дослідження в інформатиці є:

а) *інформація* як об'єкт особливого роду, її особливості та властивості; мотивація, підстави і цілі виробництва, перетворення і споживання інформації; класифікація інформації та інформаційних об'єктів; проблеми оцінки якості інформації; роль інформації в прийнятті рішень;

б) *інформаційні процеси* як процеси збору, виробництва, поширення, перетворення, пошуку, отримання, передачі та споживання інформації;

в) *інформаційні технології та інформаційні системи,* в тому числі автоматизовані інформаційні системи (ЛІС), комп'ютерні мережі, інші інформаційно-комунікаційні технології на основі використання засобів обчислювальної техніки, зв'язку і телекомунікацій.

Основними *завданнями інформатики* є:

1) визначення загальних закономірностей, відповідно до яких відбуваються процеси створення, перетворення, передачі і використання інформації в різних сферах діяльності людини;

2) розробка більш ефективних методів і засобів здійснення інформаційних процесів, визначення способів оптимальної інформаційної комунікації на базі активного використання сучасних технічних засобів.

генетики та ін.

**Лекція № 5**

**Тема 5. Довідкові правові системи. Автоматизовані правові аналітико-статистичні інформаційні системи, системи обліку і управління**

**План лекції**

Основні характеристики довідкових правових систем. Принципи пошуку документів в довідкових правових системах. Довідкова правова система «ЛІГА» (об'єм і склад інформаційних ресурсів, складання пошукових запитів, особливості роботи системи, використання логічних умов в пошукових запитах). Довідкова правова система «РАДА» (об'єм і склад інформаційних ресурсів, банки даних), області використання системи. Перспективи вживання довідкових правових систем в юридичній діяльності.

Бази та банки даних. Системи управління базами даних (СУБД).Загальна характеристика інформаційно-пошукових систем законодавства.Призначення і принципи використання автоматизованих аналітико-статистичних інформаційних систем.

**Література**

1. Баранов О. Понятійний апарат  інформаційного права / О.Баранов // Правова інформатика. – 2007. - № 3 (15). – С. 33-39.
2. Карпенков С.Х. Концепция современного естествознания: учеб. Для вузов / С.Х. Карпенков. – 6-е изд., перероб. и доп. – М.: Высш. шк., 2003. – 488 с.
3. Лисин Н. Лоскутная автоматизация, или как управлять «зоопарком» программ / Н. Лисин. – Електронний ресурс. – Режим доступу:<http://www.bytemag.ru/articles/detail.php?ID=14862>
4. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 23 лютого 2002 року № 9 // Офіційний вісник України. – 2002. - № 12. – Ст. 624.
5. Положення про технічний захист інформації в Україні: Указ Президента України від 27 вересня 1999 року № 1229/99 // Офіційний вісник України. – 1999. - № 39. – Ст. 28.
6. Про державну статистику: Закон України від 17 вересня 1992 року № 2614-ХІІ // Відомості Верховної Ради України. – 1992. - № 43. – Ст. 608.
7. Про затвердження Інструкції про умови і правила провадження підприємницької діяльності (ліцензійні умови), пов'язаної з розробленням, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів технічного захисту інформації, а також з наданням послуг із технічного захисту інформації, та контроль за їх дотриманням: наказ Ліцензійної палати України, Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 жовтня 2000 року № 92/80 // Офіційний вісник України. – 1998. - № 43. – Ст. 88.
8. Про затвердження Положення про електронні освітні ресурси: Наказ Міністерства освіти і науки, молоді і спорту України від 01 жовтня 2012 року № 1060 // Офіційний вісник України. – 2012. - № 80. – Ст. 3231.
9. Про затвердження Порядку інформаційної взаємодії між кадастрами та інформаційними системами: Постанова Кабінету Міністрів України від 03 червня 2013 року № 483 // офіційний вісник України. – 2013. - № 53- Ст. 1934.
10. Про затвердження Порядку обміну фінансово-економічними даними в інформаційно-телекомунікаційній системі «Фінанси»: Наказ Міністерства фінансів України від 16 липня 2008 року № 943 // Офіційний вісник України. – 2008. - № 59. – Ст. 2004.
11. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України: Закон України від 05 липня 1994 року № 80/94-ВР // Відомості Верховної Ради України. – 1994. - № 31. – Ст. 286.
12. Про Національний архівний фонд та архівні установи: Закон України від 24 грудня 1993 року № 3814-ХІІ // Відомості Верховної Ради України. – 1994. - № 15. – Ст. 86.
13. Про Національну програму інформатизації: Закон України від 04 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України. – 1998. - № 27. – Ст. 181.
14. Про статус і соціальний захист громадян, які постраждали внаслідок Чорнобильської катастрофи: Закон України від 28 лютого 1991 року № 796-ХІІ // Відомості Верховної Ради України. – 1991. - № 16. – Ст. 200.
15. Сазонець О. М. Інформаційні системи і технології в управлінні зовнішньоекономічною діяльністю [текст] : навч. посіб. / О. М. Сазонець. – К. : «Центр учбової літератури», 2014. – 256 с.
16. Сучасні інформаційні системи і технології: конспект лекцій / В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін.; за заг. ред. В. Г. Іванова, В. В. Карасюка. – Х.: Нац. юрид. ун-т ім. Ярослава Мудрого, 2014. – 347 с.

**Зміст лекції**

Створення сучасних ЕОМ дало можливість автоматизувати обробку даних у всіх галузях людської діяльності. Без системи обробки даних неможливо уявити промислові технології, управлінні економікою на всіх рівнях та сферах, наукові дослідження, освіту, роботу транспорту, видавничу справу тощо. Значно розширилися сфери застосування комп’ютерної техніки з появою персональних комп’ютерів і комп’ютерних мереж. Найбільш розповсюдженими системами обробки даних є інформаційні системи.

 Ринкова система господарювання в умовах формування інформаційного суспільства дозволила швидко наситити ринок інформаційними системами. Водночас, за оцінками фахівців, на ринку є десятки тисяч інформаційних систем та комп’ютерних систем з різних напрямів застосування. З появою персональних комп’ютерів користувачами інформаційних систем стали не тільки підприємства, але й фізичні особи, незалежно від віку, освіти та статі, спеціалісти будь-якої професії, науковці, співробітники сфери торгівлі, мистецтва та інші.

 Водночас постійно здійснюється вдосконалення інформаційних систем, доробки цих програм під нові потреби людей для подальшого удосконалення забезпечення організаційних, технічних і комерційних умов.

Системний підхід до різних явищ і процесів дослідницької діяльності, збільшення обсягу інформації потребувало вирішення питання про систематизоване збереження інформації.

 Термін «інформаційна система» широко використовується у законодавчих та підзаконних актах, що регулюють сферу інформаційних правовідносин, однак відсутній єдиний підхід до його визначення та розуміння. Так, у частині 1 статті 16 Закону України «Про статус і соціальний захист громадян, які постраждали внаслідок Чорнобильської катастрофи» вживається поняття «Державний реєстр України (єдина інформаційна система)», однак не розкрито його поняття в даному законодавчому акті.

 Одне з перших офіційних визначень аналізованого поняття міститься у пункті 5 частині 1 статті 1 Закону України «Про державну статистику», відповідно до якого інформаційна система органів державної статистики – це сукупність технічних, програмних, комунікаційних та інших засобів, які забезпечують процес збирання, накопичення, опрацювання, поширення, збереження, захисту та використання статистичної інформації.

 Змістовий аналіз цього Закону показує, що в даному випадку під інформаційною системою фактично розуміється система, що побудована при використанні технічних, програмних і технічних засобів. При цьому зазначено про конкретні функціональні можливості інформаційної системи: «збирання, накопичення, опрацювання, поширення, збереження, захисту та використання» інформації. Однак, недоліком даного визначення є те, що відсутність таких важливих функцій як «введення та збір даних», яка покликана забезпечити наповнення інформаційної системи органів державної статистики .

Необхідно зазначити, що у процесі встановлення правового регулювання інформаційних систем у різні часи застосовувалися різні підходи до їх визначення. У значній кількості нормативно-правових актів, акцентовано увагу на одній із ознак інформаційної системи як «автоматизація»:

1)   інформаційна система – це автоматизована система, комп’ютерна мережа, система зв’язку [7];

2)   інформаційна система – це автоматизована система, комп’ютерна мережа або система зв’язку (пункт 5 частини 1 статті 2 Положення про технічний захист інформації  в Україні) [5];

3)   інформаційна система – це автоматизована система, комп’ютерна мережа або система зв’язку (пункт 2 частини 1 статті 2 Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб) [4];

4)   інформаційна (автоматизована) система – це організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів (пункт 8 частини 1 статті 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах») [11].

Разом з тим, згідно статті 1 Закону України «Про національну програму інформатизації» [13], до інформаційних систем, що забезпечують функціонування інформаційних ресурсів належать: бібліотеки, архіви, банки даних тощо.

 Таким чином термін інформаційна система охоплює не лише технологічну, але і організаційну основу інформаційного ресурсу. Адже, наприклад, архів, згідно статті 1 Закону України «Про Національний архівний фонд та архівні установи» [12] представляє собою установу чи структурний підрозділ, що забезпечує облік і зберігання архівних документів, використання відомостей, що в них містяться. Але слід розуміти, що в даному випадку організаційну та технологічну складові інформаційного ресурсу слід розглядати як взаємодоповнюючі елементи.

У свою чергу законодавець під поняттям автоматизована система визначив організаційно-технічну систему, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів (пункт 1 частини 2 статті 1 Порядку обміну фінансово-економічними даними в інформаційно-телекомунікаційній системі «Фінанси») [10].

Це досить широкі визначення, що дозволяє віднести до інформаційних систем всі без винятку автоматизовані системи, комп’ютерні мережі та системи зв’язку. Вочевидь, такий підхід невірний, оскільки дає можливість віднести до інформаційних систем технологічні системи автоматизації аж до верстатів з числовим програмних управлінням, а з іншої сторони, виключає з переліку інформаційні системи, що не мають комп’ютерних та телекомунікаційних технічних засобів.

У законодавстві містяться також інші підходи до визначення поняття інформаційної системи: як кадастрову, геоінформаційна система чи база геопросторових даних (пункт 4 частини 2 статті 1 Порядку інформаційної взаємодії між кадастрами та інформаційними системами [9]); як організаційно впорядковану сукупність документів (масивів документів) та інформаційні технології, в тому числі з використанням технічних засобів, що реалізують інформаційні процеси та призначені для зберігання, обробки, пошуку, розповсюдження, передачі та наданні інформації (частина 5 пункту 2.1 Положення про електронні освітні ресурси) [8]; як комплекс, що включає обчислювальне і комунікаційне обслуговування, програмне забезпечення, лінгвістичні засади та інформаційні ресурси, а також системний персонал. Цей комплекс забезпечує підтримку динамічної інформаційної моделі деякої частини реального світу для забезпечення інформаційних потреб користувачів [16, с. 21].

При цьому слід звернути увагу, що «ручні інформаційні системи» («без комп’ютера») існувати не можуть, оскільки існуючі визначення показують обов’язкову наявність у складі інформаційних систем апаратно-програмних засобів. Внаслідок цього поняття «автоматизована інформаційна система», «комп’ютерна інформаційна система» і просто «інформаційна система» є синонімами.

Таким чином, в інформаційному законодавстві України має місце неоднозначне визначення терміну “інформаційна система”. Більше того, наявні визначення, розкриваючи термін “інформаційна система” як правову категорію, відносять до сфері правового регулювання суспільні відносини, які базуються тільки на використанні комп'ютерних технологій, що значно звужує поле правового регулювання. Насправді ж перелік предметних областей, в яких використовується поняття “інформаційна система” як правова категорія, набагато ширший.

Перш за все, визначимо функціональне призначення інформаційних систем. У широкому сенсі інформаційні системи призначені для своєчасного забезпечення та задоволення та потреб користувачів в інформації. Наприклад, у діяльності підприємств існує практика створення та функціонування єдиної корпоративної інформаційної системи, що задовольняє інформаційні потреби усіх співробітників, служб та підрозділів організації. Однак на практиці створення всеохоплюючої інформаційної системи складне та у певній мірі, навіть неможливе завдання, унаслідок чого на підприємстві переважно функціонують декілька різних систем, які вирішують окремі групи завдань: управління виробництвом, фінансово-господарська діяльність, електронний документообіг тощо. Частина цих завдань виконується одночасно кількома інформаційними системами, частина завдань – зовсім не автоматизована. Така ситуація отримала назву «клаптикова автоматизація» і є досить типовою для багатьох підприємств [3].

 Виходячи з того, що задоволення інформаційних потреб відбувається в результаті реалізації певних інформаційних процесів, вважатимемо, що основне функціональне призначення інформаційних систем – це забезпечення інформаційних процесів, зокрема, забезпечення створення, поширення, використання, збереження і знищення (утилізації) інформації. Такий підхід до визначення функціонального призначення інформаційних систем забезпечує інваріантність як до видів інформації й інформаційних ресурсів, так і до видів і типів інформаційних технологій, які використовуються для реалізації інформаційних процесів. Таким чином, до інформаційних систем стає можливим віднести: видавництва, бібліотеки, архіви, засоби масової інформації, телекомунікації, Інтернет тощо.

З урахуванням вищесказаного можна погодитися із наступним визначенням терміну “інформаційна система” – це організований комплекс організаційно-технічних заходів (сукупність підприємств, підрозділів і фахівців), а також безпосередньо інформаційних технологій і інформаційних ресурсів, призначених для забезпечення функціонування інформаційних процесів, зокрема забезпечення створення, поширення, використання, систематизації, збереження і знищення інформації.

Дане визначення поняття “інформаційні системи” має важливе методологічне значення для визначення об'єкта правовідносин у сфері інформаційного права завдяки тому, що високий рівень абстракції дає можливість охопити всі без винятку інформаційні системи, які забезпечують створення, поширення, використання, збереження і знищення (утилізацію) інформації, відомі на сьогодні і які можуть з'явитися в майбутньому. Сформульований термін “інформаційна система” дозволяє віднести його до родових понять, на базі яких можуть формуватися інші конкретні поняття для певних предметних сфер завдяки додатковій конкретизації і деталізації [1, с. 37].

За суттю інформаційна система є цілісною системою і цілком очевидно вона має всі властивості системи такого роду:

1. залежно від виду і конкретного призначення інформаційна система має якості, які не можуть бути зведені до властивостей елементів, що її утворюють;
2. якісні характеристики конкретної інформаційної системи залежать від якісних характеристик її елементів;
3. між елементами інформаційної системи існує зв’язок, причому, коли відбувається зміна одного компонента системи, то це призводить до зміни іншого, а іноді і системи в цілому;
4. інформаційну систему як цілісне утворення характеризує впорядкованість елементів, які її утворюють, а також зв’язків і відношень між ними;
5. інформаційна система не існує ізольовано, ця властивість проявляється у взаємозв’язку системи з іншими системами.

Інформаційна система, яка використовується науковцем, має відмінності від інших, які функціонують у різних галузях діяльності: вона повинна бути регламентована законом чи підзаконним актом, тобто юридично регламентована;  метою запобігання незаконному використанню відомостей цієї системи вона повинна бути захищена від стороннього втручання; бробка відомостей у такій системі повинна відповідати завданням наукової діяльності; в інформаційній системі у науковій сфері розміщують відомості про досліджувані об’єкти, банки даних, експериментальні дані, інформаційно-довідкові каталоги, алгоритми виконання завдань, інформаційні технології і таке інше.

 Впровадження комп'ютерної техніки дозволяє збільшити швидкість введення інформації, її обробку й одержання відповіді, що підвищує ефективність праці.

 Інформаційні системи, що створюються на базі ЕОМ, мають свої особливості і переваги: за допомогою ЕОМ в інформаційній системі можна зберігати більше інформації, ніж у системах ручного і механізованого типу; інформацію за допомогою каналів зв'язку можна передавати іншим інформаційним системам, користувачам; інформацію можна зосереджувати в одному місці незалежно від місця її одержання.

 Існує декілька підходів до класифікації інформаційних систем:

1)   за характером організації пошуку виокремлюють системи:

-      інформаційно-пошукові;

-      інформаційно-управлінські;

-      інформаційно-довідкові;

2)   за реалізацією режиму поширення та пошуку інформації розрізняють:

-      системи з режимом вибіркового поширення та пошуку інформації;

-      системи з ретроспективним режимом поширення і пошуку;

-      інтегральні системи;

3)   за характером функціональності інформаційні системи діляться на:

-      монофункціональні;

-      багатофункціональні;

4)   за масштабністю реалізації:

-      глобальні;

-      регіональні;

-      локальні;

5)   за рівнем безпеки:

-      інформаційні системи з найвищим рівнем безпеки;

-      з високими рівнем безпеки;

-      з низькими рівнем безпеки.

6)   за особливістю архітектури:

-      настільні (локальні) інформаційні системи, в яких  усі компоненти (база даних, , клієнтські програми) знаходяться на одному комп’ютері;

-      розподілені інформаційні системи, в яких компоненти розгалужені на декілька комп’ютерів;

7)    за ступенем автоматизації інформаційні системи поділяють на:

- автоматизовані, інформаційні системи в яких автоматизація може бути не повно, оскільки потрібне постійне втручання персоналу);

- автоматичні, це інформаційні системи, в яких автоматизація є повною, тобто не потрібне втручання персоналу або потрібно тільки епізодично;

8)    за характером обробки даних:

-      інформаційно-довідкові або інформаційно-пошукові ІС, в яких не має складних алгоритмів обробки даних, а метою системи є пошук і видача інформації  в зручному вигляді;

- інформаційні системи обробки даних, або вирішальні інформаційні системи, в яких дані піддаються обробці за складними алгоритмами. (автоматизовані системи управління; системи прийняття рішень);

9) за сферою застосування, оскільки інформаційні системи створюються для задоволення інформаційних потреб у рамках конкретної предметної області, то кожній предметній області (сфері застосування) відповідає свій тип інформаційної системи. Перераховувати всі ці типи не має сенсу, тому що кількість предметних областей дуже велика, але можна вказати як приклад наступні типи інформаційних систем:

- інформаційно-довідкова система – інформаційна система, призначена для пошуку інформації у рамках певної предметної області;

- економічна інформаційна система – інформаційна система, призначена для виконання функцій управління на підприємстві;

- інформаційно-аналітична система криміналістичних обліків – інформаційна система, призначена для аналітичної підтримки правоохоронної діяльності;

- медична інформаційна система – інформаційна система, призначена для використання в лікувальному чи лікувально-профілактичному закладі;

- географічна інформаційна система – інформаційна система, що забезпечує збір, зберігання, обробку, доступ, відображення і розповсюдження просторово-координованих даних (просторових даних);

10) за масштабністю охоплення завдань:

-       персональна інформаційна система призначена для вирішення деякого кола завдань однієї людини;

-       групова інформаційна система орієнтована на колективне використання інформації членами робочої групи або підрозділу;

-      корпоративна інформаційна система в ідеалі охоплює всі інформаційні процеси цілого підприємства, забезпечуючи їх повну узгодженість і прозорість. Такі системи іноді називають системами комплексної автоматизації підприємства.

 Схоже, що найбільше застосовування у науковій та емпіричній діяльності має поділ інформаційних систем за сферою застосування. Наведені вище критерії до систематизації інформаційних систем є доволі всеохоплюючими та, видається, що створення нових авторських підходів до систематизації навряд чи буде мати велику наукову цінність.

З огляду на важливість з’ясування змісту поняття «інформаційна система», а також неоднозначність визначення даного терміну як у законодавчому так і науковому обігу, можна погодитися із наступним визначенням терміну “інформаційна система” – це організаційно-технічна система, в якій за допомогою технічних та програмних засобів здійснюється забезпечення функціонування інформаційних процесів, зокрема забезпечення створення, поширення, використання, обробка, систематизації, збереження і знищення інформації.

Існування вітчизняному законодавстві визначень деяких видів інформаційних систем та відсутність їх повної класифікації в науковій літературі дозволяє погодитися із проведеною класифікацію інформаційних систем за різноманітними критеріями: за характером організації пошуку; за режимом поширення та пошуку інформації; за характером функціональності; за масштабністю реалізації; за рівнем безпеки; за степенем автоматизації; за характером обробки даних; за сферою застосування тощо.

