МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Кафедра інформаційних технологій та кібербезпеки
навчально-наукового інституту № 1

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Навчальний посібник

Київ
2024

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Кафедра інформаційних технологій та кібербезпеки
навчально-наукового інституту № 1

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Навчальний посібник

Київ
2024

УДК 004:34
С916

Авторський колектив:

Корнейко О. В. – кандидат технічних наук, професор, Національна академія внутрішніх справ;

Кудінов В. А. – кандидат фізико-математичних наук, доцент, Національна академія внутрішніх справ;

Пакриш О. Є. – кандидат технічних наук, доцент, Національна академія внутрішніх справ;

Хахановський В. Г. – доктор юридичних наук, професор, Національна академія внутрішніх справ

Рецензенти:

Звєрєв В. П. – кандидат технічних наук, старший науковий співробітник, Апарат Ради національної безпеки і оборони України;

Кобець М. В. – кандидат юридичних наук, старший науковий співробітник, Національна академія внутрішніх справ

Рекомендовано до друку Вченою радою Національної академії внутрішніх справ 29 грудня 2023 року (протокол № 26)

Матеріали подано в авторській редакції. Відповідальність за їхню якість, а також відсутність у них відомостей, що становлять державну таємницю та службову інформацію, несуть автори

Сучасні інформаційні технології в юридичній діяльності [Текст] : навч. С916 посіб. / [О. В. Корнейко, В. А. Кудінов, О. Є. Пакриш, В. Г. Хахановський]. – Київ : Нац. акад. внутр. справ, 2024. – 205 с.

У навчальному посібнику висвітлено теми, охоплені навчальною дисципліною «Сучасні інформаційні технології в юридичній діяльності», яку викладають для здобувачів ступеня вищої освіти магістра в Національній академії внутрішніх справ.

Видання призначене для науково-педагогічних працівників закладів вищої освіти МВС України, а також може бути корисним для слухачів докторантури й ад'юнктури, наукових і практичних працівників правоохоронних органів.

УДК 004:34

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АБД – адміністратор бази даних
АДІС – автоматизована дактилоскопічна інформаційна система
АРМ – автоматизоване робоче місце
БД – база даних
ВРУ – Верховна Рада України
ГУ – Головне управління
ГІС – геоінформаційна система
ДАІС – документальні автоматизовані інформаційні системи
ДІАП – Департамент інформаційно-аналітичної підтримки
ЄДРСР – Єдиний державний реєстр судових рішень
ЄІС – Єдина інформаційна система
ЄРДР – Єдиний реєстр досудових розслідувань
ЕС – експертна система
ІАС – інформаційно-аналітична система
ІБД – інтегрований банк даних
ІДС – інформаційно-довідкова система
ІІПС – інтегрована інформаційно-пошукова система
ІК – інформаційна картка
ІПНП – інформаційний портал Національної поліції
ІПС – інформаційно-пошукова система
ІС – інформаційна система
ІТ – інформаційні технології
ІКТ – інформаційно-комунікаційні технології
КМУ – Кабінет Міністрів України
КПК – Кримінальний процесуальний кодекс
МВС – Міністерство внутрішніх справ
МСФЗ – міжнародні стандарти фінансової звітності
НАВС – Національна академія внутрішніх справ
НАУ – нормативні акти України
НП – Національна поліція
НПА – нормативно-правові акти
НЦБ – Національне центральне бюро
ОДК – оперативно-довідкова картотека
ОНП – органи Національної поліції
ПД – персональні дані
ПЗ – програмне забезпечення
ПК – персональний комп’ютер
СІАЗ – система інформаційно-аналітичного забезпечення
СППР – система підтримки прийняття рішень
СУБД – система управління базами даних
ФС – файлова система
ЦУНАМІ – Централізоване управління нарядами патрульної служби поліції
ЧЧ – чергова частина

ПЕРЕДМОВА

Навчальний посібник «Сучасні інформаційні технології в юридичній діяльності» висвітлює зміст семи навчальних тем дисципліни «Сучасні інформаційні технології в юридичній діяльності», яка викладається для здобувачів ступеня вищої освіти магістра в Національній академії внутрішніх справ (далі – НАВС), а саме:

1. Загальні засади інформаційного забезпечення юридичної діяльності.
2. Нормативно-правове регулювання інформатизації юридичної діяльності.
3. Інформаційні технології в науково-педагогічній діяльності.
4. Автоматизовані системи документообігу. Інформаційні банки та бази даних.
5. Використання штучного інтелекту в юридичній діяльності.
6. Інформаційні технології статистичного аналізу правових даних.
7. Основи забезпечення кібербезпеки в юридичній діяльності.