# Комп’ютерна правова система ЛІГА:ЗАКОН

Однією з найбільш популярних комп’ютерних правових систем в Україні є спеціалізована інформаційно-пошукова система **«ЛІГА:ЗАКОН»**(розробка інформаційно-аналітичного центру «Ліга», http://www.liga.kiev.ua). Система складається з програмної оболонки, яка забезпечує пошук документів, та інформаційного ядра — текстових баз даних нормативних документів:

* ·«Загальне законодавство» — документи, прийняті вищими органами влади України: Верховною Радою України з 1990 р., Кабінетом Міністрів України з 1991 р., Президентом України з 1991 р., а також документи міністерств і відомств, які зареєстровані Міністерством юстиції України з 1993 р.; «Кодекси» — усі чинні кодекси України в контрольному стані;
* ·«Податки в Україні» — роз’яснення, листи, накази та інструкції Державної податкової адміністрації; листи, телеграми та інші документи НБУ та Міністерства фінансів; документи фінансового права, прийняті вищими органами влади, міністерствами і відомствами;
* ·«Міжнародні угоди» — міжнародні договори, угоди, конвенції;
* ·«Митне право» — документи, що регламентують митне право, видані Державною митною службою, вищими органами влади, міністерствами і відомствами;
* ·«Різне» — документи про кадрові перестановки;
* ·«ЛІГА:Столиця» — довідкова база нормативних документів, що регламентують ділове життя м. Києва;
* ·«Регіони» — документи, прийняті регіональними органами влади;
* ·«Консультації» — актуальні матеріали у вигляді анотацій статей, коментарів, відповідей на запитання з більше ніж 30 економічних видань із проблем оподаткування, підприємництва, зов­нішньоекономічної діяльності, валютного регулювання, починаючи з 1999 р.;
* ·«Типові договори і форми» — систематизовані посилання на нормативні документи, якими затверджені різні типові статути, договори, форми тощо; зразки цивільно-правових договорів і процесуальних документів;
* ·«Довідники» — довідково-аналітичні матеріали за різними напрямками (державні класифікатори, плани рахунків, ставки зборів, тарифи тощо), оформлені у вигляді систематизованих посилань на нормативні документи чи зведених таблиць; курси валют, індекси інфляції тощо з можливістю побудови динамічних графіків та їх масштабування;
* ·«Термінологічний словник» — терміни і поняття, що вживаються у нормативно-правових актах; «Моніторинг законодавства» — анотації фахівців ІАЦ «ЛІГА» до нових документів, що надходять у систему.

Система «ЛІГА:ЗАКОН» поставляється у версіях «Стандарт» і «Професіонал», які різняться за повнотою функцій та інформаційним наповненням. На основі ІПС «ЛІГА:ЗАКОН» розроблено тематичні комп’ютерні довідники, які містять у собі стандартний програмний комплекс і спеціалізоване інформаційне ядро — нормативні документи, консультації фахівців, огляд преси та довідкову інфор­мацію з певних питань:

* ·«ЛІГА:Консультант БУХГАЛТЕРА» — бухгалтерський облік, оподатковування, деякі особливості підприємницької діяльності;
* ·«ЛІГА:Консультант ЗЕД» — зовнішньоекономічна діяльність, валютне і митне регулювання, валютний контроль;
* ·«ЛІГА:ПРАКТИК-керівник» — підприємництво, бухгалтерський облік, оподатковування, зовнішньоекономічна діяльність, валютне і митне регулювання, валютний контроль, антимонополь­не законодавство, ліцензування, сертифікація, торгівля і побутове обслуговування.

Спільні особливості систем такі:

* ·зберігання текстів документів у форматах, близьких до поліграфічних, з наявністю гіпертекстових посилань і графічно зображених зв’язків між документами; розміщення всіх редакцій документів у хронологічній послідовності; контрольний стан документів, відстеження всіх змін і доповнень; систематизація документів за 35 тематичними напрямками;
* ·доступ до еталонних редакцій нормативних документів, що ідентичні внесеним до Єдиного державного реєстру нормативних актів;
* ·двомовний (український/російський) інтерфейс і пошук, мож­ливість автоматичного підрядкового перекладу;
* ·можливості ведення власних добірок документів з їх інтеграцією у папки, створення 4 типів простих закладок

# Бази даних, банк даних, інформаційна система. Традиційні файлові системи. Бази даних. Системи управління базами даних (субд).

**Основні поннятя:**

База даних (скорочено — БД) — впорядкований набір логічно взаємопов'язаних даних, що використовуються спільно та призначені для задовільненя інформаційних потреб користувачів. У технічному розумінні включно й система керування БД.

Головне завдання БД — гарантоване збереження значних обсягів інформації та надання доступу до неї користувачеві або ж прикладній програмі. Таким чином, БД складається з двох частин: збереженої інформації та системи керування нею.

З метою забезпечення ефективності доступу записи даних організовують як множину фактів (елемент даних).

Дані (date) — це компонент БД, над яким виконуються в ІС дії.

Банк даних (data bank) - це автоматизована система, сукупність інформаційних, програмних, технічних засобів і персоналу, що забезпечує зберігання, нагромадження, оновлення, пошук і видачу даних.

**База даних та банк даних , інформаційна система:**

До складу БнД входять такі складові: сукупність технічного та програмного забезпечення, база даних, СУБД, словник даних, адміністратор БД.

Головні складові банк у даних — база даних і програмний продукт, який називається системою управління базою даних (СУБД).

Система управління базами даних (СУБД) — це програмні засоби, за допомогою яких можна створювати бази даних, поповнювати їх та працювати з ними.

Банк даних (БнД) — це автоматизована система, сукупність інформаційних, програмних, технічних засобів і персоналу, що забезпечує зберігання, нагромадження, оновлення, пошук і видачу даних.

На всіх етапах життєвого циклу БД складається з двох компонентів: структури та даних. На різних рівнях опису БД її структура зображується:

* на інфологічному рівні (сутність — зв’язок);
* на датологічному рівні вона може бути однією з моделей даних — ієрархічною, мережевою, реляційною.
* на фізичному рівні (структура файлів даних і допоміжних файлів).

Більшість баз даних мають табличну структуру.

Файли даних також складаються зі структури та даних. Структура охоплює такі компоненти: ім’я поля, тип поля, довжина поля.

Використання принципів бази та банку даних передбачає організацію зберігання інформації у вигляді БД.Така організація даних усуває цілий ряд проблем:

1.відпадає потреба в кожній прикладній програмі детально вирішувати питання організації файлів;

2.усуває багаторазове введення й дублювання одних і тих самих даних;

3.не виникає проблеми зміни прикладних програм у зв’язку із заміною фізичних пристроїв або зміни структури даних;

4.підвищує рівень надійності та захищеності інформації;

5.зменшує надлишок даних.

Технологія баз і банків — провідний напрям організації внутрішньомашинного інформаційного забезпечення. Розвиток технологій баз і банків даних визначається рядом чинників: ростом інформаційних потреб користувачів, вимогами ефективного доступу до інформації, появою видів масової пам’яті, збільшенням її об’ємів, новими засобами та можливостями в галузі комунікації.

Адміністратор БД (АБД) — особа або група осіб, які відповідають за загальне керування БД. Важливе завдання адміністратора БД — захист даних від злому, несанкціонованого та некомпетентного доступу.

Для виконання функції адміністратора в СУБД передбачено різні службові програми. Адміністрування БД передбачає виконання функцій для забезпечення надійної та ефективної роботи бази даних, задоволення інформаційних потреб користувача.

**Традиційні файлові системи**

традиційних пакетних системах обробки інформації, які функціонували донедавна на машинах типу ЄС ЕОМ, дані були організовані у вигляді незв'язаних між собою локальних інформаційних файлів лінійної структури. Суть такого підходу до організації інформаційного забезпечення (І3) полягає в тому, що файли проектуються окремо для кожної конкретної задачі чи для їх комплексів. Такі системи інколи називаються файловими.

Незважаючи на відносну простоту організації файлові системи мають ряд недоліків, головними з яких є такі.

1. Надлишковість даних. Файлові системи характеризуються значною надлишковістю, оскільки нерідко для розв'язування різних задач управління використовуються одні й ті самі дані, розміщені в різних файлах.

Через дублювання даних у різних файлах пам'ять на зовнішніх запам'ятовуючих пристроях використовується неекономно, інформація одного й того самого об'єкта управління розподіляється між багатьма файлами. При цьому досить важко уявити загальну інформаційну модель предметної області.

2. Неузгодженість даних. Ураховуючи, що одна і та сама інформація може розміщуватися в різних файлах, технологічно важко простежити за внесенням змін одночасно в усі файли. Через це може виникнути неузгодженість даних, коли одне і те саме поле в різних файлах може мати різні значення.

3. 3алежність структур даних і прикладних програм. При файловій організації логічна і фізична структури файла мають відповідати їх опису в прикладній програмі. Прикладна програма має бути модифікована при будь-якій зміні логічної чи фізичної структури файла. Оскільки зміни в одній програмі часто потребують внесення змін до інших інформаційно пов'язаних програм, то інколи простіше створити нову програму, ніж вносити зміни в стару. Тому цей недолік файлових систем призводить до значного збільшення вартості супроводження програмних засобів. Зазначимо, що інколи вартість супроводження програмних засобів може досягати близько 70 % вартості їх розробки.

**Компоненти банку даних**

· Інформаційна база;

· Лінгвістичні засоби;

· Програмні засоби;

· Технічні засоби;

· Організаційно-адміністративні підсистеми та нормативно-методичне забезпечення.

**Лекція № 6**

**Тема6. Правова інформатика в системі забезпечення захисту персональних даних.**

**План лекції**

Поняття «персональні дані». Порядок реєстрації бази персональних даних. Захист персональних даних в мережі Інтернет. Проблемні питання захисту персональних даних в Україні.

**Література**

1. Аналіз Закону України про захист персональних даних: DGI/ DP/expertiseUKR(2012) / М. Жорж, Г. Саттон. – Страсбург: Рада Європи, 2012. – 63 с.

2. Бобрик В. І. Право власності на персональні дані [Електронний ресурс] / В. І. Бобрик // Вісник Хмельницького інституту регіонального управління та права. – 2002. – № 2. – С. 114– 117.

3. Булеца С. Б. Персональні дані пацієнта [Електронний ресурс] / С. Б. Булеца // Науковий вісник Ужгородського національного університету. Сер.: Право. – 2014. – Вип. 25. – С. 56–61.

4. Городиський І. М. Виконання Україною міжнародних зобов’язань із захисту персональних даних / І. М. Городиський // Інтеграція України в Європейське інформаційне суспільство: виклики та завдання / Упор. Пазюк А. В.; Рец. Гріненко О. О., Олійник О. В. – К.: ФОП Клименко, 2014. – С. 89–97.

5. Дмитренко О. А. Право фізичної особи на власні персональні дані в цивільному праві України [Текст]: автореф. дис. ... канд. юрид. наук: 12.00.03 / О. А. Дмитренко; НДІ приват. права і п-ва Акад. прав. наук України. – К., 2010. – 19 с.

6. Дмитренко О. А. Право фізичної особи на власні персональні дані в цивільному праві України [Текст]: дис. ... канд. юрид. наук: 12.00.03 / О. А. Дмитренко; НДІ приват. права і підприємництва Акад. прав. наук України. – К., 2010. – 210 арк. – Бібліогр.: арк. 187–210.

7. Інтеграція України в Європейське інформаційне суспільство: виклики та завдання / Упор. Пазюк А. В. ; Рец. Гріненко О. О., Олійник О. В. – К.: ФОП Клименко, 2014. – 221 c.

8. Каретник О. С. Поняття інформації про фізичну особу (персональні дані) в цивільному праві України [Електронний ре- 178 Захист персональних даних: правове регулювання та практичні аспекти сурс] / О. С. Каретник // Часопис Київського університету права. – 2013. – № 2. – С. 228–231.

9. Косіцин М. Проблемні питання правового регулювання повноважень Держспецзв’язку України із захисту інформації про персональні дані / М. Косіцин, Е. Плешко // Прав., нормат. та метрол. забезп. системи захисту інформації в Україні. – 2010. – Вип. 2. – С. 10–13.

10. Макушев П. В. Персональні дані як елемент системи інформаційного забезпечення державної виконавчої служби України / П. В. Макушев // Форум права. – 2013. – № 2. – С. 333–339.

11. Макушев П. В. Системи інформаційного забезпечення державної виконавчої служби України та персональні дані як їх складові / П. В. Макушев // Право і суспільство. – 2013. – № 4. – С. 70–76.

12. Оніщенко О. В. Персональні дані працівників: деякі особливості використання / О. В. Оніщенко // Вісник Академії адвокатури України. – 2012. – Число 3. – С. 173–175.

13. Пазюк А. В. Захист прав громадян у зв’язку з обробкою персональних даних у правоохоронній діяльності: європейські стандарти і Україна / А. В. Пазюк. – К.: МГО «Прайвесі Юкрейн», 2001. – 260 c.

14. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації:Автореф. дис... канд. юрид. наук: 12.00.11 / А. В. Пазюк; Київ. нац. ун-т ім. Т. Шевченка. – К., 2004. – 19 c.

15. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / В. М.Брижко, А. І.Радянська, М. Я.Швець. – К.: Тріумф, 2006. – 256 с.

16. Посібник з європейського права у сфері захисту персональних даних. – К.: К.І.С., 2015. – 216 с.

17. Погребна А. Коментар до Закону України «Про захист персональних даних» / А. Погребна // Юридичний журнал. – 2010. – №7. – [Електронний ресурс]. Цит. 02.09.2010 р. Доступно з – http://www.justinian.com.ua/article.php?id=3579 18. Романюк І. Особливості змісту та реалізації права на персональні дані в Україні та зарубіжних країнах / І. Романюк // Список рекомендованої літератури: 179 Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки. – 2013. – Вип. 2. – С. 102–106.

19. Романюк І. І. Персональні дані особи як об’єкт цивільного обороту / І. І. Романюк // Право і суспільство. – 2014. – № 6.1(2). – С. 58–65.

20. Сопілко І. М. Генезис змісту категорії «персональні дані» / І. М. Сопілко // Юридичний вісник. Повітряне і космічне право. – 2013. – № 4. – С. 62–66.

21. Чанишев Р. І. Інформація про персональні дані працівника та її захист / Р. І. Чанишев // Актуальні проблеми держави і права. – 2010. – Вип. 52. – С. 94–99. 22. Чанишева Г. І. Право на інформацію за трудовим законодавством України: монографія / Г. І. Чанишева, Р. І. Чанишев. – О.: Фенікс, 2012. – 193 c.

23. Щербіна А. О. Персональні дані в системі інформаційного забезпечення органів місцевого самоврядування / А. О. Щербіна, П. В. Макушев // Публічне право. – 2013. – № 3. – С. 39–46

24. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с.

**Зміст лекції**

1.Поняття «персональні дані».

Відповідно до статті 2 Закону України «Про захист персональних даних», «персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована». Це визначення майже тотожне визначенню, поданому в Конвенції 108 і Директиві 95/46/ЄС. 5 Закон України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних http://zakon2.rada.gov.ua/laws/show/2438-17/print1361278834285429 6 Директива 95/46/ЄС Європейського Парламенту і Ради" Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" від 24 жовтня 1995 року.

Порівняйте визначення у Законі «Про захист персональних даних» та Директиві 95/46/ЄС. Вони практично не відрізняються. «...відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована...» Закон України «Про захист персональних даних» «...будь-яка інформація, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити...» Директива 95/46/ЄС Визначення надзвичайно широке. Воно не є конкретним і бути таким не може. За 30 років з часу підписання 28 січня 1981 року Конвенції 108 багато чого змінилося. Те, що не було персональними даними, стало ними завдяки стрімкому розвитку інформаційних технологій. Таким чином, поняття має бути настільки широким, щоб охопити всі процеси обробки відомостей про особу, які існують сьогодні, про які ми знаємо, і ті процеси, які настануть завтра і які підпадатимуть під це визначення. Визначення поняття «персональні дані» розберемо більш детально. Воно складається з чотирьох частин: 1) «відомості чи сукупність відомостей»; 2) «про фізичну особу»; 3) «фізична особа»; 4) «ідентифікована або може бути конкретно ідентифікована».

«ВІДОМОСТІ ЧИ СУКУПНІСТЬ ВІДОМОСТЕЙ…» За природою відомості чи сукупність відомостей про особу можуть мати об'єктивний або суб'єктивний характер. Наприклад, об'єктивна інформація: аналіз крові особи, кардіограма, заробітна плата, зафіксована у відомості, та ін. Суб'єктивна інформація, наприклад службова характеристика. Вона може відображати суб'єктивну точку зору того, хто її написав, скажімо, керівника, у якого може бути конфлікт з працівником. Але від цього інформація не перестає бути персональною інформацією, тому що вона стосується безпосередньо того, про кого написана характеристика. За змістом відомості можуть відображати приватне чи сімейне життя або заняття особи. Тобто це можуть бути відомості, пов'язані з трудовими відносинами, соціальною поведінкою, або такі, що свідчать про те, замовником чи виконавцем є особа, і т. д. Водночас, незалежно від того, у якій сфері виникають відносини, які вимагають обробки відомостей про особу, такі відомості є персональними даними. Окремо виділяють так звану «чутливу інформацію».

У Законі «Про захист персональних даних» встановлено особливі вимоги до обробки певних категорій персональних даних. Це відомості про расове, етнічне походження, політичні, релігійні, світоглядні переконання, здоров'я, статеве життя, членство у політичних партіях, профспілках. Слід зауважити, що в Конвенції 108 до «чутливої інформації» відносять і «відомості про судимість». Відомості про особу можуть бути будь-якими за формою. Очевидно, що найбільш часто використовується, чи зустрічається, алфавітно-цифровий формат: таблиці, тексти, повідомлення і т. д., тобто те, що зручно обробляти в такому вигляді засобами автоматизованої обробки.

Може бути графічний формат: графіки, шаржі, карикатури, фото, звукові записи, а також відеозаписи, кінозаписи і т. д. Незалежно від того, в якому форматі інформація зберігається, в якому середовищі вона обробляється: чи це відеозображення, чи паперові носії, чи просто обробка файлів у комп'ютерній системі, — все одно ця інформація є персональними даними.

«…ПРО фізичну особу,…» Відомості можуть стосуватися фізичної особи безпосередньо або опосередковано. Безпосередньо - це коли, наприклад,йдеться про чиюсь конкретну особову справу, скажімо, Іваненка Івана Івановича. Або, наприклад, про історію хвороби Петренка, або банківський рахунок з номером, ідентифікаційним кодом конкретної особи. Однак часто бувають випадки, коли інформація стосується нас опосередковано.

Наприклад, ведеться реєстр нерухомого майна, а з цим майном пов’язані особи, які є його власниками, які його обслуговували або робили ремонт. Опосередковано ці відомості стосуються і цих людей. Або, скажімо, ведеться відеоспостереження у супермаркеті. Ніхто там не здійснює відеоспостереження за конкретною особою, а лише за торговим залом. Але якщо ми проходимо у торговому залі, то залишається не лише наше відеозображення, а й інформація про те, коли і з ким ми були в магазині, які товари купували, які роздивлялися, який у нас був настрій у цей час, який номер набирали по телефону, та багато іншої інформації. «…про ФІЗИЧНУ ОСОБУ,…» Відповідно до статті 24 Цивільного кодексу України «Людина як учасник цивільних відносин вважається фізичною особою».

Інформація про померлу людину не є її персональними даними. Цивільна правоздатність фізичної особи виникає в момент її народження і припиняється в момент смерті. «Інтереси зачатої, але ще не народженої дитини» можуть бути визнані як інтереси фізичної особи. Це означає, що персональні дані про протікання вагітності у деяких випадках можуть розглядатися не лише як персональні дані мами, а як персональні дані особи, яка потім виросла і досягла відповідного віку.