Навчальним планом передбачено 90 навчальних годин на опанування зазначеної дисципліни. З них: аудиторна робота з викладачем – 40 н.г. (лекційне заняття – 4 н.г., семінарське заняття – 6 н.г., практичні заняття – 30 н.г.); самостійна робота – 50 н.г. Форма підсумкового контролю – залік.

Зазначимо, що для сучасних фахівців-юристів своєчасне володіння актуальною, достовірною та повною інформацією є надзвичайно важливим елементом їх ефективної діяльності. Тому сучасні інформаційні технології (далі – ІТ) не тільки міцно утвердилися в юриспруденції, але й сприяють появі нових галузей та інститутів права, здійснюють безпосередній вплив на правове життя суспільства. Комп'ютерні технології є незамінним ефективним засобом роботи сучасного юриста та основним способом удосконалення її організації. Сучасна юридична діяльність нерозривно пов'язана з грамотною організацією інформаційних процесів, а також освоєнням і використанням сучасних ІТ. Сьогодні ефективність роботи юриста доволі часто визначає те, наскільки досконало він володіє тією або іншою комп'ютерною технологією. Без зайвого перебільшення можна стверджувати, що персональний комп'ютер (далі – ПК) нині став основним робочим інструментом фахівця-юриста, а знання ним сучасного програмного забезпечення (далі – ПЗ) та інформаційно-комунікаційних технологій (далі – ІКТ), уміле використання їх у практичній діяльності органів Національної поліції України (далі – ОНП) – це запит часу.

Навчальний посібник призначений для здобувачів ступеня вищої освіти магістра НАВС, а також для науково-педагогічних працівників закладів вищої освіти системи Міністерства внутрішніх справ (далі – МВС) України. Він може бути корисним для слухачів докторантури й аспірантури, наукових і практичних працівників органів та підрозділів МВС України, Національної поліції (далі – НП) України.

РОЗДІЛ І
ЗАГАЛЬНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ЮРИДИЧНОЇ ДІЯЛЬНОСТІ

1.1. Мета, завдання та основні поняття навчальної дисципліни «Сучасні інформаційні технології в юридичній діяльності»

Метою викладання навчальної дисципліни «Сучасні інформаційні технології в юридичній діяльності» є підготовка висококваліфікованих та конкурентоспроможних фахівців в галузі знань «Право», які мають відповідні теоретичні знання, практичні уміння та навички застосовувати новітні інноваційні технології в науково-педагогічній та практичній юридичній діяльності, що дозволить впроваджувати ідею, доктрину і принцип верховенства права в правосвідомість людей та практику захисту прав людини.

Основними завданнями вивчення дисципліни «Сучасні інформаційні технології в юридичній діяльності» є: формування у здобувачів вищої освіти системних та глибоких знань про можливості та перспективи новітніх інформаційних технологій, а також відпрацювання умінь і навичок їх використання у наукових дослідженнях, освітньому процесі та юридичній діяльності.

Конкретні завдання навчальної дисципліни:

– поглиблення у здобувачів знань щодо системи інформаційного забезпечення юридичної діяльності МВС, НП, інших державних органів України;

– поглиблення у здобувачів знань, умінь і навичок щодо нормативно-правового регулювання інформатизації юридичної діяльності;

– отримання здобувачами умінь і навичок щодо використання сучасних інформаційних технологій у науково-педагогічній діяльності;

– отримання здобувачами спеціалізованих умінь і навичок щодо роботи з автоматизованими системами документообігу, основними відкритими інформаційно-пошуковими системами (далі – ІПС) та базами даних (далі – БД) системи МВС, НП, інших державних органів України;

– отримання здобувачами знань, умінь і навичок щодо використання штучного інтелекту (далі – ШІ), експертних систем (далі – ЕС) та систем підтримки прийняття рішень (далі – СППР) в юридичній діяльності;

– поглиблення у здобувачів знань, умінь і навичок щодо можливостей сучасних ІТ статистичного опрацювання правових даних;

– поглиблення у здобувачів знань, умінь і навичок щодо безпеки роботи зі службовою та конфіденційною інформацією в юридичній діяльності;

– отримання здобувачами знань, умінь і навичок щодо комплексного використання сучасних інформаційних технологій в юридичній діяльності.