Приклад Суд однієї з європейських країн визнав, що нанесено шкоду особі, дитячі малюнки якої залишились в дитячому садочку і були згодом використані. Особа виросла, знайшли її малюнки, роздрукували, і психологи за малюнками (проаналізувавши, де хатинка намальована – справа, зліва, зверху, яким шрифтами) зробили психологічний портрет цієї особи. Це було визнано незаконним втручанням у приватне життя. «…ІДЕНТИФІКОВАНА АБО МОЖЕ БУТИ КОНКРЕТНО ІДЕНТИФІКОВАНА» Особа може бути ідентифікована прямо і опосередковано. Якщо на якомусь документі чи у файлі вказано прізвище, ім'я, по батькові або якась додаткова інформація, дата народження, фото, місце народження, то, зрозуміло, особу можна прямо ідентифікувати. Закон «Про захист персональних даних» містить фразу: «може бути конкретно ідентифікована». Для визначення того, чи можна особу встановити, мають враховуватися всі засоби, використання яких ймовірно очікувати для її встановлення.

До початку обробки персональних даних той, хто їх обробляє, зобов'язаний визначити, які дані будуть вважатися персональними. Не слід забувати, що якщо до персональних даних відносити дуже багато інформації, то, відповідно, збільшаться затрати на їх обробку і захист, якщо ж перелік таких даних звести до мінімуму, то існуватимуть ризики, що можна випадково завдати шкоду фізичним особам.

Приклад: Стосовно такого поняття, як «ІР-адреса» в європейських країнах відбувалися суди, які визнавали, що ІР-адреса— це персональні дані особи. Останній суд був у листопаді позаминулого року. Позов на користувача, який незаконно «завантажував» музику, подала компанія, яка захищає права власності на музичні твори. Щоб знайти цього користувача, треба було з'ясувати, яка у нього ІР-адреса. Суд визнав, що нема підстав для видачі ІРадреси, оскільки це приватні персональні дані користувача. Тобто в черговий раз було визнано, що ІР-адреса- це персональні дані.

В Україні більшість телекомунікаційних компаній погодилися, що номер телефону і номер мобільного абонента, навіть того, який не уклав письмову угоду, а використовує послуги передоплаченого зв'язку, придбавши стартовий пакет, - це персональні дані. У цьому випадку особа може бути досить просто ідентифікована. Найпростіший спосіб ідентифікації - зателефонувати за номером і запитати: «Ви хто?» Можуть бути, звичайно, значно складніші процедури ідентифікації, але все ж при певних зусиллях особа може бути ідентифікована. Визначення персональних даних є сталим, але із змінами технологій змінюється відомості, які відносяться до персональних даних.

Наприклад, обробка біометричних та генетичних даних, кілька десятків років тому вимагала значних ресурсів, ніхто не вважав генетичний код персональними даними. А на сьогодні застосування методів ідентифікації фізичних осіб з використанням генетичного коду є досить поширеним, і при цьому, безумовно здійснюється обробка персональних даних. У Директиві 95/46/ЄС є таке положення: «Для визначення того, чи можна особу встановити, повинні враховуватися всі засоби, використання яким контролером (володільцем) чи будь-якою іншою особою ймовірно очікувати для встановлення вищезгаданої особи». Це означає, що різні суб'єкти мають можливість використовувати різні засоби для встановлення особи. Тобто в різних ситуаціях підхід до процедури ідентифікації буде різний. У більшості випадків не викликає жодних сумнівів, що реєстрація на будь-якому сайті без конкретного прізвища, а лише за псевдонімом - є обробкою персональних даних.

В Україні сумлінне виконання Закону щодо захисту персональних даних для бізнесу є справою скоріше репутаційного характеру, ніж побоювання незначних штрафів у випадку порушення положень щодо обробки персональних даних. Приклад В Україні провадяться дослідження лікарських засобів. У відповідних медичних документах є закодована інформація про особу, яка погодилася брати участь у дослідженні. Згодом інформація про перебіг її хвороби, про те, як ліки діяли на піддослідного, передається у компанію, яка замовила дослідження. І хоча в документах, переданих замовникові, не зазначено прізвищ та імен, але за кодом, назвою лікувального закладу при певних умовах можна ідентифікувати особу.

ПРИНЦИПИ ОБРОБКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ Закон України «Про захист персональних даних» встановлює вимоги до обробки та захисту персональних даних. Зазначені вимоги відображають положення, запроваджені Конвенцією 108 та розвинуті у Директиві 95/46/ЄС. Зручно представити всю сукупність вимог щодо захисту персональних даних у рамках восьми базових принципів обробки персональних даних.

Персональні дані повинні: − оброблятися сумлінно і законно (за наявності підстав та з дотриманням вимог); − отримуватися із конкретними законними цілями та не оброблятися у способи, несумісні із цими цілями; − бути адекватними, не надлишковими, відповідати цілям обробки; − бути точними та своєчасно оновлюватися; − не зберігатися довше, ніж це необхідно; − оброблятися з дотриманням прав фізичної особи, включаючи право на доступ до даних; − оброблятися з дотриманням вимог щодо захисту інформації; − не передаватися за межі країни без відповідного захисту.

Розглянемо більш детально кожен із вищезазначених принципів. 1. Принцип законності обробки Персональні дані повинні оброблятися сумлінно й законно, за наявності підстав та з дотриманням вимог. У Законі України «Про захист персональних даних» говориться, що персональні дані повинні оброблятися законно (п. 8 ст. 6). Слід зауважити, що європейські експерти вказують на відсутність у нашому Законі норми про те, що персональні дані мають оброблятися чесно. У Великій Британії, наприклад, чітко виписано критерії «чесності» обробки персональних даних. Від того, наскільки повно і детально в організації прописано й реалізовано процедури обробки персональних даних, залежить розмір штрафних санкцій у разі виявлення порушень.

Проект документу, який може замінити чинну нині Директиву 95/46/ЄС,- Генеральний регламент щодо захисту персональних даних, містить, вимоги про необхідність запровадження стандартизації, сертифікації у сфері захисту персональних даних, тобто елементів оцінки відповідності, з позначенням рівнів захисту. Вказаним Генеральним регламентом передбачається також необхідність розробки, спеціально для захисту персональних даних у тих чи інших інформаційних системах, технічних і програмних засобів (data protection by design) та налаштування за замовчуванням (by defoult) засобів загального користування, наприклад інтернет-оглядачів, таким чином, щоб персональні дані користувачів були максимально захищені. При цьому, звичайно, будуть запроваджуватися й процедури оцінки відповідності таких засобів установленим вимогам.

Закон України «Про захист персональних даних» вимагає обробляти персональні дані «законно», тобто на законних підставах. Закон визначає такі підстави обробки персональних даних: 1) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень; 2) укладення та виконання правочину, стороною якого є суб’єкт персональних даних або який укладено на користь суб’єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб’єкта персональних даних; 3) згода суб’єкта персональних даних на обробку його персональних даних; 4) захист життєво важливих інтересів суб’єкта персональних даних; 5) необхідність захисту законних інтересів володільців персональних даних, третіх осіб, крім випадків, коли суб’єкт персональних даних вимагає припинити обробку його персональних даних та потреби захисту персональних даних переважають такий інтерес. Закони встановлюють випадки, коли обробка персональних даних може здійснюватися в інтересах національної безпеки, економічного добробуту та прав людини без згоди особи.

Наприклад, Законом України «Про оперативно-розшукову діяльність» передбачається у визначених випадках збирання та вивчення документів і даних, що характеризують спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину, джерело та розміри їх доходів. Цивільним кодексом України (далі - ЦКУ) допускається використання без згоди особи її імені для висвітлення її діяльності або діяльності організації, в якій вона працює чи навчається, що ґрунтується на відповідних документах (стенограми, протоколи, аудіо-, відеозаписи, архівні матеріали тощо). Без згоди фізичної особи - боржника, якщо інше не встановлено договором або законом, може здійснюватися, відповідно до ЦКУ, заміна кредитора у зобов'язанні, а отже, і передача первісним кредитором новому кредитору документів, які засвідчують права, що передаються, та інформації, яка є важливою для їх здійснення. Виключно законами запроваджуються загальнодержавні реєстри, збір відомостей про осіб до яких є обов'язковим для встановлених категорій цих осіб.

Якщо в законі є конкретна підстава для обробки персональних даних, тоді не потрібна згода. Підзаконні акти повинні лише прописувати процедури збору та обробки персональних даних. На сьогодні низка чинних нормативно-правових актів органів державної влади, прийнятих до набуття чинності Закону України «Про захист персональних даних» установлюють не лише процедури обробки відомостей про фізичних осіб, а й подекуди визначають обов'язковість обробки персональних даних певних категорій осіб. приведення їх у відповідність до положень Закону України «Про захист персональних даних». Іншою законною підставою для обробки персональних даних є згода особи, надана відповідно до сформульованої мети обробки; щодо обсягу персональних даних, які можуть бути включені до бази персональних даних; щодо доступу до персональних даних третіх осіб; щодо передачі персональних даних про фізичну особу з бази персональних даних і передачу персональних даних іноземним суб'єктам. Тобто згода - це не якийсь один документ, у якому написано, наприклад, «...даю згоду на обробку моїх персональних даних з будь-якою метою».

Схожі формулювання на практиці інколи трапляються, але вони не відповідають жодним вимогам. У Законі України «Про захист персональних даних» визначено, що згода повинна бути документована, зокрема письмова. Отже, вимога щодо виключно письмової згоди є необов'язковою. Документована процедура - це встановлений спосіб проведення певної діяльності чи процесу; процедура, визначена певним документом; процедура, яка встановленим порядком введена в дію. Відповідно до статті 205 ЦКУ правочин, для якого законом не встановлена обов'язкова письмова форма, вважається вчиненим, якщо поведінка сторін засвідчує їхню волю до настання відповідних правових наслідків.

Тобто якщо на підприємстві, в організації, установі документовано встановлена процедура стосовно того, в яких випадках певні дії певного суб'єкта є згодою, то ця процедура може бути використана для констатації факту, що документовану згоду на обробку персональних даних цього суб'єкта було надано, а отже, обробка персональних даних є законною. Підтвердженням цього може бути такий приклад: отримуючи чеки у крамницях, ми ж не пишемо щоразу: «Я даю згоду на те, щоб мені виписали чек». Це і так абсолютно зрозуміло з наших дій. Форми надання згоди можуть бути різними, зокрема, це можуть бути документи на паперових носіях з реквізитами або електронні документи, засвідчені електронно-цифровими підписами, або документи з реквізитами на будь-яких інших носіях.

Наприклад, документи, створені з допомогою фото-, відео- або аудіофіксації. Останній вид документів широко використовується в банківській сфері. Формою надання згоди може бути, наприклад, відмітка на електронній сторінці документа чи в електронному файлі, що обробляється в інформаційній системі на основі документованих програмно-технічних рішень, які не дозволяють обробку персональних даних до того часу, поки суб'єкт не виконає дії, щоб підтвердити надання їм згоди, і забезпечують реєстрацію дій суб'єкта персональних даних та цілісність протоколів реєстрації таких дій. У принципі, така процедура надання згоди певною мірою рекомендована Типовим порядком обробки персональних даних у базах персональних даних .

Зазвичай, відвідувачі веб-ресурсів надають поінформовано згоду на збір та обробку відомостей про них, ознайомившись із політикою захисту персональних даних на сайті та зробивши відмітку про згоду з цією політикою. Підстави для обробки «чутливих» даних: 1) однозначна згода суб'єкта; 2) обов'язки у сфері трудових правовідносин; 3) захист інтересів: − суб'єкта; − іншої особи у разі недієздатності суб'єкта; 4) обробка персональних даних членів (осіб, що підтримують контакти): − релігійними та громадськими організаціями; − політичними партіями та професійними спілками; Типовий порядок обробки персональних даних у базах персональних даних. Затверджено наказом Міністерства юстиції України від 30.12.2011 N 3659/5. Зареєстровано в Міністерстві юстиції України 3 січня 2012 р. 5) дані вже були оприлюднені суб'єктом; 6) задоволення або захист правової вимоги; 7) дані стосуються: − звинувачень у вчиненні злочинів, вироків суду; − оперативно-розшукової чи контррозвідувальної діяльності; − боротьби з тероризмом; 8) забезпечення лікування (обробка медичним працівником).

Обробка відомостей про расове, етнічне походження, політичні, релігійні, світоглядні переконання, здоров'я, статеве життя, членство в політичних партіях, профспілках (так звані «чутливі» дані) здійснюється за умов надання однозначної згоди на обробку персональних даних. Державна служба України з питань захисту персональних даних рекомендує обробляти такі «чутливі» персональні дані за умов надання письмової згоди.

Форми надання згоди: документ на паперовому носії з реквізитами, що дає змогу ідентифікувати цей документ та фізичну особу. Добровільне волевиявлення суб'єкта персональних даних засвідчується його підписом електронний документ, включаючи обов'язкові реквізити документа, що дають змогу ідентифікувати цей документа фізичну особу. Добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних засвідчується електронним підписом суб'єкта персональних даних документ з реквізитами на будь-якому іншому носії,зокрема фото -, відео-, аудіофіксація добровільного волевиявлення суб'єкта персональних даних відмітка на електронній сторінці документа чи у електронному файлі,що обробляється в інформаційній системі на основі документованих програмно-технічних рішень, які, у свою чергу не дозволяють обробки персональних даних до того часу, поки суб'єкт персональних даних не виконає дії, що підтверджують надання ним відповідної згоди та забезпечують реєстрацію дій суб'єкта персональних даних та цілісність протоколів реєстрації таких дій.

2. Принцип конкретності мети обробки персональних даних Персональні дані повинні отримуватися для конкретної законної мети і не оброблятися у спосіб, не сумісний із цією метою. Таким чином, з якою метою персональні дані збираються, з такою метою вони і повинні оброблятися. При цьому суб'єкт, по-перше, має знати, з якою метою він надає свою згоду. При наданні згоди суб'єкт має право зробити зауваження, що частіше всього на практиці зводиться до того, що суб'єкту надається якась альтернатива, він може вибрати якийсь варіант із загального переліку. Якщо обробка персональних даних не відповідає конкретно визначеним при наданні згоди цілям, суб'єкт персональних даних може застосовувати засоби правового захисту.

3.Принцип пропорційності. Персональні дані повинні бути адекватними, не надмірними, відповідати меті обробки. Що означає - бути «адекватними, не надмірними»? Наприклад, для чого житловоексплуатаційному підприємству або готелю можуть знадобитися відомості про місце роботи осіб? Для чого в анкетах при отриманні дисконтних карт точно знати вік покупця, а то й дату його народження? Адже частіше використовується лише вікова категорія. Зрозуміло, що під час прийняття на роботу треба надавати певні документи, відомості особистого характеру тощо. Але кількість оброблюваних персональних даних повинна відповідати меті обробки. У будь-якому разі, якщо обробляються персональні дані, треба знати, для чого ті чи інші дані потрібні, та й спосіб обробки повинен відповідати цілям обробки.

4. Принцип якості даних. Персональні дані мають бути точними і своєчасно оновлюватися. 9 Це означає, що повинна бути встановлена процедура оновлення цих даних. Якщо це, наприклад, дисконтна програма, то відомості повинні періодично оновлюватися. Має бути встановлена процедура підтримки точності й оновлення персональних даних.

5. Принцип обмеження терміну обробки даних Персональні дані повинні оброблятися у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, у строк, не більший, ніж це потрібно відповідно до їх законного призначення. У деяких випадках законодавство визначає, який період часу зберігаються та обробляються персональні дані. Наприклад, копія паспорта, яку здають під час обміну валюти, зберігається, відповідно до банківської процедури, п'ять років, а тоді має бути знищена; певний час зберігаються відомості про відеоспостереження в магазині. А це означає, що має бути прописана процедура знищення цих відомостей. Якщо цієї процедури немає - це теж порушення.

6.Принцип прозорості та опозиції. Закон України «Про захист персональних даних» установлює права суб'єктів персональних даних. Кожен має право знати, хто і де обробляє його персональні дані (ст. 8 Закону України «Про захист персональних даних»). Здавалося б, це дуже просто, а насправді - це не зовсім так.

Якщо проаналізувати будь-які анкети, у 30% з них не зазначається, хто збирає персональні дані. Така сама ситуація і з відеоспостереженням. Коли ми заходимо в супермаркет або в офіс, ми не знаємо, хто веде відеозапис. Це може бути охорона супермаркету або і фірми чи інша компанія, яка орендує тут приміщення. Коли ми відвідуємо інтерактивний сайт, то часто не знаємо, хто саме і для чого збирає у себе персональні дані. І таких прикладів безліч Основним у таких випадках є те, що коли хтось узявся обробляти персональні дані, він має забезпечити, щоб особи, чиї дані обробляються, знали, хто це робить і де. З точки зору суб'єкта персональних: даних важливо, щоб він знав, до кого звернутися, щоб вимагати захисту своїх прав.

Суб'єкт має право знати, кому передаються його персональні дані, з якою метою вони обробляються, він: повинен знати, як отримати доступ до своїх персональних даних, та мати можливість отримати цей доступ без пояснення причин. Доступ до персональних даних суб'єкта надається йому безкоштовно. Ще раз нагадаємо, що кожен має право вимагати знищення чи виправлення своїх персональних даних, якщо вони обробляються незаконно чи є недостовірними. Кожен має право звертатися з питань захисту своїх персональних даних до уповноваженого органу з цього питання, а також застосовувати засоби правового захисту, тобто звертатися до суду

7.Персональні дані повинні оброблятися з дотриманням вимог щодо захисту інформації. Інформаційна система, в якій обробляються персональні дані, має бути належним чином захищена (п. 7 ст. 8 Закону України «Про захист персональних даних»). У простих випадках - це забезпечення доступу до приміщень та до інформаційних систем лише осіб, які мають на це право, розмежування доступу з використанням паролів, реалізація мінімальних вимог щодо реєстрації подій в інформаційній системі відповідно до встановлених на підприємстві процедур. Для великих підприємств та й для малих підприємств, які ставлять за мету мінімізувати ризики, - це створення й незалежна оцінка системи управління інформаційною безпекою відповідно до міжнародних і національних стандартів, створення й оцінка комплексних систем захисту інформації в інформаційнотелекомунікаційних системах, застосування широкого переліку рекомендованих заходів. Це питання - складне і потребує окремого викладення.

8. Обмеження передачі даних іноземним суб'єктам. Передача персональних даних іноземним суб'єктам відносин, пов'язаним із персональними даними, здійснюється лише за умов забезпечення належного захисту персональних даних. Не всі країни, з якими співпрацюють українські підприємства, підписали і ратифікували Конвенцію 108, і не всі країни мають законодавство, спрямоване на захист персональних даних.

У такому випадку передача персональних даних можлива лише за умов 10 виконання імпортером персональних даних контрактних зобов'язань, визначених експортером даних. Відповідальність за дотримання вимог закону стосовно захисту персональних даних покладається на експортера даних, який у договорі з імпортером даних передбачає низку взаємних зобов'язань і процедур, спрямованих на дотримання цих зобов'язань. У разі передачі персональних даних у країни, які ратифікували Конвенцію 108 і мають законодавство, спрямоване на захист персональних даних, також доцільно у договорі визначити низку важливих зобов'язань щодо дотримання кожною зі сторін вимог законодавства, чітко визначити процедури, спрямовані насамперед на забезпечення дотримання прав суб'єктів персональних даних.

Суб'єкт персональних даних має право отримувати інформацію про умови надання доступу до персональних даних, інформацію про третіх осіб, яким передаються персональні даних, а отже, і до контрактних положень, які визначають процедури передачі персональних даних про нього за кордон.

ІІІ. СУБ'ЄКТИ ВІДНОСИН І БАЗА ПЕРСОНАЛЬНИХ ДАНИХ Хто є суб'єктами відносин, пов'язаних із персональними даними? Хто, власне, обробляє персональні дані? Закон України «Про захист персональних даних» вводить такі поняття: володілець персональних даних — фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом. розпорядник персональних даних — фізична чи юридична особа, якій володільцем бази персональних даних або законом надано право обробляти ці дані. третя особа — будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника бази персональних даних та уповноваженого державного органу з питань захисту персональних даних, якій володільцем чи розпорядником бази персональних даних здійснюється передача персональних даних відповідно до закону.