Розглянемо ***основні поняття,*** які необхідно згадати перед вивченням дисципліни «Сучасні інформаційні технології в юридичній діяльності».

Формування загальновідомчих та галузевих інформаційних підсистем, які складають основу системи інформаційного забезпечення юридичної діяльності, здійснюється згідно з такими ***принципами*** [71]:

1) функціонального призначення (інформаційні підсистеми оперативно-розшукового, оперативно-довідкового, організаційно-управлінського призначення, кримінальної статистики, спеціалізовані);

2) нормативно-правової забезпеченості;

3) фактичності даних;

4) доцільності впровадження та експлуатації;

5) нарощення та розвитку.

Формування інформаційних підсистем системи інформаційного забезпечення юридичної діяльності покладено на ***інформаційні служби***:

1. У МВС України – *Департамент інформатизації*.

2. У Національній поліції України – *Департамент інформаційно-аналітичної підтримки*.

Інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (ст. 1 Закону України «Про інформацію») [2].

Документ – це матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі (ст. 1 Закону України «Про інформацію») [2].

Інформаційно-комунікаційні технології – це результат інтелектуальної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік та послідовність виконання операцій для збирання, обробки, накопичення та використання інформаційної продукції, надання інформаційних послуг (ст. 1 Закону України «Про Національну програму інформатизації») [23].

Основні види інформаційної діяльності – це створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації (ст. 9 Закону України «Про інформацію») [2].

Види інформації за змістом (ст. 10 Закону України «Про інформацію»):

1) інформація про фізичну особу (ст. 11);

2) інформація довідково-енциклопедичного характеру (ст. 12);

3) інформація про стан довкілля (екологічна інформація) (ст. 13);

4) інформація про товар (роботу, послугу) (ст. 14);

5) науково-технічна інформація (ст. 15);

6) податкова інформація (ст. 16);

7) правова інформація (ст. 17);

8) статистична інформація (ст. 18);

9) соціологічна інформація (ст. 19);

10) критична технологічна інформація (ст. 19^1);

11) інші види інформації [2].

За порядком доступу інформація поділяється на: 1) відкриту інформацію; 2) інформацію з обмеженим доступом (ст. 20 Закону України «Про інформацію») [2].

Інформація з обмеженим доступом поділяється на: 1) конфіденційну; 2) таємну; 3) службову (ст. 21 Закону України «Про інформацію») [2].

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень (ст. 21 Закону України «Про інформацію») [2].

Ступінь секретності («особливої важливості», «цілком таємно», «таємно») – це категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою (ст. 1 Закону України «Про державну таємницю») [8].

Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, не може перевищувати для інформації із ступенем секретності «особливої важливості» – 30 років, для інформації «цілком таємно» – 10 років, для інформації «таємно» – 5 років (ст. 13 Закону України «Про державну таємницю») [8].

Захист інформації – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї (ст. 1 Закону України «Про інформацію») [2].

Технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації (ст. 1 Закону України «Про державну таємницю») [6].

Властивості інформації: 1) достовірність; 2) своєчасність; 3) повнота; 4) зрозумілість; 5) об'єктивність; 6) актуальність; 7) корисність; 8) об'ємність; 9) конфіденційність; 10) цілісність; 11) доступність; 12) захищеність та ін. [72].

ФОРМАТИ ДАТИ

1. Короткий (цифровий) формат:

(якщо день, місяць – одинарні числа, то добавляємо «0»)

19.11.2023 *Україна, Німеччина, Норвегія, Сербія, Франція, Швейцарія*

19/11/2023 *Англія, Бельгія, Італія, Іспанія, Бразилія, Латинська Америка*

19-11-2023 *Данія, Нідерланди, Португалія*

2023-11-19 *Угорщина, Польща, Словаччина, Словенія, Чехія, Швеція*

11-19-2023 *США*

2. Середній формат: 19-лис-2023 *(бази даних)*

3. Довгий словесно-цифровий формат: 19 листопада 2023 р.