Володілець (у документах з питань захисту персональних даних Ради Європи та Європейського Союзу — «контролер, англійською controller») — юридична або фізична особа, яка обробляє персональні дані від свого імені. Це може бути організація або приватна особа: підприємець, адвокат, лікар, хто завгодно, крім осіб, які обробляють персональні дані в особистих побутових цілях.

Важливо, що володілець встановлює мету, визначає склад персональних даних та процедури їх обробки. Розпорядник (у документах з питань захисту персональних даних Ради Європи та Європейського Союзу — процесор, англійською- processor) не встановлює самостійно мету обробки персональних даних, не визначає їх склад та процедури обробки. Розпорядник діє від імені володільця, який визначив мету обробки персональних даних розпорядником, установив склад персональних даних та встановив розпоряднику процедури обробки.

Володільцем чи розпорядником бази персональних даних можуть бути підприємства, установи та організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи — підприємці, які обробляють персональні дані відповідно до закону. Як визначити, ким є та чи інша організація: володільцем чи розпорядником? У чому різниця? Розпорядник — це той, кому володілець доручив обробляти персональні дані відповідно до договору, це організація, яка обробляє персональні дані в інтересах володільця.

СУБ’ЄКТИ ВІДНОСИН ВОЛОДІЛЬЦІ / РОЗПОРЯДНИКИ ВОЛОДІЛЕЦЬ РОЗПОРЯДНИК ПРАВО надано законом, договором або за згодою ПРАВО надано володільцем або законом 11 затверджує мету обробки персональних даних встановлює склад персональних даних встановлює процедури обробки та захисту персональних даних здійснює збір та обробку персональних даних від імені володільця з визначеними володільцем цілями реєструє базу персональних даних склад персональних даних встановлює володілець, розпорядник зазначається при реєстрації бази персональних забезпечує захист персональних даних від незаконної обробки та доступу забезпечує захист персональних даних від незаконної обробки та доступу надає часткове або повне право обробки персональних даних іншим суб’єктам Якщо говорити про державного реєстратора, то найчастіше володільцем є орган державної влади, який є держателем реєстру, а розпорядником - підприємство або установа, яка визначена адміністратором реєстру.

Розпорядник не може визначати мету обробки персональних даних, а обробляти персональні дані може тільки з тою метою, яку йому визначив володілець. Розпорядник несе набагато менше відповідальності, ніж володілець. Розпорядник може обробляти персональні дані лише з метою і в обсязі, визначеними у договорі. Якщо відсутній договір, яким організація, володілець, доручає обробляти персональних дані з визначеною володільцем метою та у визначених володільцем обсягах іншій організації, то ця інша організація не може бути розпорядником. Не може бути розпорядником підрозділ юридичної особи або працівник організації — володільця персональних даних. Ним може бути лише окрема юридична особа або окремий приватний підприємець.

Існують ще деякі особливості. Конвенція 108 встановлює, що її вимоги розповсюджуються на групи осіб, які здійснюють діяльність без створення юридичної особи. 1. Профспілкові організації, деякі громадські об'єднання не є юридичними особами, але вони здійснюють обробку персональних даних. 2. Приватна особа здійснює обробку персональних даних, але робить вона це не для непрофесійних особистих чи побутових потреб. Наприклад, модератор працює у соціальній мережі, він визначає мету діяльності групи, має, відповідно до політики цієї соціальної мережі, можливість включити чи не включити інших осіб до складу групи, дозволити розмістити їхню точку зору чи не дозволити її розміщення. Тобто він встановлює склад персональних даних і процедури їх обробки. Отже, на ці дії поширюються вимоги Закону України «Про захист персональних даних» у частині, що такої обробки стосується. Третя особа Якщо якась організація не є володільцем, не є розпорядником і не є уповноваженим органом з питань захисту персональних даних, то її можна визначити як третю сторону.

При цьому третя особа у більшості випадків теж може бути володільцем персональних даних або розпорядником, який діє від імені іншого володільця. 3 точки зору підприємства, установи чи організації, яка є володільцем бази персональних даних та здійснює обробку персональних даних працівників, місцеві органи влади, виконавчі органи фондів соціального страхування від нещасних випадків, від тимчасової втрати працездатності, соціального захисту інвалідів, пенсійного, Державної інспекції з питань праці, служби зайнятості, податкової служби, органів прокуратури тощо є третіми особами, яким персональні працівників передаються у випадках, 12 визначених законом. Зазначені органи зобов'язані вжити заходів щодо забезпечення вимог законодавства про захист персональних даних.

Тобто у відносинах стосовно обробки персональних даних беруть участь: володілець персональних даних, розпорядники, які діють в інтересах володільця, та уповноважений орган з питань захисту персональних даних, який здійснює нагляд за обробкою персональних даних. Якщо персональні дані передаються для обробки іншому, крім зазначених, суб'єкту, цей суб'єкт є третьою стороною і, як правило, - іншим володільцем персональних даних. • База персональних даних Закон «Про захист персональних даних» вводить поняття бази персональних даних як іменованої сукупності упорядкованих персональних даних в електронній формі та/або у формі картотек. Із застосуванням цього поняття виникало багато складнощів унаслідок низки причин. Різні цілі, склад персональних даних та процедури - різні бази персональних даних Конвенція 108 трактує як «файл даних для автоматизованої обробки», будь-який масив даних, що піддається автоматизованій обробці, і рекомендує кожній країні визначитися, чи буде вона застосовувати Конвенцію 108 до файлів персональних даних, які не обробляються автоматизовано. Конвенцію 108 було прийнято у 1981 році, коли технології давали змогу автоматизовано обробляти лише певні категорії масивів даних.

На сьогодні автоматизовано можуть оброблятися відомості про особу, які містяться у найрізноманітніших масивах даних: у цифровому, текстовому форматі, у графічній формі, у формі відеожображень. Зараз складно знайти процеси, де не використовується автоматизована обробка, навіть звичайні паперові документи готуються з використанням комп'ютерної техніки і піддаються автоматизованій обробці: скануванню, розпізнаванню тексту чи зображень, пошуку необхідних елементів даних тощо.

Термін «база персональних даних», що використовується у Законі «Про захист персональних даних», часто помилково ототожнюють з терміном «база даних», який передбачає конкретну технологію автоматизованої обробки. База персональних даних не є базою даних. Використання терміну «база персональних даних» передбачає, що володілець персональних даних визначає мету їх обробки у базі персональних даних, склад цих даних та процедури їх обробки з певною метою. Різні цілі, склад персональних даних та процедури — різні бази персональних даних Володільцем яких баз персональних даних є підприємство, установа чи організація? Наприклад, мета обробки персональних даних пацієнтів лікувального закладу і працівників лікувального закладу різна. Одні — лікують, а інші — лікуються. Мета обробки персональних даних у цих двох різних персональних даних сформульована в різних законах. У першому випадку це можуть бути, наприклад, Закон України «Основи законодавства України про охорону здоров'я», у другому — Кодекс законів про працю України.

Склад персональних даних, що обробляються в цих персональних даних теж різний. Слід зазначити, що лікувальний заклад, крім зазначених цілей, імовірно, обробляє персональні дані з метою здійснення господарської діяльності для забезпечення функціонування — з метою закупівлі ліків, здійснення ремонту будівель, вивезення сміття, тощо. Персональні дані, які використовуються у цій сфері діяльності, можуть належати до іншої бази персональних даних. Цей приклад є типовим і для інших категорій організацій. Зазвичай, визначення трьох баз персональних даних: клієнтів (користувачів, відвідувачів, пацієнтів, покупців, тощо), працівників та контрагентів,- достатньо в діяльності організації.

Приклад. 13 У телекомунікаційній компанії здійснюється обробка персональних даних працівників компанії, користувачів послуг зв'язку, а також обробка персональних даних у допоміжних бізнес-процесах. Можна обмежитися також трьома базами персональних даних. Кількості баз персональних даних в організації законодавством не обмежена. Підприємство, установа чи організація самостійно визначають та відображають в організаційних документах в яких саме базах персональних даних здійснюється їх обробка. Чи є обробка персональних даних у системі відеоспостереження обробкою персональних даних в окремій базі даних?

У цьому випадку персональні дані, отримані з допомогою системи відеоспостереження, можуть оброблятися в окремій базі персональних даних, або кількох базах, або існувати як складова частина обробки персональних даних у тій чи іншій базі персональних даних: відеоспостереження в робочих приміщеннях можна віднести до обробки персональних даних в базі персональних даних працівників, відеоспостереження чи реєстрація дій клієнтів – до іншої бази персональних даних. Якщо йдеться про різні цілі, різний склад персональних даних і різні процедури - це означає, що мають існувати різні бази персональних даних. Якщо, скажімо, у мобільному телефоні працівника є інформація про інших працівників цього підприємства, то можна говорити про елементи бази персональних даних працівників. При цьому метою обробки може бути організація функціонування підприємства, зокрема забезпечення виконання планових завдань. Або якщо в мобільному телефоні працівника обробляються персональні дані клієнтів компанії, то це можна вважати елементом іншої бази персональних даних - бази персональних даних клієнтів компанії. Звичайно, у цьому випадку такі дії не є обробкою персональних даних працівником «для непрофесійних особистих чи побутових потреб», а отже, це потрапляє під застосування Конвенції 108 та законодавства про захист персональних даних.

Таке використання персональних даних є окремими процедурами обробки персональних даних в інтересах підприємства, і кожен працівник зобов'язаний дотримуватись положень внутрішніх документів компанії і етичних норм при спілкуванні із клієнтами і працівниками. Зрозуміло, що якщо у мобільному телефоні містяться номери телефонів працівників установи, в якій працює особа, і вона використовує їх не з метою організації виконання завдань установи, то це буде порушенням законодавства про захист персональних даних. Відповідно до рекомендацій Ради Європи держава не повинна збирати в одну базу персональних даних інформацію, яка обробляється з різними цілями. Це робиться для того, щоб держава не мала можливості робити повний профайлінг фізичної особи, тобто відслідковувати всі події, пов’язані з конкретною особою та поєднувати відомості із різних джерел стосовно осіб, про яких обробляються відомості в державних установах.

IV. ОРГАН НАГЛЯДУ, ВІДПОВІДАЛЬНИЙ ЗА ЗАБЕЗПЕЧЕННЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ Кожна країна, яка приєдналася до Конвенції 108 створює уповноважений орган з питань захисту персоанльних даних даних. На який покладаються функції розслідування та втручання, участі у судовому розгляді, розгляд заяв суб’єктів про порушення їх прав та прийняття рішення. Закон України «Про захист персональних даних» встановлює, що уповноважений орган з питань захисту персоанльних даних здійснює в межах своїх повноважень контроль за додержанням вимог законодавства про захист персональних даних шляхом проведення віїних та безвиїзних перевірок із забезпеченням відповідно до закону доступу до інформації, пов'язаної з обробкою персональних даних у базі персональних даних, та до приміщень, де здійснюється їх обробка. Уповноваженим органом з питань захисту персональних даних є Державна служба України з питань захисту персоанльних даних. З 1 січня 2014 року функції уповноваженого органу з питань захисту персоанльних даних покладаються на Уповноваженого Верховної Ради України з прав людини.

V. ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ З ВИКОРИСТАННЯМ ВЕБ-РЕСУРСІВ Веб-ресурс – сукупність сторінок в Інтернеті, яка може бути ідентифікована, адресована і супроводжувана в мережевій інформаційній системі. У момент збору персональних даних суб’єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, права такого суб’єкта, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані. Вимоги Закону України «Про захист персональних даних» та застосування його положень при обробці персональних даних з використанням веб-ресурсів повністю кореспондуются з рекомендаціями Комітету Міністрів Ради Європи щодо захисту недоторканості приватного життя в Інтернеті10, рекомендаціями Робочої групи11, що функціонує відповідно до статті 29 Директиви 95/46/ЄС та рекомендаціями Міжнародної робочої групи з питань захисту персональних даних в телекомунікаціях12 . 5.1. Категорії персональних даних що найчастіше обробляються в Інтеренет Найчастіше персональні дані з використанням веб-ресурсів обробляються в рамках таких процесів як: заповнення відвідувачами веб-ресурсів анкет реєстрація та отримання логіна та пароля реєстрація з використанням облікового запису соціальної мережі надання електронної адреси відвідувача для зворотного зв’язку. При цьому можуть оброблятися персональні дані надзвичайно широкого діапазону: від анкетних персональних даних, які явно є відомостями про особу яка ідентифікована, так і відомостей які можуть стосуватися особи опосередковано або які можуть використовуватися в процесі ідентифікації особи: відомостей про оплату послуг з використанням платіжних карт, логіни та паролі, записи в соціальній мережі, номери телефонів, електронні адреси, тощо. Питання що стосуються таких специфічних категорій даних як IP-адреса, кукі, та інші відомості які часто використовуються як для технічного забезпечення надання якісних послуг користувачу, так і для відслідковування поведінки відвідувачів веб-сторінки вимагають окремого обговорення та коротко викладені в розділі 5.4. 5.2. Типові порушення законодавства з питань захисту персональних даних при обробці персональних даних з використанням веб-ресурсів та рекомендації щодо їх усунення Під час виїзних та безвиїзних перевірок дотримання володільцями законодавства з питань захисту персональних даних до планів перевірок включалися також і питання дотримання законодавства про обробці персональних даних з використанням веб-ресурсів володільців.

Комісіям надавалась необхідна інформація - копії чи виписки з документів, письмові та усні пояснення. Як правило, комісіями не використовувалося право на безперешкодний доступ до комп’ютерів та магнітних носіїв, що передбачено законодавством. Натомість, ефективно використовувався механізм огляду електронного документа для вивчення матеріалів, розміщених на сайті, процедур обробки персональних даних на сайті та механізмів функціонування веб-ресурсу володільця, про що складалися акти оглядів електронних документів за встановленою формою.

Найчастіше виявлялися такі порушення: 1. У момент збору персональних даних суб’єкт персональних даних НЕ ПОВІДОМЛЯЄТЬСЯ про володільця персональних даних (найменування юридичної особи – володільця та її адресу), склад та зміст зібраних персональних даних, права такого суб’єкта, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані. 2. Зміст персональних даних був явно НАДМІРНИМ відповідно до визначеної мети обробки персональних даних. 3. Процедури обробки персональних даних були визначені на сайті, але не були визначені розпорядчими документами володільця, як це передбачено законодавством. результатами перевірок Державної служби України з питань захисту персональних даних підготовлено обов’язкові до виконання ПРИПИСИ про усунення порушень. Жодного припису не було оскаржено у судовому порядку. Здійснено та здійснюється доопрацювання процедур обробки персональних даних в використанням веб-ресурсів, зокрема встановлено процедури повідомлення відвідувачів сайтів про свої права, про склад та зміст персональних даних, що збираються, про мету збору персональних даних та про осіб, яким передаються його персональні дані. Як правило, таке повідомлення здійснюється у формі окремого розділу сайту («Політика обробки персональних даних», «політика приватності», чи «політика конфіденційності»). Усуваються інші порушення, зокрема такі як надання безвідкличної чи безстрокової згоди на обробку персональних даних, передача персональних даних невстановленим третім особам, тощо. Відновлено право суб’єкта персональних даних на знищення своїх даних, в разі відсутності підстав для їх обробки. Окремі володільці призупинили функціонування своїх веб-ресурсів до усунення порушень.

5.3. Прозорість та відкритість забезпечення приватного життя в Інтернеті Державна служба України з питань захисту персональних даних підтримує ініціативи, спрямовані на зростання обізнаності тих, хто обробляє персональні дані, та тих, чиї персональні дані обробляються з кращими практиками та стандартами обробки персональних даних. За ініціативи ВГО «Українська асоціація захисту персональних даних» у жовтні 2012 року було прийнято Декларацію «За недоторканість приватного життя в Інтернеті»13, до якої приєдналися провідні національні телекомунікаційні компанії. У лютому 2013 року було проведено перше дослідження в рамках громадського моніторингу відкритості та прозорості обробки персональних даних в Інтернеті. Хоча використовувалися прості і доступні кожному методики, результати насторожують і варті уваги, адже, за результатами дослідження встановлено, що понад 75% веб-сайтів українського сегменту Інтернет, за явних ознак обробки персональних даних, не надають користувачам жодних відомостей про найменування володільця персональних даних.

Це свідчить про те, що відвідувачі сайтів не мають можливостей на захист свої персональних даних. Громадські ініціативи, спрямовані на забезпечення прозорості і відкритості обробки персональних даних є надзвичайно важливими. 5.4. Відслідковування поведінки відвідувачів веб-ресурсів (web-tracking) За вкрай низького рівня правової культури володільців персональних даних, які здійснюють їх обробку з використанням веб-ресурсів українського сегменту Інтернет, коли ігноруються найпростіші вимоги закону при зборі та обробці персональних даних, важко говорити про небезпеку для приватного життя користувачів Інтернет некоректного використання автоматизованих засобів відслідковування особливостей поведінки користувачів Інтернет при відвідуванні веб-сайтів. Але обговорювати це необхідно, адже цілком раціональні засоби, що використовуються для забезпечення кращого задоволення споживацьких потреб, за умов надмірного їх використання, надмірного збору відомостей про споживачів, фізичних осіб, які за певних обставин можуть бути ідентифікованими, можуть призвести до втручання в приватне життя. В країнах Європи цій проблемі надається значної уваги . Для відслідковування особливостей поведінки відвідувачів веб-ресурсів використовуються такі технології як: надсилання до пристрою користувача кукі першої та кукі третьої сторони; збирання в базах веб-ресурсів детальної інформації протягом тривалого часу про відвідані сторінки, вибрані режими, натиснуті клавіші, тощо, та її подальша обробка; збирання в базах веб-ресурсів інформації про апаратні та програмні засоби, які встановлено у користувача, та ін. Звичайно, в цій сфері заходів, що можуть вживатися Державною службою з питань захисту персональних даних, для забезпечення прогресу, мало. Адже ДСЗПД, в ході перевірок може лише зафіксувати незаконне надсилання кукі третьої сторони та вимагати, щоб такі операції здійснювалися лише за наявності законних підстав. Володільці персональних даних, які здійснюють обробку персональних даних з використанням веб-ресурсів часто навіть не знають, які треті сторони отримують відомості про те, що користувач відвідав їх ресурс. Необхідно інформування як володільців персональних даних, так і суб’єктів персональних даних про механізми автоматизованого збору відомостей про поведінку відвідувачів в Інтернет, про законні підстави для обробки персональних даних про відвідування сайтів, про необхідність повідомлення відвідувачів про механізми автоматизованої обробки персональних даних та про їх права.

VI. ДОТРИМАННЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ДОСЛІДЖЕННЯХ В ІНТЕРЕНЕТ В залежності від різновиду опитування в Інтернет відносини між суб’єктами, пов’язаними з персональними даними також можуть бути різними, а отже застосовуються різні положення законодавства.

6..1 Дослідження, що передбачають активну взаємодію з респондентами Перший різновид - дослідження, що передбачають активну взаємодію з респондентами16: опитувальні листи респондент отримує по e-mail або скачує з сайта, заповнює відповідну форму й пересилає через e-mail; оnline (e-mail-опитування, Web-опитування) – респондент відповідає на поставлені запитання в режимі реального часу й може миттєво переглянути дійсні на поточний час, результати опитування. Очевидно, що організація, яка здійснює опитування є володільцем персональних даних, а респондент є суб’єктом персональних даних (рис.6.1). Досліднику необхідно звернути увагу на законні підстави для збору та обробки персональних даних та забезпечення прав суб’єкта персональних даних. Законними підставами у даному випадку може бути договір, укладений з респондентом (письмовий договір, чи договір приєднання згідно зі статтею 634 Цивільного кодексу України), або надана згода на обробку персональних даних. На дослідника покладається доведення факту наявності законних підстав для обробки персональних даних в разі звернення респондента зі скаргою до уповноваженого органу чи до суду. Звичайно тут має бути чітко позначено мета дослідження, ваша процедура щодо захисту персональних даних, тобто які персональні дані ви збираєте, для чого ви їх зберігаєте, як довго вони будуть зберігатися. Мова йде про ретельно прописану політику вашого дослідження. Під час збору даних ви зобов’язані повідомити суб’єкта про його права, тобто чітко сказати, хто про що повинен знати, обов’язково повідомити респондента про його право приймати або не приймати участі в дослідженнях, на який стадії ваші дані стають анонімі, яка ступень псевдо анонімності даних у дослідженнях. Не обов’язково ваш респондент муси знати про всі етапи роботи з його даними, але лише до того етапу, коли його дані агрегуються та стають анонімними, неможливими для ідентифікації. Навіть при опитуванні, яке не передбачає ідентифікацію респондента, зазвичай обробка персональних даних (логін, пароль, відповіді на запитання та ін..) здійснюється. В разі виплати респондентам винагороди, при розігруванні призів здійснюється ідентифікація респондентів.