(наприклад: нормативно-правові та фінансові документи)

4. Довгий словесний формат:

Дев'ятнадцяте листопада дві тисячі сімнадцятого року *(договір, заповіт)*

5. Повний формат: 19.11.2023 08:15:20

(наприклад: фіскальний чек, відеореєстратор, журнал дзвінків, sms, створення файлу, протокол слідчої дії)

1.2. Основні інформаційні підсистеми системи інформаційного забезпечення юридичної діяльності

1.2.1. Формування та використання поліцією інформаційних ресурсів відповідно до норм Закону України «Про Національну поліцію»

Відповідно до ст. 19 Конституції України «органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України» [1]. Відповідно до ст. 32 Конституції України «не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини».

Повноваження поліції у сфері інформаційно-аналітичного забезпечення передбачені ст. 25 Закону України «Про Національну поліцію» [3].

***Поліція в рамках інформаційно-аналітичної діяльності*:**

1) формує бази (банки) даних, що входять до Єдиної інформаційної системи (далі – ЄІС) Міністерства внутрішніх справ України;

2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади;

3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;

4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями.

Поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень.

Формування інформаційних ресурсів поліцією передбачено ст. 26 Закону України «Про Національну поліцію» [3].

Поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до Єдиної інформаційної системи Міністерства внутрішніх справ України, ***стосовно***:

1) осіб, щодо яких поліцейські здійснюють профілактичну роботу;

2) виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили, руху кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких направлено до суду;

3) розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду;

4) розшуку безвісно зниклих;

5) установлення особи невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком;

6) зареєстрованих в органах внутрішніх справ кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій;

7) осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученнями органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт);

8) осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією;

9) зареєстрованих кримінальних та адміністративних корупційних правопорушень, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах;

10) іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні;

11) викрадених номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних із учиненням правопорушень, відповідно до заяв громадян;

12) викрадених (втрачених) документів за зверненням громадян;

13) знайдених, вилучених предметів і речей, у тому числі заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери;

14) викрадених транспортних засобів, які розшукуються у зв'язку з безвісним зникненням особи, виявлених безгосподарних транспортних засобів, а також викрадених, втрачених номерних знаків;

15) виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів на рух окремих категорій транспортних засобів;

16) зброї, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї;

17) викраденої, втраченої, вилученої, знайденої зброї, а також добровільно зданої зброї із числа тієї, що незаконно зберігалася;

18) бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону.

Під час наповнення баз (банків) даних, визначених у п 7 ч. 1 ст. 26 Закону поліція забезпечує збирання, накопичення мультимедійної інформації (фото, відео-, звукозапис) та біометричних даних (дактилокартки, зразки ДНК).

Використання поліцією інформаційних ресурсів передбачено ст. 27 Закону України «Про Національну поліцію» [3]. Поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних» [17]. Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано.

Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів, передбачених статтями 26, 27 цього Закону [3], фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій Міністерства внутрішніх справ України.

1.2.2. Класифікація основних видів обліків Міністерства внутрішніх справ України та Національної поліції

Основні види обліків Міністерства внутрішніх справ України та Національної поліції можна умовно *класифікувати* на:

1) оперативного призначення;
2) експертно-криміналістичного призначення;
3) статистичного та аналітичного призначення;
4) адміністративного (управлінського) та загального призначення.

Інформація ***оперативних обліків*** умовно поділяється на:

– облік осіб і їх характеристик;
– облік подій;
– облік предметів та речей.

Приклади оперативних обліків: «Інтегрована інформаційно-пошукова система (далі – ІІПС) МВС України», «Оріон», «Скорпіон», «Наркобізнес», «Оперативно-довідкова картотека», «Граніт», «Кримінальна статистика» тощо.

Інформація ***експертно-криміналістичних обліків*** поділяється на:

1. Оперативно-пошукові обліки.
2. Інформаційно-довідкові обліки.

Приклади оперативно-пошукових обліків: 1) дактилоскопічні обліки; 2) колекції слідів злому; 3) слідів взуття; 4) слідів транспортних засобів; 5) волокон; 6) замків і ключів; 7) фальшивих грошей; 8) підроблених рецептів і бланків документів; 9) кулегільзотеки; 10) колекції суб'єктивних портретів; 11) колекція фонограм з голосами осіб, які анонімно повідомляли про загрозу вибуху тощо.