6.2. Дослідження, що не передбачають прямої взаємодії з суб’єктами персональних даних Інший різновид досліджень в Інтернеті – збір та аналіз інформації про відвідування певних сторінок сайтів компаній-партнерів, що не передбачає прямої взаємодії з 1 18 респондентами: надання послуг компаніям партнерам щодо вивчення аудиторії їх сайту. При цьому можуть застосовуватися різні технології, але часто,згідно з позицією Державної служби України з питань захисту персональних даних17 такі технології пов’язані з обробкою персональних даних18, зокрема: здійснюється обробка IP-адрес та унікальних ідентифікаторів Cookies, що дозволяє відстежувати суб’єктів - користувачів конкретного комп’ютер, навіть якщо їх справжні імена невідомі; аналізуються відомості про тип інтернет-браузерів, які використовуються відвідувачами сайта (наприклад, Microsoft Internet Explorer, Mozilla Firefox, Google Chrome або Opera); операційна система (ОС), яку вони використовують (наприклад, Windows XP); розширення екрану монітора; глибина кольору екрану монітора, активні процеси в комп’ютері відвідувачів сайту та ін.

**Лекція № 7**

**Тема 7. Системна інформатизація судочинства**

**План лекції**

Веб-портал «Судова Влада Україна». Автоматизація процесів документообігу. Автоматизація процесів реєстрації та створення документів. Забезпечення технологічних процесів проходження судових справ. Контроль дотримання процесуальних термінів. Контроль виконання документів. Технічне фіксування (аудіо та відеозапис) та протоколювання судового процесу. Автоматичний розподіл судових справ до розгляду. Формування статистичної звітності на базі первинної інформації.

**Література**

1. Туркіна І. Інформаційні технології в судовій системі / І. Туркіна. – [Електронний ресурс]. – Режим доступу: [http://www.kbuapa.kharkov.ua/e-book/putp/2011-3/doc/4/05.pdf].
2. Про Стратегію реформування судоустрою, судочинства та суміжних правових інститутів на 2015–2020 роки: Указ Президента України від 20.05.2015 року № 276/2015 // Офіційний вісник Президента України. – 2015. – № 13. – Ст. 864.
3. Овчинников Є.І. Системна інформатизація кримінального судочинства / Є.І. Овчинников, М.Я. Швець, Ю.А. Клімашевська. – [Електронний ресурс]. – Режим доступу: [http://www.scourt.gov.ua/clients/vs.nsf/0/0206ECB2F1B9A93988256DA50066A8E3?OpenDocument].
4. Абраменко, Ю. Ю. (2009). Зарубіжний досвід е-урядування та проблеми його імплементації в Україні. Публічне адміністрування: теорія та практика, Електронний збірник наукових праць. 2 (2). Взято з http://www.dridu.dp.ua/zbirnik/2009-02/09ayypiu.pdf
5. Барбара, В. П. (2006). Використання комп’ютерних технологій у судочинстві.Вісник Верховного Суду України, 1 (65), 36–39
6. Бринцев, О. В. (2016). «Електронний суд» в Україні. Досвід та перспективи, Монографія. Серія: «Інноваційне суспільство і розвиток законодавства». (с. 72). Харків: Право
7. Вдовіна, О. О. (2014). Нормативно-правові засади впровадження автоматизованого судового документообігу. Бібліотекознавство. Документознавство.Інформологія, 4, 29–32
8. Вдовіна, О. О. (2015). Використання електронного документообігу в системі судочинства України. Вісник ХДАК, 46, 82–91
9. Ємельянова, В. (2009). Автоматизована система електронного документообігу «Діловодство суду» — ще один крок до відкритості судів для громадян. Вісник Вищого адміністративного суду України, 2, 43–48.
10. Концепція галузевої програми інформатизації судів загальної юрисдикції та інших установ судової системи, погоджена Державним агентством з питань науки, інновацій та інформатизації України (лист від 28 серпня 2013 року № 1/06-1-805). Взято з http://court.gov.ua/49271/
11. Концепція електронного суду України, розроблена Державним підприємством «Інформаційні судові системи» у 2012 році. Взято з http://kbs.org.ua/files/koncept\_d.pdf
12. Семенченко, А. І. (Ред.) (2009). Концепція розвитку електронного урядування в Україні. Київ
13. Положення про автоматизовану систему документообігу суду: Затверджено Рішенням Ради суддів України 26.11.2010 № 30 (у редакції рішення Ради суддів України від 02 квітня 2015 року № 25). Взято з http://court.gov.ua/sudova-vlada/969076/polozhenniapasds
14. Про реалізацію проекту щодо обміну електронними документами між судом та учасниками судового процесу: Наказ Державної судової адміністрації України: від 31.05.2013 р., № 72. Взято з http://dsa.court.gov.ua/dsa/14/N722013/113
15. Розпорядження Кабінету міністрів України «Про схвалення Концепції розвитку електронного урядування в Україні». Чинний від 13.12.2010.Взято з http://zakon1.rada.gov.ua/laws/show/2250-2010-%D1%80
16. Чирський, Ю. В. Запровадження системи електронного документообігу в Україні. Взято з http://old.minjust.gov.ua/7546
17. Шамрай, О. В. (2014). Електронний суд в українському судочинстві: нормативне регулювання та перші практичні здобутки. Університетські наукові записки, 3 (51), 174–184

**Зміст лекції**

Електронний документообіг, створення та функціонування якого базується на сучасних інформаційно-комунікаційних технологіях (ІКТ), є головною складовою електронного врядування, маючи значні переваги, порівняно зі звичним, паперовим документообігом. ІКТ впроваджується в усі сфери суспільного життя, зокрема й у сферу здійснення правосуддя.

Рекомендації Комітету міністрів Ради Європи, положення національних стратегічних документів, законів України «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис» тощо передбачають, що електронне судочинство, як складова загальнодержавного електронного врядування, є шляхом до поліпшення доступності правосуддя та підвищення його оперативності. Тому головна мета впровадження електронного судочинства — забезпечення ефективності судової системи та якості здійснення правосуддя загалом.

Питанням електронного судочинства як окремого напряму електронного урядування останнім часом приділяють увагу дедалі більше дослідників, серед котрих: В. Барбара (2006), О. Бринцев (2016), В. Ємельянова (2009), А. Єлістратов, О. Шамрай (2014) та ін.

Окремо розглядалися проблеми організації електронного документообігу, захисту та юридичної обґрунтованості електронних документів, проте немало важливих питань, пов’язаних з упровадженням електронного діловодства в судову систему, потребують подальшого дослідження.

Згідно з Концепцією розвитку електронного урядування, в Україні електронне урядування (е-урядування) розуміється як форма організації державного управління, яка завдяки широкому застосуванню ІКТ сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади, органів місцевого самоврядування, наданню в дистанційному режимі комплексу державних послуг для людини та громадянина, суспільства, держави та бізнесу (користувачі).

Упровадження електронного урядування передбачає реалізацію комплексного й індивідуалізованого підходів до надання державних послуг користувачам без безпосереднього контакту з державними службовцями (деперсоніфікація) (Розпорядження Кабінету міністрів України «Про схвалення Концепції розвитку електронного урядування в Україні». Чинний від 13.12.2010).

З метою вирішення питань щодо запровадження в Україні системи електронного урядування 24 лютого 2003 № 208 р. прийнято Постанову Кабінету Міністрів України «Про заходи щодо створення електронної інформаційної системи “Електронний уряд”», відповідно до якої передбачено створити належні нормативно-правові засади функціонування системи «Електронний уряд», створити умови для оперативного та доступного надання інформаційних послуг громадянам та юридичним особам за допомогою електронної інформаційної системи «Електронний уряд», яка забезпечує: взаємодію органів виконавчої влади між собою, з громадянами та юридичними

особами на основі сучасних інформаційних технологій, інтегрувати державні електронні інформаційні ресурси і системи в Єдиний вебпортал органів виконавчої влади (Чирський).

Реалізація ідеї електронного врядування викликає значний інтерес у всьому світі. США, Великобританія, Швеція, Данія, Норвегія, Латвія, Естонія та багато інших країн застосовують або починають застосовувати методи електронного урядування. Зокрема уряд США надає громадянам різноманітні послуги через мережу інтернет: видачу ліцензій, сплату штрафів тощо.

***Метою впровадження е-урядування в Україні є*** розвиток електронної демократії для досягнення європейських стандартів якості електронних державних послуг, відкритості та прозорості влади для людини, громадянина, громадських організацій, бізнесу.

Відповідно до базових положень Концепції галузевої програми інформатизації судів, здійснення організаційного забезпечення діяльності судів загальної юрисдикції, інших органів та установ судової системи — одне із основних завдань Державної судової адміністрації (ДСА) України. ДСА, як центральний орган виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України, створює необхідні умови для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією за

допомогою широкого використання ІКТ (Концепція галузевої програми інформатизації судів загальної юрисдикції та інших установ судової системи, погоджена Державним агентством з питань науки, інновацій та інформатизації України (лист від 28 серпня 2013 року № 1/06-1-805)).

*Головною метою Концепції* є формування умов для створення та функціонування Єдиної судової інформаційної системи, що надає інформаційну й технологічну підтримку судочинству на принципах дотримання балансу між потребою громадян, суспільства і держави у вільному обміні інформацією і необхідними обмеженнями на її розповсюдження. Вона являє собою сукупність нормативно-правових, організаційно-розпорядчих заходів, програмно-технічних та телекомунікаційних засобів, що зумовлюють збирання, оброблення, накопичення, аналіз та зберігання інформації, взаємодію окремих підсистем уніфікованої й взаємопов’язаної через відповідні стандарти та протоколи, програмні інтерфейси, стандарти даних, стандарти документів, мереж, ведення архіву та відповідні управлінські процеси інфраструктури (Концепція галузевої програми інформатизації судів загальної юрисдикції та інших установ судової системи, погоджена Державним агентством з питань науки, інновацій та інформатизації України (лист від 28 серпня 2013 року № 1/06-1-805)).

У контексті Концепції розвитку електронного врядування в Україні головні стратегічні напрями розвитку електронного судового діловодства та документообігу визначено з урахуванням різноманітності існуючих систем електронного документообігу в органах державної влади та органах місцевого самоврядування. Усі вони спрямовані на створення інтегрованої системи електронного документообігу, мета якої — забезпечення руху документів (укази, постанови, закони, розпорядження, повідомлення, звіти, аналітичні довідки тощо), скорочення терміну підготовки та прийняття рішень завдяки автоматизації процесів колективного створення та використання документів в органах державної влади, зокрема в судових установах. Така система є складовою підсистемою («Судове діловодство та документообіг») у структурі Єдиної судової інформаційної системи (Концепція галузевої програми інформатизації судів загальної юрисдикції та інших установ судової системи, погоджена Державним агентством з питань науки, інновацій та інформатизації України (лист від 28 серпня 2013 року № 1/06-1-805)).

Зважаючи на визначену в Концепції програмну етапізацію впровадження та розвитку системи електронного урядування, яка належить до складних соціальних систем, розглянемо завдання ЕСДД.

На першому етапі розвитку електронного урядування передбачається:– формування необхідної нормативно-правової та нормативно-технічної бази, зокрема єдиних стандартів, протоколів та регламентів взаємодії суб’єктів електронного врядування, законодавче визначення електронних державних послуг тощо;

– створення Національного реєстру електронних інформаційних ресурсів та веб-сайтів (веб-сторінок) органів державної влади та органів місцевого самоврядування;

– започаткування надання органами державної влади й органами місцевого самоврядування інформаційних та консультаційних послуг фізичним, юридичним особам з використанням мережі інтернет, поглибленою інформатизацією суспільства, держави та бізнесу (Семенченко, 2009; Розпорядження Кабінету міністрів України «Про схвалення Концепції розвитку електронного урядування в Україні». Чинний від 13.12.2010).

Ці завдання є визначальними для формування відповідних напрямів розвитку ЕСДД щодо забезпечення та вдосконалення нормативно-правової, нормативно-технічної бази електронного діловодства й інформатизації традиційного (паперового) діловодства для функціонування веб-порталу судової влади та Єдиного державного реєстру судових рішень.

***Концепція електронного урядування*** складається з двох взаємозалежних та водночас самостійних структур: внутрішня урядова інформаційна інфраструктура, аналог корпоративної мережі, та зовнішня інформаційна інфраструктура, що взаємодіє з громадянами й організаціями. У рамках «електронної держави» інтегруються інформаційні ресурси органів державної влади, а також створюється

система онлайнових послуг (Чирський).

Другий етап розвитку електронного врядування спрямовано на розвиток послуг електронного урядування, що охоплюють усі сфери життєдіяльності громадян, організацій та функціонування державних органів: опанування технологій інтерактивної взаємодії органів державної влади з громадянами та представниками бізнесу, можливості двосторонніх комунікацій, здійснення деяких операцій у режимі реального часу.

Третій етап — двостороння взаємодія органів державної влади та органів місцевого самоврядування з людиною та громадянином.

Передбачається тиражування та впровадження в широку практику діяльності органів державної влади й органів місцевого самоврядування типових технологічних рішень, створення об’єднаних порталів міністерств, відомств, служб тощо, через які можна здійснювати відповідні транзакції. Можливість здійснення основних видів транзакцій в електронній формі завершує перехід до електронно-інформаційного середовища взаємодії

У контексті цих двох етапів визначено стратегічний напрям розвитку ЕСДД, який водночас віддзеркалює положення Концепції галузевої програми інформатизації судів стосовно створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією на основі широкого використання ІКТ. Це — супровід та участь у функціонуванні Єдиної судової інформаційної системи через її підсистеми, що взаємодіють із

громадськістю: інтернет-портал; державний реєстр судових рішень;

звернення громадян; інформаційний кіоск (Концепція галузевої програми інформатизації судів загальної юрисдикції та інших установ судової системи, погоджена Державним агентством з питань науки, інновацій та інформатизації України (лист від 28 серпня 2013 року № 1/06-1-805)).

У межах четвертого етапу електронного урядування — розвитку та вдосконалення системи електронного урядування — заплановано створення електронної системи органів державної влади, органів місцевого самоврядування на основі єдиних стандартів, а також Єдиний веб-портал електронного врядування як єдину точку доступу до всіх видів послуг для громадян та організацій, що репрезентуватиме весь комплекс електронних державних послуг і надаватиме доступ до них за технологією «єдиного вікна», відповідно до потреб і функціональних аспектів

Згідно з пріоритетними *напрямами інформатизації судів*, що означено в Концепції галузевої програми інформатизації судів,сформульовано такі ***напрями розвитку ЕСДД***:

– загальні — автоматизація процесів документообігу, зокрема: реєстрації та створення документів; забезпечення технологічних процесів проходження судових справ; контроль дотримання процесуальних термінів; контроль виконання документів; технічне фіксування (аудіо та відеозапис) та протоколювання судового процесу; автоматичний розподіл судових справ до розгляду.

– функціональні — на рівні підсистеми Єдиної судової інформаційної системи «Судове діловодство та документообіг», передбачають забезпечення:

– судового діловодства на всіх етапах судового процесу, починаючи з надходження судової справи до суду, завершуючи її переданням до архіву для зберігання;

– автоматизації процесів проходження процесуальних документів;

– загального діловодства і документообігу внутрішніх та зовнішніх документів;

– процесуального контролю та контролю виконання документів та відстеження життєвого циклу справ та документів;

– обліку та контролю використання бланків суворої звітності під час видачі (виготовлення) копій судових рішень (Концепція галузевої програми інформатизації судів загальної юрисдикції та інших установ судової системи, погоджена Державним агентством з питань науки, інновацій та інформатизації України (лист від 28 серпня 2013 року № 1/06-1-805)).

Таким чином, можна сформулювати головні стратегічні напрями впровадження електронного судового діловодства в контексті Концепції розвитку електронного урядування України та Концепції галузевої програми інформатизації судів.

Забезпечення, вдосконалення нормативно-правової та нормативно-технічної бази СЕДД для створення та функціонування

Єдиної судової інформаційної системи, що надає інформаційну та технологічну підтримку судочинству на принципах дотримання балансу між потребами громадян, суспільства і держави у вільному обміні інформацією.

Інформатизація та автоматизація судового діловодства, документообігу для забезпечення функціонування веб-порталу судової влади та Єдиного державного реєстру судових рішень, з можливостями формування інформаційних ресурсів, надання електронних консультаційних послуг фізичним та юридичним особам з використанням мережі інтернет.

Супровід та участь у функціонуванні Єдиної судової інформаційної системи через її підсистеми щодо взаємодії з громадськістю:

інтернет-портал; державний реєстр судових рішень; звернення громадян; інформаційний кіоск.

Удосконалення організаційних та технологічних основ ЕСДД з метою інтегрування до захищеної системи міжвідомчого електронного документообігу; до єдиної системи контролю результативності діяльності органів державної влади; єдиної інфраструктури міжвідомчої автоматизованої інформаційної взаємодії та взаємодії державних органів з фізичними та юридичними особами; доручення до впровадження засобів електронних ресурсів та електронних послуг з метою забезпечення віддаленого доступу до інформації про діяльність органів державної влади.

Удосконалення автоматизованої системи документообігу потребує узгодження документів первинного обліку судових справ і матеріалів відповідно до вимог автоматизованої системи з урахуванням норм чинного законодавства, а також затвердження наказів ДСА України, які регламентують питання ведення діловодства та архівної роботи в судах. Крім того, виникає немало практичних питань, що потребують вивчення та залучення до їх вирішення компетентних органів.

Відзначено конкретно-прикладні завдання розвитку й удосконалення ЕСДД для органів судової влади:

– модернізувати комп’ютерне (апаратне, програмне і технологічне) забезпечення систем автоматизованого документообігу в адміністративних судах, оскільки існуюча програма не передбачає тих обсягів інформації, які щодня потрібно вносити в електронну базу, що призводить до збоїв у роботі програми та технічних помилок.

– затвердити технічні регламенти, необхідні для впровадження та функціонування систем електронного документообігу й електронного цифрового підпису в органах судової влади.

– вирішити питання кадрового забезпечення інформаційно-технологічних підрозділів органів судової влади, постійного підвищення кваліфікації їхніх працівників.

– підвищити загальний рівень комп’ютерної грамотності населення, передусім через упровадження нових методів навчання із застосуванням сучасних ІКТ.

В аналізі нинішнього стану правосуддя, який подано у Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015–2020 роки, схваленій Указом Президента України від 20.05.2015 року № 276/2015 акцентується на недостатньому рівні єдності та послідовності судової практики; відсутності чи недостатньому рівні використання можливостей сучасних інформаційних систем (електронне правосуддя)

Отже, в умовах проведення судово-правової реформи особливого значення набуває вдосконалення якості судочинства, розширення доступу громадян до правосуддя і забезпечення гласності розгляду справ судами, у тому числі шляхом створення та ефективного застосування комп’ютерних технологій та інформаційних систем.

 Інформатизація судової діяльності в Україні є одним з головних напрямів реформування судової системи.

**Інформатизація судової діяльності**– організований процес створення сприятливих умов для доступу до інформації, що використовується в судочинстві, її зберігання, обробки і передачі в електронній формі на основі ресурсів і послуг судових інформаційних систем з метою підвищення ефективності правосуддя.

**Судові інформаційні системи становлять** сукупність баз даних, що забезпечують обробку технологій і програмно-технічних засобів, які застосовуються у судовій діяльності.

 Незважаючи на специфіку інформатизації судової діяльності та важку формалізованість процесів судочинства упродовж останніх років в Україні все ж реалізовано низку проектів щодо оснащення суддів та працівників апаратів судів засобами нових інформаційних технологій.

Необхідно зазначити, що судовий розгляд справ як діяльність, пов’язана з аналізом і правовою оцінкою доказів, може бути визначений як інформаційний процес, що спирається на особливі види інформації: докази у справі, з одного боку, та законодавче, нормативно-правове поле України – з іншого. Впровадження сучасних інформаційних технологій у зазначену діяльність потребує створення такого предметного інформаційного середовища, яке забезпечить суддю необхідними даними, мінімізує затрати його часу на виконання технічної роботи, що в результаті сприятиме оперативності прийняття судових рішень.

 Інформаційне забезпечення судочинства має за мету надати судді у зручному режимі роботи структуровану систему даних і знань щодо кожної судової справи: 1) законодавчі та відомчі нормативні акти; 2) статистичні дані про розгляд справ у судах; 3) матеріали узагальнення судової практики; 4) інформаційні ресурси центральних органів державної влади; 5) інформаційні ресурси органів внутрішніх справ України, прокуратури, інших інституцій, що беруть участь у процесі; 6) інформацію з міжнародного права.

 Враховуючи ще й такі аспекти судочинства, як відкритість та прозорість, а також необхідність забезпечення права громадян України на інформацію, особливу увагу слід звернути на створення інформаційно-пошукових систем матеріалів судової практики. Питання створення таких систем, як і взагалі питання доступу до правосуддя, неодноразово висвітлювалося в документах Ради Європи як одна з найважливіших умов справедливого застосування закону. На жаль, в Україні це питання ще не знайшло свого достатнього вирішення.

 З огляду на це, вказана вище Стратегія, з-поміж напрямів реформування системи судоустрою, судочинства та суміжних правових інститутів виокремлює забезпечення належної координації правових інститутів та єдності інформаційної системи.

 Підвищення ефективності правосуддя та оптимізація повноважень судів різних юрисдикцій планується досягти шляхом забезпечення широкого використання інформаційних систем для надання більшої кількості послуг «електронного правосуддя»; створення в судах інформаційних систем електронного менеджменту, зокрема введення повноцінних електронних систем, у тому числі системи електронного документообігу, та відстеження справ (до вищих інстанцій), електронних повідомлень, електронних викликів, електронного розгляду справ (у деяких випадках), електронних платежів, аудіо- та відеофіксації засідань, інформаційної системи внутрішньої бази даних, інформаційної системи законодавчої бази даних, удосконалення системи забезпечення рівного та неупередженого розподілу справ між суддями, зокрема, визначення судді та (або) складу колегії суддів на всіх стадіях судового провадження; поетапне запровадження інструментів «електронного правосуддя», що дасть змогу користувачам звертатися до суду, сплачувати судовий збір, брати участь у провадженнях та отримувати необхідну інформацію і документи електронними засобами [2].

Особлива увага відводиться забезпеченню належної координації правових інститутів та єдності інформаційної системи, що, з-поміж іншого включає покращення управління та забезпечення взаємосумісності інформаційних систем судів, прокуратури, адвокатури, пенітенціарної служби та інших органів юстиції.

Судовий розгляд кримінальних справ як діяльність, пов’язана з аналізом і правовою оцінкою доказів, може бути визначений як інформаційний процес, що спирається на особливі види інформації: докази у справі, з одного боку, та законодавче, нормативно-правове поле України — з іншого. Впровадження сучасних інформаційних технологій у зазначену діяльність потребує створення такого предметного інформаційного середовища, яке забезпечить суддю необхідними даними, мінімізує затрати його часу на виконання технічної роботи, що в результаті сприятиме оперативності прийняття судових рішень.

Інформаційне забезпечення судочинства має за мету надати судді у зручному режимі роботи структуровану систему даних і знань щодо кожної судової справи:

1) законодавчі та відомчі нормативні акти;

2) статистичні дані про розгляд справ у судах;

3) матеріали узагальнення судової практики;

4) інформаційні ресурси центральних органів державної влади;

5) інформаційні ресурси органів внутрішніх справ України, прокуратури, інших інституцій, що беруть участь у кримінальному процесі;

6) інформацію з міжнародного права.

Враховуючи ще й такі аспекти судочинства, як відкритість та прозорість, а також необхідність забезпечення права громадян України на інформацію, особливу увагу слід звернути на створення інформаційно-пошукових систем матеріалів судової практики. Питання створення таких систем, як і взагалі питання доступу до правосуддя, неодноразово висвітлювалося в документах Ради Європи як одна з найважливіших умов справедливого застосування закону. На жаль, в Україні це питання ще не знайшло свого достатнього вирішення. Тільки частина документів, які становлять судову практику, міститься в базі даних «Законодавство». База даних «Рішення Верховного Суду України», яка накопичується з 1998 р., включає в себе понад 8000 документів. Оскільки ці рішення мають важливе значення для забезпечення однакового застосування закону, вкрай важливо, щоб доступ до них, у тому числі до зазначеної бази, мали всі судді України й інші учасники судового процесу, які мають таке право відповідно до закону. Це виключило б потребу в запитах, які часто можна зустріти в матеріалах кримінальних справ: «Просимо надіслати копію судового рішення...» (наприклад, для з’ясування питання про зняття судимості).

Завдання інформаційного забезпечення робіт із вивчення й узагальнення судової практики теж пов’язане з проблемою створення єдиного розподіленого інформаційного ресурсу «Рішення судів України». Великий інтерес у суддів викликають також інформаційні ресурси установ судової експертизи: їх територіальне розміщення, поштова й електронна адреси, службові телефони, дані про керівників судово-експертних установ і судових експертів, повний перелік (класифікація) виконуваних ними експертиз і вирішуваних у межах цих експертиз питань. Важливе значення мають дані про експертні спеціальності, за якими присвоєна експертна кваліфікація, строк атестації експертів.

Вирішуючи питання інформаційного забезпечення судді в рамках інтегрованої інформаційної системи судочинства, слід підкреслити важливість доступу до інформаційних ресурсів органів внутрішніх справ. Актуальність цієї проблеми відзначається багатьма спеціалістами, що працюють у галузі інформатизації судочинства. Як повідомляє Р. Абдулін, у Курганській області більшість суддів Російської Федерації при розгляді кримінальних справ мають можливість одержувати відомості про попередню судимість чи притягнення до кримінальної відповідальності з Інформаційного центру УВС області в автоматичному режимі. Підкреслюємо, мають можливість одержувати інформацію не згідно із запитом — усним, письмовим або з використанням електронної пошти, а в автоматичному режимі 1.

У матеріалах багатьох справ, розглянутих судами України, можна знайти лист такого змісту: «На ваш запит надсилаємо копію...» І лежить справа в суді й чекає, поки буде здійснено цю процедуру: запит — відповідь.

Інформатизація судового діловодства

Визначаючи систему документації, що застосовується в судочинстві, як і в будь-якій іншій сфері діяльності, як сукупність взаємопов’язаних документів, можна стверджувати, що в діяльності суду використовуються дві такі системи, незалежні одна від одної. Перша — пов’язана з процесуальною діяльністю з розгляду судових справ. Основні складові цієї системи передбачені процесуальними кодексами України, інструкціями з діловодства в судах. Друга — властива всім підприємствам і установам організаційно-розпорядницька система документації, визначена прийнятими в державі стандартами й доповнена в кожній установі її внутрішніми інструкціями.

У законодавчому забезпеченні робіт по впровадженню електронного документообігу в Україні зроблено перші кроки — прийнято закони України від 22 травня 2003 р.: № 851-IV «Про електронні документи та електронний документообіг» та № 852-IV «Про електронний цифровий підпис». Отже, на виконання «Прикінцевих положень» Закону «Про електронні документи та електронний документообіг» слід розробити програму заходів щодо впровадження електронних документів, електронного документообігу та електронного цифрового підпису в судовому процесі.

Зазначимо, що впровадження електронного документообігу у судочинство має свої особливості й пов’язане з деякими проблемами. Наприклад, протокол допиту свідка (підозрюваного, затриманого) зобов’язані підписати слідчий та особа, що дає свідчення. Отже, щоб забезпечити юридичну силу такому документові, його необхідно оформляти тільки в паперовому вигляді. І хоч ідея електронної судової справи здається дуже привабливою, при роботі зі справою, яка складається із сотні томів, природно виникає запитання: що ж робити з таким обсягом електронної інформації? Проте потреба допомогти судді в роботі над судовою справою є дуже актуальною. Зазначимо також, що тут виникає цікаве завдання: створити інформаційну технологію підтримки прийняття судового рішення як структурованої системи представлення матеріалів справи, установлення взаємозв’язку між фактами, документами, що їх підтверджують, та висновками обвинувачення.

Уже сьогодні більшість процесуальних документів — обвинувальні висновки, постанови, рішення суду тощо — виготовляється з використанням засобів обчислювальної техніки або друкарських машинок. До машинописних документів можна застосовувати процедури сканування та розпізнавання тексту, в результаті чого створюються їх електронні копії, наявність яких дає можливість оформити, так би мовити, електронну проекцію судової справи.

Відповідно до положень Закону від 7 лютого 2002 р. «Про судоустрій України», Кримінально-процесуального кодексу України вирішення кримінальної справи, як правило, складається з таких етапів:

1) досудовий розгляд (порушення кримінальної справи, дізнання, досудове слідство);

2) розгляд справи в суді першої інстанції;

3) розгляд справи за апеляцією;

4) касаційне провадження у справі (у порядку виключного провадження);

5) виконання вироку.

За останні роки у справі інформатизації кримінального судочинства зроблено чимало — створено систему інформаційного забезпечення органів внутрішніх справ, розроблено інформаційну технологію підтримки діяльності Верховного Суду України. Враховуючи набутий досвід, можна сформулювати першочергові завдання. Йдеться передусім про визначення переліку тих даних у справі, які в електронному вигляді можуть формуватися на одному етапі й використовуватися для реєстрації та прийняття рішення — на іншому.

На першому етапі — досудового розгляду — електронна справа може містити: відомості про обвинуваченого на момент вчинення злочину; відомості про цей злочин; обвинувальний висновок. Після розгляду справи в суді першої інстанції до електронної справи можуть бути долучені: відомості про розгляд справи в суді, вирок (ухвала, постанова).

Після апеляційного розгляду: відомості про розгляд апеляції, рішення суду апеляційної інстанції.

На етапі розгляду справи в касаційному порядку: відомості про касаційний розгляд, рішення суду касаційної інстанції.

При зверненні вироку до виконання згідно з ч. 2 ст. 404 КПК: розпорядження про його виконання, форма № 6.

Впровадження системи проходження електронної проекції кримінальної справи можливе лише за умови розроблення єдиної системи класифікаторів, які використовуються при реєстрації даних у справі. У зв’язку з цим потребують узгодження класифікатори:

1) видів економічної діяльності;

2) роду занять, службового становища;

3) злочинів;

4) мір покарання.

Розглядаючи схеми провадження в справах у кожній судовій інстанції, зазначимо, що кожна з них має свої особливості. Крім того, істотно різняться між собою правила провадження в кримінальних справах і справах, що виникають із цивільних та адміністративних правовідносин. Але в усіх видах провадження можна виділити окремі складові, які, утворюючи основу судового діловодства, не залежать від конкретного виду провадження. До них належать такі етапи:

1) надходження справи (заяви) до суду;

2) передача її на розгляд;

3) попередній розгляд;

4) судовий розгляд;

5) відправлення пошти.

Справа автоматизації діловодства в різних правових інституціях України робить перші кроки. Є приклади систем, які, будучи орієнтованими на формування й аналіз статистичних даних, у режимі дублювання паперового діловодства та документообігу відтворюють лише деякі елементи останніх. Відомі також факти прямого впровадження готових чи мінімально адаптованих програмно-апаратних комплексів. Такі підходи мають істотні недоліки, оскільки впровадження програмного продукту, орієнтованого на виконання лише певних функцій, має вплив на весь цикл провадження у справі й вимагає додаткових трудозатрат. Спираючись на засади системного підходу до справи інформатизації судочинства, слід з позицій інформаційних технологій комплексно розглядати всю систему діловодства, пов’язаного з надходженням та розглядом судової справи.

Системи підтримки прийняття рішень у судочинстві

Незважаючи на сучасні науково-технічні досягнення, з усього ланцюжка певного технологічного процесу сучасна наука не дозволяє автоматизувати процеси прийняття рішення й формування управлінського впливу, тому що вони великою мірою залежать від волі людини. І це не тільки технічна, а й правова проблема, оскільки прийняті рішення передбачають юридичну відповідальність, яку не можна перекласти на комп’ютер.

Функціонування системи судочинства пов’язане зі значною кількістю інформації як внутрішньої (матеріали справи), так і зовнішньої (законодавство, економічні, соціальні фактори тощо). У кібернетиці вони дістали назву складних систем. Результати їх аналізу мають бути спрямовані на прийняття обгрунтованих і максимально виважених рішень. Інформаційні системи, призначені для комплексного аналізу даних, що опрацьовуються, тенденцій розвитку останніх, називаються системами підтримки прийняття рішень.

Процес аналізу будь-якої сфери діяльності полягає у вивченні об’єкта чи явища, виявленні їх найбільш важливих характеристик. Виявлені характеристики подаються як та чи інша модель предметної області, дослідження якої дає можливість робити певні висновки стосовно самого предмета. Підкреслюючи неможливість побудови повної моделі складної соціальної системи (у тому числі системи судочинства), дослідники висувають концепцію макромоделювання, яка полягає в тому, що вирішення генерального завдання підмінюється вирішенням його частини: з усього надзвичайно складного механізму системи виділяються лише деякі зв’язки та відношення. Виявлені в процесі дослідження моделі властивості переносяться на саме явище, що дозволяє під час вивчення останнього уточнювати його модель, одержуючи нові, більш точні знання стосовно предмета дослідження.

Розроблення інформаційних моделей судочинства є справою окремих глибоких досліджень.

Виходячи, наприклад, із повноважень Верховного Суду України (гл. 8 Закону «Про судоустрій України») можна визначити основні види його діяльності:

— діловодство та документообіг, пов’язані з розглядом судових справ;

— ухвалення судових рішень;

— аналіз судової статистики;

— узагальнення судової практики;

— управління діяльністю судової палати, суду в цілому.

Перелічені види діяльності утворюють комплекс взаємозв’язаних процесів, які мають під собою єдину основу — інформацію (у тому чи іншому вигляді) стосовно кожної окремої справи й судового розгляду в цілому. Взаємозв’язаність полягає в тому, що жоден із цих видів діяльності не може здійснюватись окремо: для аналізу судової статистики потрібні дані, одержані в результаті виконання робіт із діловодства та документообігу, а для узагальнення судової практики чи управління діяльністю судової палати — дані статистичної звітності.

Аналізуючи матеріали кримінальних справ, можна дійти висновку, що інформаційна модель кримінального судочинства складається з двох частин: матеріальної (характеристики злочину, його суб’єкта, міри вини, видів покарання, результатів розгляду та підстав прийнятих рішень тощо) і процесуальної (дати надходження справи в суд, дати попереднього розгляду, причин перенесення судових засідань, підстав повернення справи на додаткове розслідування, новий судовий розгляд, дати набрання рішенням законної сили тощо).

На основі вивчення й аналізу цих даних у справі можна запропонувати три класи систем підтримки прийняття рішень у судочинстві.

1. Підтримка прийняття судового рішення, що базується на інформаційній моделі судової справи, формалізації діяльності, пов’язаної з аналізом та оцінкою судових доказів. Важливим завданням у цьому напрямі є структуризація процесуальних документів, представлення їх із використанням сучасної розширеної мови розмітки документів XML, що забезпечує можливість їх подальшої автоматизованої обробки й аналізу. Вивчення структури та змісту інформації, що міститься в обвинувальному висновку і в судових рішеннях, свідчить на користь розв’язання такого завдання.

2. Інформаційна підтримка узагальнення судової практики, що здійснюється на основі аналізу судової статистики, вивчення практики розгляду справ певної категорії та прийнятих у них рішень.

3. Підтримка діяльності керівників суду, спрямованої на організацію його роботи, яка повинна спиратися на різні можливі довідки, статистичні дані щодо розгляду справ у суді, їх складності та класифікації, навантаження суддів. Системи цього класу повинні відзначатися широкими можливостями зміни структури бази даних, наявністю засобів формування довільних звітів, засобів наочного представлення інформації у вигляді графіків, діаграм тощо.

Системи підтримки прийняття рішень у судочинстві, претендуючи на роль штучного інтелекту, не підміняють суддю, а виконують роль його електронного помічника й радника в процесі прийняття ним рішення. Головне завдання цих систем — підсилити велич людського інтелекту, обгрунтованість його рішень за допомогою надання широкої фактографічної бази, зручного та швидкого оперування даними й наочного представлення інформації.

**Лекція № 8**

**Тема 8. Правове забезпечення інформаційної безпеки. Основні положення Доктрини інформаційної безпеки України.**

**План лекції**

Основні засади інформаційної безпеки України. Інформаційна безпека в системі забезпечення національної безпеки України. Загрози інформаційній безпеці України. Напрями державної політики у сфері інформаційної безпеки України. Інформаційна безпека держави, суспільства та його громадян. Завдання, об'єкти посягань та форми проведення інформаційних війн. Ієрархія нормативних актів щодо забезпечення інформаційної безпеки.

**Література**

1. Богунов В. С. Щодо проблеми законодавчого врегулювання моніторингу телекомунікацій // Матер, наук.-практ. конф. 29 червня 2004 р. "Концептуальні засади забезпечення державної безпеки України". - К.: НА СБУ, 2004. - С. 53-56.

2. Ліпкан В. А, Максименко Ю. Є, Желіховськии Л. В. Інформаційна безпека України в умовах євро інтеграції: Навчальний посібник. -К.: КНТ, 2006. - 280 с. (Серія: Національна і міжнародна безпека).

3. Марущак А І. Інформаційне право: регулювання інформаційної діяльності: Навчальний посібник. - К.: Скіф, КНТ, 2008. - 344 с.

4. Марущак А /. Правомірні засоби доступу громадян до інформації: Науково-практичний посібник. - Біла церква: Буква, 2006. - 432 с.

5. Петрик В, М., Кузьменко A. M., Остроухое В. В. та ін. Соціально-правові основи інформаційної безпеки: Навчальний посібник / За ред. В. В. Остроухова. - К.: Росава, 2007. - 496 с.

6. Приватне життя і поліція. Концептуальні підходи. Теорія та практика. - Авторський колектив / Відп. ред. Ю. І. Римаренко. - К.: КНТ, 2006. - 740 с. - (Людина. Суспільство. Поліція)

7. Савельев Д. Некоторые проблемы международного права телекоммуникаций [Електронний ресурс] // Інтернет-сторінка "Право та інтернет".

8. Системна інформатизація законотворчої та правоохоронної діяльності. Монографія / Кер. авт. кол. Швець M. Я.; за ред. Дурдинця В. В., Зайчука О. В., Тація В. Я. - К.: Навчальна книга. - 2005. - 639 с.

9. Фронтов В., Тихвинский В. Регулирование телекоммуникаций в России и странах СНГ: Монография. - "Горячая линия-Телеком", 2006. - 368 с.

10. Юдін О. К., Богуш В. М. Інформаційна безпека держави: Навчальний посібник. - X.: Консул, 2005. - 576 с.

OECD. Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. – Paris:OECD,2002. – 28 p.

3. Проблеми впровадження культури безпеки в Україні: аналітична доповідь / Ю.М.Скалецький, Д.С.Бірюков, О.О.Мартюшева, Л.Д.Яценко. – К.: НІСД,2012. – 56 с.

4. Міжнародне безпекове середовище: виклики і загрози національній безпеці України / Б.О.Парахонський, Г.М.Яворська, О.О.Резнікова; за ред. К.А.Кононенка. – К.: НІСД,2013. – 56 с. 5. Сащук Г.М. Безпекові виміри телепростору: Монографія / Г.М.Сащук. – К.: Грамота, 2007. – С.16.

11. Конституція України: ухвалена на п'ятій сесії Верховної Ради України 28 червня 1996 р. // Відомості Верховної Ради (ВВР) України - 1996. - № ЗО . - Ст. 141.

12. Закон України "Про основи національної безпеки України" від 19 червня 2003 p. № 964-1V // ВВР України. - 2003. - № 39. -Ст. 351.