Приклади *інформаційно-довідкових обліків*. Колекції зразків: 1) документів суворого обліку, цінних паперів та грошей; 2) зброї та боєприпасів; 3) наркотичних засобів, психотропних речовин, їх аналогів і прекурсорів; 4) рельєфних підошов взуття; 5) інструментів, що використовуються при зломах; 6) лакофарбових покриттів; 7) вибухових пристроїв і речовин; 8) протекторів шин; 9) волокон і волосся; 10) паливно-мастильних матеріалів; 11) підроблених номерів вузлів, деталей та агрегатів автотранспорту тощо.

Сьогодні професійна діяльність юриста пов'язана з опрацюванням значних обсягів правових відомостей з різних галузей права. Їх обсяг настільки великий, що для оперативного доступу до них, їх систематизації, своєчасного і коректного використання юристами все більш актуальним стає застосування спеціалізованих програмно-технічних засобів – правових інформаційно-пошукових систем [70; 74; 75].

1.2.3. Правові інформаційно-пошукові системи

Найбільш відомими на українському ринку правовими ІПС є: «Законодавство України» (безкоштовна) (рис. 1.1, 1.2), «Єдиний державний реєстр нормативно-правових актів» (безкоштовна) (рис. 1.3), «Ліга: Закон» (платна) (рис. 1.4), «Нормативні акти України» (платна) (рис. 1.5) [75].

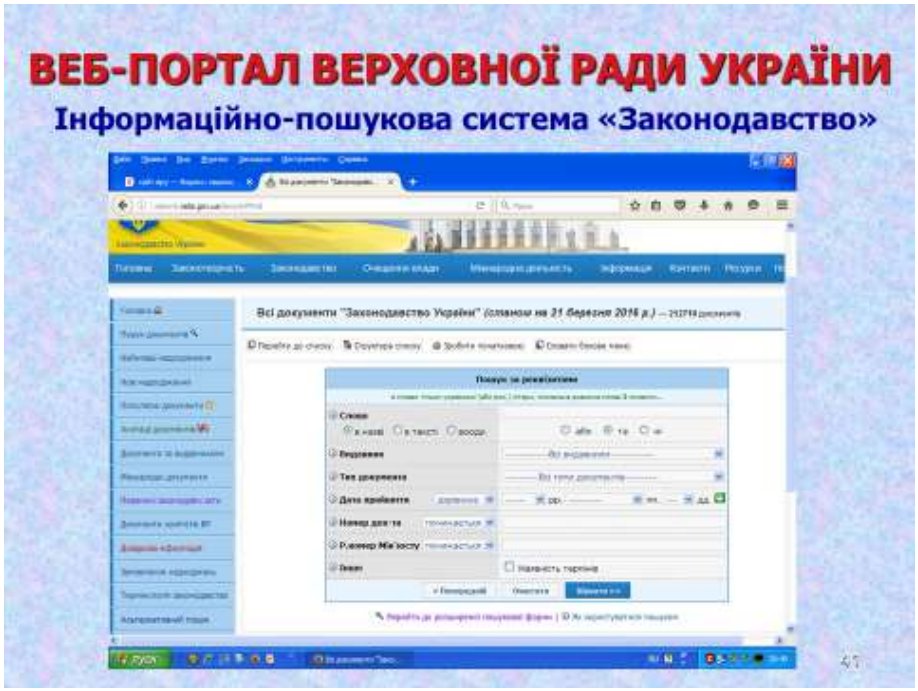


Рис. 1.1. Вебсторінка «Пошук за реквізитами» офіційного вебпорталу ІПС «Законодавство України» [77] (http://zakon3.rada.gov.ua/laws/a#Find)