13. Закон України "Про інформацію" від 2 жовтня 1992 р. // ВВР України. - 1992. - № 48. - Ст. 650.

14. Закон України "Про державну таємницю" від 21 січня 1994 р. // ВВР України. - 1994. - № 16. - Ст. 93.

15. Закон України "Про телекомунікації" від 18 листопада 2003 р. // ВВР України. - 2004. - № 12. - Ст. 155.

16. Закон України "Про зв'язок" від 16травня 1995 р. (в редакції від 5 червня 2003 р.) // ВВР України. - 2006. - № 30. - Ст. 258.

17. Закон України "Про радіочастотний ресурс" від 1 червня 2000 р. // ВВР України - 2000. - № 36. - Ст. 298.

**Зміст лекції**

Значним кроком на шляху створення системи нормативно-правового регулювання забезпечення інформаційної безпеки України стало прийняття Верховною Радою України Конституції України від 28 червня 1996 р. В ній, зокрема, є норми, що стосуються забезпечення інформаційної безпеки України та які є визначальними для побудови національної системи інформаційної безпеки (статті 1-8; 15; 18; 19; 34; 78; пункти 2 і 9 ч. 1 ст. 85; пункти 19-20 ч. 1 ст. 106; ст. 182; пункти 7 і 10 ст. 138).

Так, зокрема, у ч. 1 ст. 17 Конституції України забезпечення інформаційної безпеки України оголошено "справою всього українського народу". При цьому з точки зору захисту прав людини і громадянина в інформаційній сфері найбільш знаковою є ст. 34 Конституції. Відповідно до цієї статті кожному гарантується " право на свободу думки й слова, на свободу вираження своїх поглядів і переконань", а також "право вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або іншим способом за своїм вибором ".

Реалізацію гарантованих ст. 34 Конституції України прав може бути "обмежено законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою попередження заворушень або злочинів, для охорони здоров'я населення, для захисту репутації або прав інших людей, для попередження розголошення інформації, отриманої конфіденційно, або для підтримки авторитету й неупередженості правосуддя". Як видно, коло обмежень досить широке, однак кожне з них повинне бути визначене законом.

У статті 107 Основного Закону закріплено законність функціонування Ради національної безпеки і оборони України як координаційного органу з питань національної безпеки при Президентові України.

Викладені положення Конституції України, в свою чергу, стали поштовхом до розробки всього пакета нормативно-правових актів, необхідних для ефективного забезпечення національної безпеки України в інформаційній та інших сферах її існування - зовнішньо-та внутрішньополітичній, державної безпеки, військовій та сфері безпеки державного кордону, економічній, соціальній, гуманітарній, науково-технологічній та екологічній.

Відповідно до ст. 34 Конституції України здійснення гарантованих нею прав - "права на свободу думки й слова, на свободу вираження своїх поглядів і переконань", "права вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або іншим способом за своїм вибором" - може бути "обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою попередження заворушень або злочинів, для охорони здоров'я населення, для захисту репутації або прав інших людей, для попередження розголошення інформації,, отриманої конфіденційно, або для підтримки авторитету й неупередженості правосуддя". Отже, коло обмежень досить широке, однак кожне з них повинне бути визначене законом.

У січні 1997 р. Верховна Рада України схвалила "Концепцію (основи державної політики) національної безпеки України" (далі - концепція). Цей документ нормативно закріпив загальні положення та принципи забезпечення національної безпеки України, національні інтереси і загрози національній безпеці, основні напрями державної політики національної безпеки, систему її забезпечення та повноваження основних суб'єктів цієї системи. Серед основних принципів її забезпечення названі пріоритет прав людини, верховенство права й демократичний цивільний контроль за військовою сферою й іншими структурами в системі забезпечення національної безпеки.

Поряд з іншими можливими загрозами національній безпеці зазначені й загрози в інформаційній сфері - "інформаційна експансія з боку інших держав, витік інформації, що становить державну та іншу, передбачену законом, таємницю" а також конфіденційної інформації, що є власністю держави".

Серед основних напрямів реалізації державної політики національної безпеки в інформаційній сфері Концепцією були визначені:

- вживання комплексних заходів щодо захисту свого інформаційного простору й входження України у світовий інформаційний простір;

- усунення негативних факторів порушення інформаційного простору, інформаційної експансії з боку інших держав [протидія СІО, АІА та іншим деструктивним ІПВ. - Прим, авт.];

- розробка та запровадження необхідних засобів І режимів одержання, зберігання, поширення й використання суспільно значимої інформації, створення розвинутої інфраструктури в інформаційній сфері.

Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 р, № 514/2009 (далі - Доктрина) визначає інформаційну безпеку як самостійну сферу забезпечення національної безпеки України та одночасно як невід'ємну складову кожної а її сфер.

Основною метою реалізації положень Доктрини задекларовано створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету.

Доктрина визначає принципи забезпечення інформаційної безпеки України, життєво важливі інтереси в інформаційній сфері України в контексті інтересів особи, суспільства, держави, а також реальні та потенційні загрози інформаційній безпеці України - у сфері державної безпеки та у зовнішньополітичній, воєнній, внутрішньополітичній, економічній, соціальній, гуманітарній, науково-технологічній, екологічній сферах.

Відповідно до положень Доктрини, діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства і людини за трьома головними напрямами: інформаційно-психологічному, технологічного розвитку та захисту інформації.

Держава для забезпечення інформаційної безпеки України має вживати відповідних заходів в усіх сферах, де існують реальні та потенційні загрози - у сфері державної безпеки та у зовнішньополітичній, воєнній, внутрішньополітичній, економічній, соціальній, гуманітарній, науково-технологічній, екологічній сферах.

У Законі України "Про основи національної безпеки України" від 19 червня 2003 р. № 964-ІУ нормативно закріплено компетенцію та функції усіх визначених законом суб'єктів забезпечення національної безпеки України в усіх сферах, зокрема в інформаційній.

Цей Закон відповідно до п. 17 ч. 1 ст. 92 Конституції України визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності, зокрема в інформаційній сфері.

Відповідно до ст. З Закону об'єктами національної безпеки в інформаційній сфері є: а) людина і громадянин - їхні конституційні права і свободи; б) суспільство - його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; в) держава - її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Основними принципами забезпечення національної безпеки в інформаційній сфері е: пріоритет прав і свобод людини і громадянина; верховенство права; пріоритет договірних (мирних) засобів у розв'язанні конфліктів; своєчасність і адекватність заходів захисту національних інтересів реальним і потенційним загрозам; чітке розмежування повноважень та взаємодія органів державної влади у забезпеченні національної безпеки; демократичний цивільний контроль над Воєнною організацією держави та іншими структурами в системі національної безпеки; використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки.

Згідно зі ст. 4 Закону суб'єктами забезпечення національної безпеки в інформаційній сфері є: Президент України; Рада національної безпеки і оборони України; Верховна Рада України; Кабінет Міністрів України; міністерства та інші центральні органи виконавчої влади;

Збройні сили України, Служба безпеки України та інші військові формування, утворені відповідно до законів України; суди загальної юрисдикції; прокуратура України; місцеві державні адміністрації та органи місцевого самоврядування.

Повноваження суб'єктів забезпечення національної безпеки визначені у ст. 9 Закону України "Про основи національної безпеки України", а також у відповідних профільних законах та положеннях, що предметно регулюють правовий статус кожного з них.

Національна безпека України в інформаційній сфері забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах.

Вибір конкретних засобів і шляхів забезпечення національної безпеки України в інформаційній сфері обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам.

Основні напрями державної політики в інформаційній сфері, визначені в ст. 8 Закону:

- забезпечення інформаційного суверенітету України;

- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

- активне залучення засобів масової інформації до протидії корупції, зловживанням службовим становищем, іншим явищами, які загрожують національній безпеці України;

- забезпечення неухильного дотримання конституційного право громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність ЗМІ, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Відповідно до Закону України "Про основи національної безпеки України" цільові настанови та керівні принципи державного будівництва в інформаційній сфері, а також напрями діяльності органів державної влади в конкретній обстановці визначаються Стратегією національної безпеки України з метою своєчасного виявлення, відвернення і нейтралізації реальних і потенційних загроз національним інтересам України в інформаційній та інших сферах життєдіяльності. Положення Стратегії національної безпеки України, які стосуються забезпечення інформаційної безпеки нашої держави, буде розкрито нами долі у характеристиці нормативно-правових актів Президента України.

Ще одним важливим для забезпечення інформаційної безпеки України нормативним актом є Закон України "Про інформацію" від

2 жовтня 1999 р. № 2657-ХІІ (далі - Закон). Цим Законом закладено правові основи інформаційної діяльності, стверджено інформаційний суверенітет України, закріплене право на інформацію та на доступ до неї, визначено систему відносин і зобов'язань у цій сфері, прийняту для демократичної держави, визначено правові форми міжнародного співробітництва в галузі інформації"

Під інформацією цей Закон (ст. 1) розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує П охорону, захищає особу та суспільство від неправдивої інформації. Дія цього Закону поширюється на інформаційні відносини, які виникають у всіх сферах життя і діяльності суспільства і держави під час одержання, використання, поширення та зберігання інформації (зокрема й використання мережі Інтернет).

Відповідно до ст. 7 Закону суб'єктами інформаційних відносив є: громадяни України, юридичні особи та держава. Ними можуть бути також Інші держави, їх громадяни та юридичні особи, міжнародні організації та особи без громадянства.

Об'єктами інформаційних відносин є документована або публічно оголошувана інформація про події та явища в галузі політики, економіки, культури, охорони здоров'я, а також у соціальній, екологічній, міжнародній та інших сферах (ст. 8 Закону).

Окрім того, Законом закріплене право на інформацію, гарантоване Конституцією України (ст. 34), а також гарантії цього права. Згідно зі ст. 9 Закону, всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій. Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України. Реалізація права на інформацію зазначеними суб'єктами не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Також Закон у ст. 12 дає визначення інформаційної діяльності: "Це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави". З метою задоволення цих потреб органи державної влади та органи місцевого і регіонального самоврядування створюють інформаційні служби, системи, мережі, бази і банки даних. Порядок їх створення, структура, права та обов'язки визначаються Кабінетом Міністрів України або інтими органами державної влади, а також органами місцевого і регіонального самоврядування.

Основними напрямами інформаційної діяльності е: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо (ст. 12 Закону).

Держава зобов'язана постійно дбати про своєчасне створення, належне функціонування і розвиток інформаційних систем, мереж, банків і баз даних у всіх напрямах інформаційної діяльності. Держава гарантує свободу інформаційної діяльності за цими напрямами всім громадянам та юридичним особам в межах їх прав і свобод, функцій і повноважень.

Відповідно до ст. 13 Закону основними видами інформаційної діяльності є одержання, використання, поширення та зберігання інформації. Одержання, використання, поширення та зберігання документованої або публічно оголошуваної інформації здійснюється у порядку, передбаченому цим Законом та іншими законодавчими актами в галузі інформації.

Окрім висвітлених вище положень, в Законі України "Про інформацію" також розкриваються: 1) галузі, види, джерела інформації та режим доступу до неї (Розділ III); 2) учасники інформаційних відносив, їх права та обов'язки (Розділ IV); 3) охорона інформації та загальні положення про відповідальність за порушення законодавства про інформацію (Розділ У); 4) міжнародна інформаційна діяльність, співробітництво з іншими державами, зарубіжними та міжнародними організаціями в галузі інформації (Розділ VI).

Іншим важливим законодавчим актом, що регулює інформаційну діяльність у сфері державної таємниці, є Закон України "Про державну таємницю" від 21 січня 1994 р. № 3855-ХІІ.

Зокрема, цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

Дія цього Закону поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші органи державної влади, Верховну Раду АР Крим, Раду міністрів АР Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі - органи державної влади, органи місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці (ст. 3).

Відповідно до ст. 4 Закону державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики визначає Верховна Рада України. Окрім того, Законом визначено компетенцію органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці (ст. 5 Закону), здійснення права власності на секретну інформацію та її матеріальні носії (ст. 6 Закону), а також порядок фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею (ст. 7 Закону).

В розділі її Закону України "Про державну таємницю" розкрито низку положень щодо віднесення інформації до державної таємниці. Зокрема, відповідно до ст. 8 Закону, до державної таємниці у порядку, встановленому цим Законом, відноситься інформація: 1) у сфері оборони; 2) у сфері економіки, науки і техніки; 3) у сфері зовнішніх відносин; 4) у сфері державної безпеки та охорони правопорядку.

Не належить до державної таємниці інформація:

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

- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

- про факти порушень прав і свобод людини і громадянина;

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

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

У статті 9 Закону розкрито компетенцію, права, обов'язки та відповідальність державних експертів з питань таємниць, а в ст. 10 - порядок віднесення інформації до державної таємниці.

Окремою нормою (ст. 12) в Законі визначено положення щодо Зводу відомостей, що становлять державну таємницю. Ці положення конкретизовані в наказі СБ України № 440 від 12 серпня 2005 р.р яким затверджено Звід відомостей, що становлять державну таємницю.

Положення щодо засекречування та розсекречування матеріальних носіїв інформації детально розкриті в Законі у Розділі ПІ.

Відповідним розділом в Законі виділено положення щодо охорони державної таємниці (Розділ IV). При цьому в ст. 18 Закону розкриті основні організаційно-правові заходи щодо охорони державної таємниці.

Зокрема, з метою охорони державної таємниці впроваджуються:

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

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

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

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

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

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

- спеціальний порядок допуску та доступу громадян до державної таємниці;

- технічний та криптографічний захисти секретної інформації. Окремими нормами в Законі врегульовані обов'язки громадян України щодо збереження державної таємниці (ст. 28), обмеження їх прав у зв'язку з допуском та доступом до державної таємниці (ст. 29), а також положення щодо належної їм компенсації у зв'язку з виконанням робіт, які передбачають доступ до державної таємниці (ст. ЗО).

Закон України "Про державну таємницю" також містить низку важливих положень щодо встановлення обмежень на оприлюднення секретної інформації (ст. 31), щодо передачі державної таємниці іноземній державі чи міжнародній організації (ст. 32), а також обмежень, пов'язаних з державною таємницею, щодо перебування і діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, а також розташування та переміщення об'єктів і технічних засобів, що їм належать (ст. 33).

Технічний та криптографічний захисти секретної інформації здійснюються в порядку, встановленому нормативними актами Президента України.

Окрім висвітлених вище положень, в Законі України "Про державну таємницю" також розкриваються загальні положення про відповідальність за порушення законодавства про державну таємницю (Розділ VI), зміст яких конкретизовано у відповідних статтях Кримінального кодексу України та Кодексу України про адміністративні правопорушення.

Вагомим кроком для забезпечення інформаційної безпеки України на шляху впровадження та використання новітніх інформаційних технологій в усі сфери діяльності держави та суспільного життя стало прийняття законів України "Про Національну програму інформатизації" від 4 лютого 1998 р. № 74/98-ВР та "Про Концепцію Національної програми інформатизації" від 4 лютого 1998 р. № 75/98.

Базовим законом у сфері інформатизації на сучасному етапі е Закон України "Про Національну програму інформатизації" від 4 лютого 1998 р. № 74/98-ВР (далі - Закон), однією із двох головних цілей якої проголошене забезпечення інформаційної безпеки держави.

Врегульована цим Законом Національна програма інформатизації визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення.

Національна програма інформатизації спрямована на створення умов, необхідних для забезпечення громадян, суспільства та держави своєчасною, достовірною та повною інформацією шляхом широкого використання новітніх інформаційних технологій, забезпечення інформаційної безпеки держави.

Національна програма інформатизації включає положення про:

- Концепцію Національної програми інформатизації;

- сукупність державних програм з інформатизації;

- галузеві програми та проекти інформатизації;

- регіональні програми та проекти інформатизації;

- програми та проекти інформатизації органів місцевого самоврядування.

Призначенням законодавства про Національну програму інформатизації є запровадження правових, організаційних, науково-технічних, економічних, фінансових, методичних та гуманітарних засад регулювання процесу формування та виконання цієї Програми та окремих її завдань (проектів). Закон також встановлює основні функції органів державної влади у процесі інформатизації, зокрема:

- забезпечення інформаційної безпеки держави;

- встановлення стандартів, норм і правил використання засобів інформатизації;

- забезпечення доступу громадян та їх об'єднань до інформації органів державної влади та органів місцевого самоврядування, а також до інших джерел інформації;

- визначення пріоритетних напрямів інформатизації з метою подальшої її підтримки шляхом державного фінансування та пільгового оподаткування;

- інформатизацію науки, освіти, культури, охорони довкілля та здоров'я людини, державного управління, національної безпеки та оборони держави, пріоритетних галузей економіки;

- підтримку вітчизняного виробництва програмних і технічних засобів інформатизації;

- підтримку фундаментальних наукових досліджень для розроблення швидкісних математичних і технічних засобів обробки інформації;

- забезпечення підготовки спеціалістів з питань інформатизації та інформаційних технологій;

- організацію сертифікації програмних і технічних засобів інформатизації;

- державне регулювання цін і тарифів на використання телекомунікаційних та комп'ютерних мереж для потреб інформатизації у бюджетній сфері;

- захист авторського права на бази даних і програми, створені для потреб інформатизації та особистої інформації.

У законі визначено етапи формування і виконання, порядок здійснення експертизи, механізм контролю за виконанням Національної програми інформатизації, замовників, науково-технічну раду та виконавців програми, їх права та обов'язки.

В свою чергу, в Законі України "Про Концепцію Національної програми інформатизації" від 4 лютого 1998 р. № 75/98 (далі - Закон) важливим фактором подолання відставання України у сфері інформатизації названа ефективна державна політика інформатизації.

Окрім того, в цьому Законі закріплені принципи державної політики у сфері інформатизації, визначені основні завдання, напрями, порядок формування та виконання основних етапів програми, очікувані результати.

Зокрема, Законом визначені такі основні напрями інформатизації:

- вироблення державної політики у сфері інформатизації та організаційно-правове забезпечення інформатизації;

- формування національної інфраструктури інформатизації, яка включає: міжнародні та міжміські телекомунікаційні та комп'ютерні мережі; систему інформаційно-аналітичних центрів різного рівня;

- інформаційні ресурси; інформаційні технології; систему науково-дослідних установ з проблем інформатизації; виробництво та обслуговування технічних засобів інформатизації;

- створення системи підготовки висококваліфікованих фахівців у сфері інформатизації;

Правову основу користування радіочастотним ресурсом України, повноваження держави щодо визначення умов користування цим ресурсом, права, обов'язки і відповідальність органів державної влади, що здійснюють управління і регулювання в цій сфері, а також фізичних і юридичних осіб, які користуються радіочастотним ресурсом встановлює Закон України "Про радіочастотний ресурс України" від 1 червня 2000 р. № 1770-ІИ.

Дія Закону поширюється на відносини між органами державної влади України, фізичними та юридичними особами щодо розподілу, виділення смуг радіочастот, присвоєння радіочастот радіоелектронним засобам, користування радіочастотним ресурсом України, забезпечення конверсії радіочастотного ресурсу України, а також електромагнітної сумісності.

Закон залежно від напрямів використання радіочастотного ресурсу поділяє користувачів на спеціальні й загальні, визначає їх права й обов'язки (ст. 6) та відповідальність (ст. 7). До числа спеціальних користувачів радіочастотного ресурсу України відносяться підрозділи й органи Міноборони України, СБУ, СЗР України, ДССЗІ України, МВС України, МИС України, ДПС України, Управління державної охорони, Держдепартамент з питань виконання покарань, податкова міліція ДПА України, а також Мінтрансзв'язку України (в частині застосування радіоелектронних засобів об'єднаної цивільно-військової системи організації повітряного руху України та забезпечення польотів, а також застосування таких засобів Державною спеціальною службою транспорту).

До числа загальних користувачів радіочастотного ресурсу України належать такі користувачі: суб'єкти господарювання, які використовують цей ресурс для надання телекомунікаційних послуг, розповсюдження телерадіопрограм із застосуванням власних або орендованих радіоелектронних засобів; технологічні користувачі і радіоаматори - юридичні чи фізичні особи, які користуються ресурсом без надання телекомунікаційних послуг.