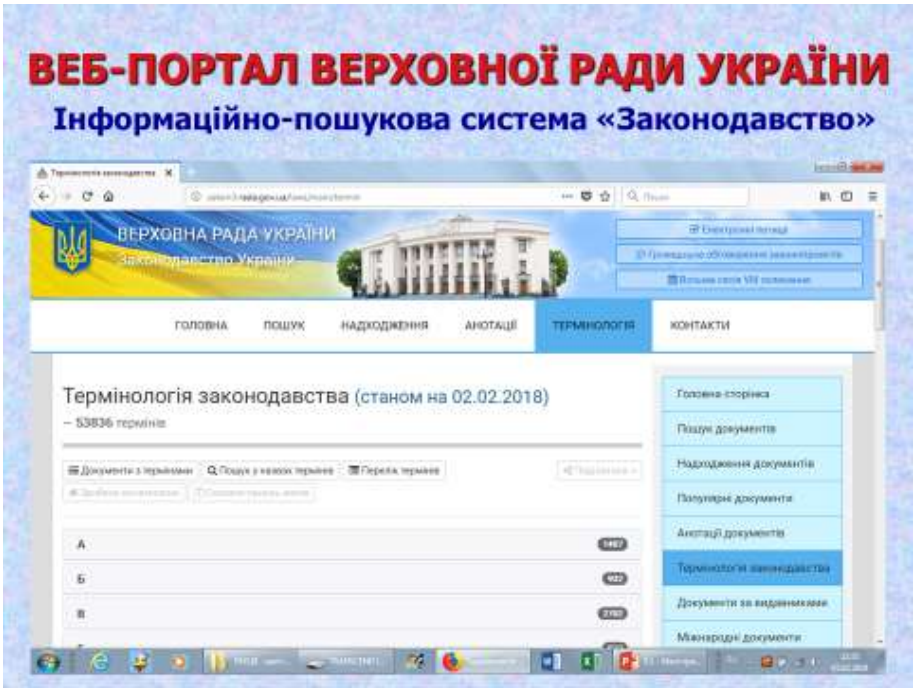


Рис. 1.2. Вебсторінка «Термінологія законодавства» офіційного вебпорталу ІПС «Законодавство України» (http://zakon3.rada.gov.ua/laws/main/termin)

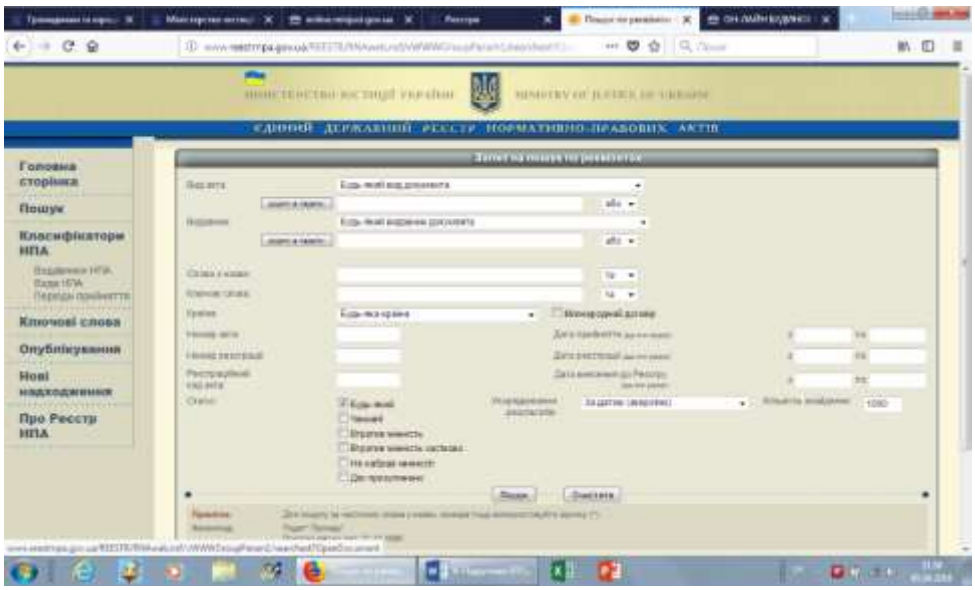


Рис. 1.3. Вебсторінка «Єдиний державний реєстр нормативно-правових актів» вебпорталу Міністерства юстиції України (http://www.reestrnpa.gov.ua/REESTR/RNAweb.nsf/vWWWGroupParam1/searchext?OpenDocument)