Державне управління у сфері користування радіочастотним ресурсом України відповідно до статей 10 і 11 Закону здійснюють Кабінет Міністрів України та Державна адміністрація зв'язку Мінтрансзв'язку України як центральний орган виконавчої влади у галузі зв'язку (ЦОВЗ).

Органом регулювання у сфері користування радіочастотним ресурсом України є Національна комісія з питань регулювання зв'язку (НКРЗ), яка утворюється відповідно до Закону України "Про телекомунікації" (ст. 17). Повноваження НКРЗ щодо регулювання у сфері користування радіочастотним ресурсом України визначені ст. 14 Закону.

Державний нагляд за користуванням радіочастотним ресурсом України, запобігання правопорушенням під час користування ресурсом у смугах радіочастот загального користування а також притягнення в установленому законом порядку до адміністративної відповідальності осіб, винних у порушенні законодавства про радіочастотний ресурс України, здійснює Державна інспекція зв'язку. Порядок здійснення державного нагляду щодо смуг радіочастот загального користування затверджується НКРЗ. Державний нагляд за користуванням радіочастотним ресурсом України у смугах радіочастот спеціального користування здійснює Генеральний штаб Збройних сил України в межах своєї компетенції та в порядку, визначеному законом.

Присвоєння радіочастот, видача дозволів на експлуатацію загальним користувачам радіочастотного ресурсу, призначення позивних сигналів радіоелектронним засобам у смугах радіочастот загального користування, ведення реєстру присвоєнь радіочастот, проведення моніторингу використання радіочастотного ресурсу України у смугах радіочастот загального користування та інші завдання виконує "Український державний центр радіочастот" (УДЦР).

Присвоєння смуг радіочастот радіоелектронним засобам і випромінювальним пристроям, а також радіочастотний моніторинг у смугах радіочастот спеціального користування здійснюється Генштабом Збройних сил України.

Окремо Закон у ст. 24 визначає повноваження Національної ради України з питань телебачення і радіомовлення щодо регулювання у сфері користування радіочастотним ресурсом України.

Розділ V Закону визначає умови та встановлює порядок визначення можливості застосування радіоелектронних засобів та випромінювальних пристроїв на території України, порядок їх ввезення з-за кордону, реалізації й експлуатації, загальні положення щодо стандартизації та метрологічного забезпечення у сфері користування радіочастотним ресурсом України.

Загальні положення щодо користування радіочастотним ресурсом України передбачені у Розділі VI Закону. Зокрема, ст. 30 Закону визначає засади і принципи користування радіочастотним ресурсом. Порядок ліцензування користування радіочастотним ресурсом розкритий у статтях 31-39 Закону.

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 р. № 2594-ІУ (далі - Закон) регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

Зокрема, об'єктами захисту в таких системах відповідно до Закону є інформація, що обробляється, та програмне забезпечення, яке призначене для обробки цієї інформації (ст. 2 Закону).

Суб'єктами відносин, пов'язаних із захистом інформації в системах, ст. З Закону визначає: власників інформації та інформаційно-телекомунікаційних систем, користувачів інформації та систем, а також уповноважений орган у сфері захисту інформації в інформаційно-телекомунікаційних системах.

У Законі зазначено, що порядок доступу до інформації визначається власником інформації. Порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження щодо цієї інформації визначаються законодавством України. У передбачених Законом випадках та у встановленому ним порядку доступ до інформації в системі може здійснюватися і без дозволу її власника (ст. 4 Закону).

Відносини між власником інформації та власником системи визначаються договором. Умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації (ст. 8 Закону). Відповідальність за забезпечення захисту інформації в системі покладається на власника системи (ст. 9 Закону).

Закон визначає повноваження уповноваженого органу у сфері захисту інформації в системах, відповідальність за порушення законодавства про захист інформації в системах (ст. 10 Закону).

Окремо в числі нормативних актів, які регулюють сферу забезпечення інформаційної безпеки держави, слід виділити Закон України "Про захист суспільної моралі" 20 листопада 2003 р. Лг 1296-ІУ (далі - Закон), який встановив правові основи захисту суспільства від розповсюдження продукції, що пропагує культ насильства, жорстокості, порнографії та негативно впливає на суспільну мораль.

Закон забороняє виробництво та обіг у будь-якій формі продукції порнографічного характеру в Україні. Критерії віднесення продукції до такої, що має порнографічний характер, встановлюються спеціально уповноваженим органом виконавчої влади у сфері культури та мистецтв.

Виробництво та обіг у будь-якій формі продукції сексуального чи еротичного характеру та продукції, що містить елементи насильства та жорстокості, дозволяються виключно за умови дотримання обмежень, встановлених законодавством.

Окрім того, забороняються виробництво та розповсюдження продукції, яка:

- пропагує війну, національну та релігійну ворожнечу, зміну шляхом насильства конституційного ладу або територіальної цілісності України;

- пропагує фашизм та неофашизм;

- принижує або ображає націю чи особистість за національною ознакою;

- пропагує бузувірство, блюзнірство, неповагу до національних і релігійних святинь;

- принижує особистість, с проявом знущання з приводу фізичних вад (каліцтва), з душевнохворих, літніх людей;

- пропагує невігластво, неповагу до батьків;

- пропагує наркоманію, токсикоманію, алкоголізм, тютюнопаління та інші шкідливі звички.

Відповідно до ст. 4 Закону сфера його дії поширюється на діяльність органів державної влади, органів місцевого самоврядування у частині державного регулювання і контролю за обігом продукції сексуального чи еротичного характеру, на діяльність установ та організацій усіх форм власності, юридичних осіб та громадян у сфері обігу відповідної продукції на території України, а також за її межами, якщо суб'єктами правовідносин е громадяни України та юридичні особи, зареєстровані відповідно до чинного законодавства України.

Змістом державної політики у сфері захисту суспільної моралі е створення в Україні необхідних правових, економічних та організаційних умов, які сприяють реалізації права на національний інформаційний простір, вільний від матеріалів, що становлять загрозу фізичному, інтелектуальному, морально-психологічному стану населення країни.

Основними напрямами державного регулювання обігу інформаційної продукції, що впливає на суспільну мораль, є:

- формування єдиної комплексної системи забезпечення захисту моральних засад і утвердження здорового способу життя у сфері інформаційної діяльності, освіти та культури;

- недопущення пропаганди в електронних та інших засобах масової інформації культу насильства, жорстокості, поширення порнографії;

- впровадження експертної оцінки відео-, аудіо-, друкованої інформації та інформації на електронних носіях, розроблення механізмів і методик віднесення її до такої, що завдає шкоди суспільній моралі;

- підтримка національної культури, мистецтва, кінематографії, книговидання, поліпшення системи пропаганди кращих зразків світової літератури, культури та мистецтва;

- заборона демонстрації неліцензійної аудіо-, відеопродукції на всіх національних телерадіокомпаніях;

- встановлення контролю за обігом продукції, що становить загрозу суспільній моралі;

- приєднання до міжнародних договорів з питання захисту суспільної моралі.

Закон, окрім встановлення порядку та обмежень на виробництво та обіг продукції і видовищних заходів сексуального (еротичного) характеру (статті 8-9, 11-14), також передбачає у ст. 7 здійснення захисту морального та фізичного життя неповнолітніх від негативного впливу.

Окремо Закон регламентує експертну діяльність органами державної влади та реєстрацію продукції і видовищних заходів сексуального чи еротичного характеру (у ст. 10), а також порядок проведення експертизи продукції і видовищних заходів сексуального чи еротичного характеру (ст. 20).

ІНФОРМАЦІЙНА БЕЗПЕКА (ІБ) - стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди.

Це визначення найбільш оптимальне тому, що об'єднує пасивну (стан захищеності) та активну (стан інформаційного розвитку) складові, а також є лаконічним і передбачає поділ інформаційної безпеки на різновиди.

Інформаційний вплив - організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення змін у свідомість особи чи населення (корекція поведінки) та (або) інформаційно-технічну інфраструктуру об'єкта та (або) фізичний стан людини.

Інформаційно-психологічний вплив (ІПВ) - вплив на свідомість особи і населення з метою внесення змін у їх поведінку та (або) світогляд.

Інформаційно-технічний вплив (ІТВ) - вплив на інформаційно-технічну інфраструктуру об'єкта з метою забезпечення реалізації необхідних змін у його роботі (зупинка роботи, несанкціонований витік інформації, програмування на певні помилки, зниження швидкості обробки інформації та ін.), а також вплив на фізичний стан людини. ІТВ становить загрозу безпеці інформаційно-технічної інфраструктури та фізичному стану людини.

Безпека інформаційно-технічної інфраструктури - це стан захищеності, який забезпечує її ефективне використання та захист від можливого ІТВ.

Безпека інформаційно-технічної інфраструктури поділяється на безпеку:

- машинно-технічних засобів (автоматизованих систем та мереж);

- програмного забезпечення;

- режиму захисту від несанкціонованого витоку інформації.

пливи не завдають суттєвої шкоди національним інтересам (див. схему ).

Спеціальні інформаційні операції (СІО) - це сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію, які передбачають прихований вплив на її свідомість і поведінку за допомогою використання організованої інформації та інформаційних технологій для досягнення певної мети.

Акції інформаційної агресії (АІА) - легальні та (або) протиправні акції, які проводяться шляхом поширення упередженої, неповної або недостовірної інформації, що можуть призвести до негативного впливу на інформаційну безпеку держави.

Інформаційний тероризм - небезпечні діяння з інформаційного виливу на соціальні групи й окремих осіб, державні органи влади управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також викривлення об'єктивної інформації, що спричиняє виникнення кризових ситуацій у державі, нагнітання страху і напруги в суспільстві.

Комп'ютерна злочинність - це відносно масове, соціальне явище, яке складається з суспільно небезпечних діянь, де електронно-обчислювальні машини, мережі, системи та представлена в них інформація є знаряддям або предметом злочинних діянь.

Об'єктами забезпечення ІБ держави є:

- інформаційно-телекомунікаційна інфраструктура (суб'єкти та засоби створення, поширення інформації і передачі даних);

- інформація (особиста, конфіденційна, власність держави, з обмеженим доступом);

- свідомість (особи, групи осіб, суспільства).

Поняття інформаційної безпеки можна разглядати у декількох ракурсах. По-перше, це стан захищенності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави.

Під інформаційним середовищем розуміють сферу діяльності суб’єктів, пов’язану із створенням, обробленням й споживанням інформації.

По-друге, інформаційна безпека – це стан захищенності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Стан інформованості визначає ступінь адекватності сприйняття суб’єктами навколишньої дійсності і як наслідок – обгрунтованість рішень і дій, що приймаються.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

*Об’єктами інформаційної безпеки* можуть бути: свідомість, психіка людини; інформаційні системи різного масштабу й різного призначення. До соціальних об’єктів інформаційної безпеки відносять особистість, колектив, державу, суспільство, світове товариство.

До *суб’єктів інформаційної безпеки* належать: держава, що здійснює свої функції через відповідні органи; громадяни, суспільні або інші організації і обʹєднання, що володіють повноваженнями щодо забезпечення інформаційної безпеки відповідно до законодавства.

Види інформаційної безпеки

Інформаційна безпека особистості – це захищенність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо.

Інформаційна безпека держави характеризується мірою захищенності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. В рамках цієї концепції проводиться системна класифікація дестабілізуючих факторів та інформаційних загроз безпеці особистості, суспільства, держави; обгрунтовуються основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції щодо способів і форм забезпечення інформаційної безпеки.

**Загрози інформаційній безпеці**

Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєвоважливим інтересам особистості, суспільства й держави в інформаційній сфері. Основні загрози інформаційній безпеці поділяють на три групи:

- загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

- загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання);

- загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову).

Фактори загроз за видовою ознакою поділяються на політичні, економічні і організаційно-технічні.

Явища та процеси природного й штучного походження, що породжують інформаційні загрози, називають дистабілізуючими факторами.

*Джерелами дестабілізуючих факторів* можуть бути як окремі особи, так й організації і їхні об’єднання. Особливу групу джерел складають інформаційні системи та засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей та інших причин.

Джерелом дестабілізуючих факторів може бути також природне середовище. Кожному джерелу властиві певні види дестабілізуючих факторів, які можна подати у вигляді міждержавних і внутрішньодержавних.

До внутрішньодержавних дестабілізуючих факторів відносять: правовий вакуум у більшості питань забезпечення інформаційної безпеки; порушення законодавства з питань інформаційної безпеки; політичні конфлікти; відмови, збої, технічні помилки інформаційних систем (засобів); природні явища, що ускладнюють передачу, прийом і зберегання інформації або руйнують інформаційні системи.

Міждержавні дестабілізуючі фактори – це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії тощо).

Конституція України : Закон України від 28.06.96 р. № 254к/96-ВР // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – Ст. 141. 13

2. Про інформацію : Закон України від 02.10.92 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

3. Про внесення змін до Закону України “Про інформацію” : Закон України від 13.01.11 р. № 2938-VI // Офіційний вісник України. – 2011. – № 10.

4. Про основи національної безпеки України : Закон України від 19.06.03 р. № 964-ІV // Відомості. Верховної Ради України. – 2003. – № 39. – Ст. 351.

5. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009 // Офіційний вісник Президента України. – 2009. – № 20. – С. 18. – Ст. 677.

6. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

7. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI : за станом на 16.01.12 р. // Відомості Верховної Ради України. – 2010. – № 34. – С. 1188. – Ст. 481.

8. Про електронні документи та електронний документообіг : Закон України від 22.05.03 р. № 851-IV : за станом на 16.01.12 р. // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275.

9. Про Концепцію Національної програми інформатизації : Закон України від 4 лютого 1998 р. № 75/98-ВР // Відомості Верховної Ради України (ВВР), 1998, N 27-28, ст.182

10. Про затвердження Програми інф інформатизації законотворчого процесу у Верховній Раді України на 2012-2017 роки : Постанова Верховної Ради України від 05.07.2012 // Відомості Верховної Ради (ВВР), 2013, № 37, ст.492

11. Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України : Наказ МВС України від 12.10.2009 № 436 // Офіційний вісник України від 11.01.2010 № 101, стор. 409 12. Правова інформатика. / М.Швець, В. Брижко, Л.Задорожня, Ю.Клімашевська, В.Фурашев, В.Хахановський, В.Цимбалюк та ін. – У 2-х т. – К.: Парлам. вид-во, 2005. – Т. 1. – 416 с.

13. Цимбалюк В. С. Інформаційне право (основи теорії і практики). — К.: «Освіта України», 2010. – 388 с.

14. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє / В.Фурашев, Д.Ланде, О.Григор’єв, О.Фурашев. – К.: “Інжиніринг” 2005. – 164 с.

15. Пономаренко В. С., Журавльова І. В., Туманов В. В. Основи захисту інформації. Навчальний посібник. — Харків: Вид. ХДЕУ, 2003. — 176 с.

16. Інформаційне право та правова інформатика у сфері захисту персональних даних / В.Брижко, М.Гуцалюк, В.Цимбалюк, М.Швець; За ред. д.е.н., професора, члена-кореспондента Академії правових наук України М.Швеця. – К.: НДЦПІ АПрН України, 2005. – 451 с.

17. Чубукова С.Г., Элькин В.Д. Основы правовой информатики (юридические и математические вопросы информатики): Учебное пособие / Под ред. проф. М.М. Рассолова. – М.: Юридическая фирма «КОНТРАКТ», 2004. – 252 с.

18. Швець М. та ін. Системна інформатизація правоохоронної діяльності / М. Швець С. Антоненко, В. Буржинський, Б. Раціборинський, М. Целуйко, В. Хахановський; за ред. В. Дурдинця, В. Євдокимова, М. Швеця. – [Кн. 1]. – К.: НДЦПІ АПрН України, 2006. – 287 с.

19. Грайворонський М. В., Новіков О. М. Безпека Інформаційно-Комунікаційних Систем. – К.: Видавнича група BHV, 2009. – 608 с.

20. The Schengen acquis - Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders // Official Journal L 239 , 22/09/2000 P. 0013 - 0018 Допоміжна

21. Про державну таємницю: Закон України від 21.01.94 р. № 3855-ХІІ // Відомості Верховної Ради України. – 1994. – № 16. – С. 422. – Ст. 93.

22. Про доступ до публічної інформації : Закон України від 13.01.11 р. № 2939- VI // Відомості Верховної Ради України. – 2011. – № 32. – С. 1491. – Ст. 314. 15

23. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.94 р. №80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. Ст. 286.

24. Про телекомунікації : Закон України від 18.11.03 р. № 1280-IV : за станом на 16.01.12 р. // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

25. Про Національну програму інформатизації : Закон України від 04.02.98 р. № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27 – 28. – Ст.181.

26. Про Національну систему конфіденційного зв`язку : Закон України від 10.01.02 р. № 2919-ІІІ // Відомості Верховної Ради України. – 2002. – № 15. – Ст. 103.

27. Про затвердження Концепції технічного захисту інформації в Україні : Постанова Кабінету Міністрів України від 08.10.97 р. № 1126 : за станом на 16.01.12 р. – Режим доступу : <http://zakon2.rada.gov.ua>

28. Про Стратегію національної безпеки України : Указ Президента України від 12.02.07 р. № 105/2007 // Офіційний вісник України. – 2007. – № 11. – С. 7. – Ст. 389.

29. Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року “Про невідкладні заходи щодо забезпечення інформаційної безпеки України” : Указ Президента України від 23.04.08 р. № 377/2008 // Офіційний вісник Президента України. – 2008. – № 18. – С. 24. – Ст. 570. 30. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В.П. Горбулін, О.Г. Додонов , Д.В. Ланде. – К. : Інтертехнологія, 2009. –164 с. 31. Комп'ютерний тероризм: суперхакери, кібер-терористи, кібер-криміналісти: Монографія / Біленчук П.Д., Гуцалюк М.В., Кравчук О.В., Козир М.В. / За заг. ред. П.Д. Біленчука. - К.: Наука і життя, 2008.

32. Безпека глобальних інформаційних систем та мереж : консп. лекцій /Зубок В.Ю., Корнейко О.В., Ланде Д.В., Мохор В.В. / Під заг. ред. О.В. Корнейка. - К.: Вид-во ІСЗЗІ НТУУ "КПІ", 2010. -162 с. 16

33. Інформаційне насильство та безпека: світоглядно-правові аспекти: Монографія / Дзьобань О.П., Пилипчук В.Г. / За заг. ред. проф. В.Г. Пилипчука. – Харків: Майдан, 2011. – 244 с. 34. Інформаційна безпека людини як споживача телекомунікаційних послуг: Монографія / Арістова І.В., Сулацький Д.В. – К. : Право України, 2012. – 182 с.

35. Правові проблеми протидії новітнім викликам, загрозам і правопорушенням в інформаційній сфері / Савінова Н.А., Стрельбицький М.П. // Правова доктрина України. – 2 том: Публічно-правова доктрина України. – Харків: «Право», 2013. – С. 832 – 861.

36. Проблеми захисту національних інтересів України у сфері державної безпеки в умовах геополітичних трансформацій ХХІ сторіччя : монографія / О.П. Дзьобань, В.Я. Настюк, В.В. Бєлєвцева. – Х.: Право. – 2013. – 296 с.

37. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію : Постанова Кабінету Міністрів України від 27.11.98 р. № 1893 : за станом на 16.01.12 р. // Офіційний вісник України. – 1998. – № 48. – С. 31.

38. Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів : Постанова Кабінету Міністрів України від 17.03.04 р. № 326 : за станом на 16.01.12 р. // Офіційний вісник України. – 2004. – № 11. – С. 45. – Ст. 665.

39. Правові особливості використання документів, переданих за допомогою електронних комунікацій / Баранов О.А. // Правова інформатика. – 2013. – № 1(37). – С. 3-10.

40. Інформаційно-правове регулювання документованої інформації / Коваленко Л.П. // Інформація і право. – 2013. – № 1(7). – С. 58-63.

41. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. – К.: Кондор, 2004. – 384 с. 42. 4. Гавловський В., Гриценко В., Цимбалюк В.С. Організаційно-правові питання формування державної інформаційної політики в Україні. Науковий 17 вісник. Збірник наукових праць Академії державної податкової служби України. № 3 (17). – 2002 - С. 177-182.