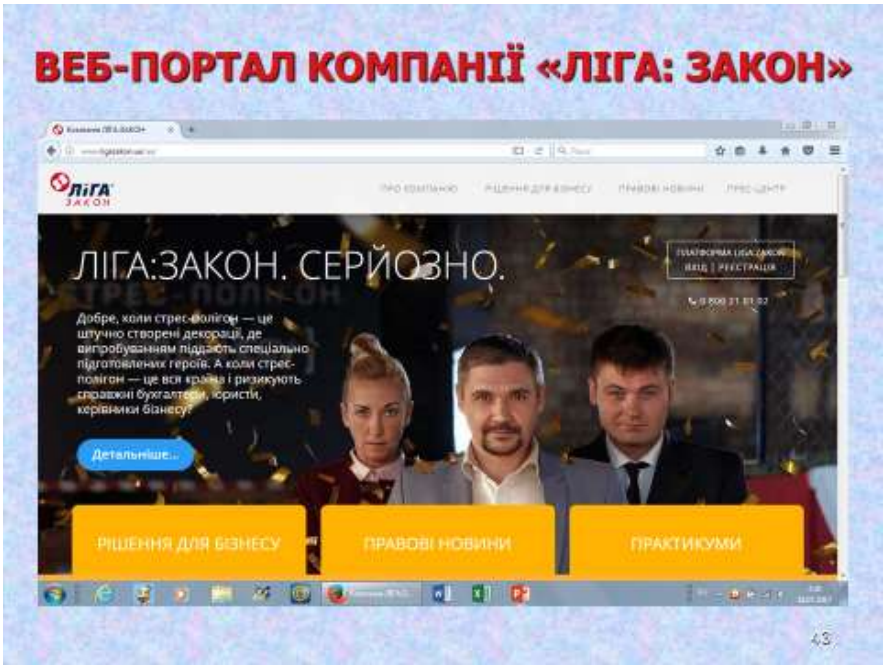


Рис. 1.4. Головна вебсторінка офіційного вебпорталу компанії «Ліга: Закон» (http://www.ligazakon.ua/ua/)

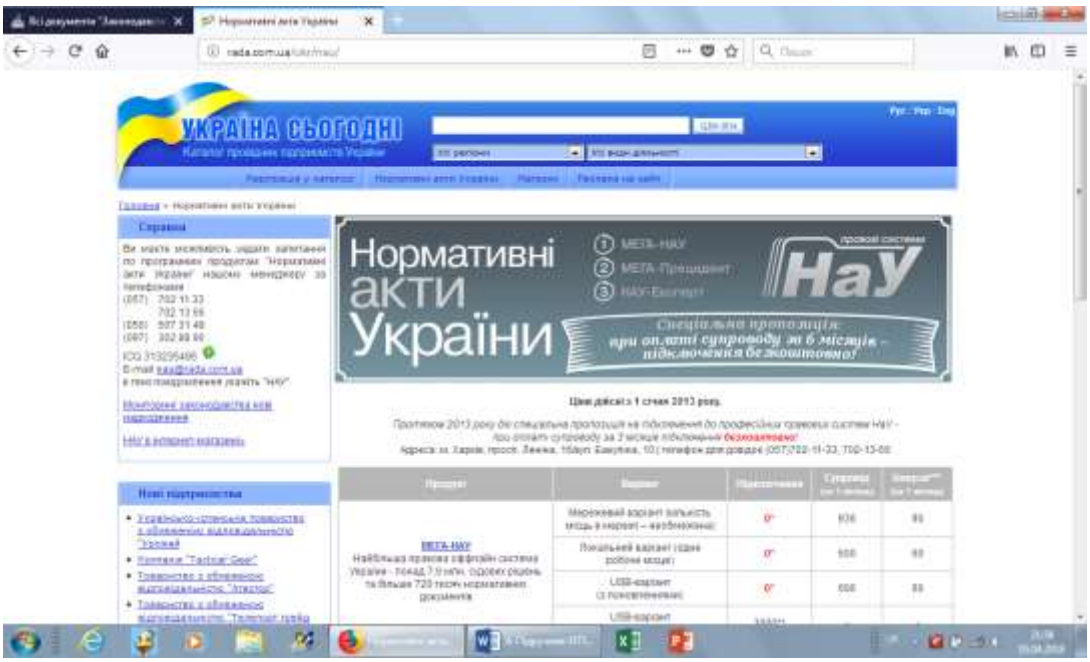


Рис. 1.5. Головна вебсторінка офіційного вебпорталу інформаційно-пошукової системи «Нормативні акти України» (http://rada.com.ua/ukr/nau/)

1.2.4. Реєстри вебпорталу Міністерства юстиції України

У правозастосовній діяльності можна також використовувати можливості низки реєстрів вебпорталу Міністерства юстиції України (рис. 1.6, 1.7).

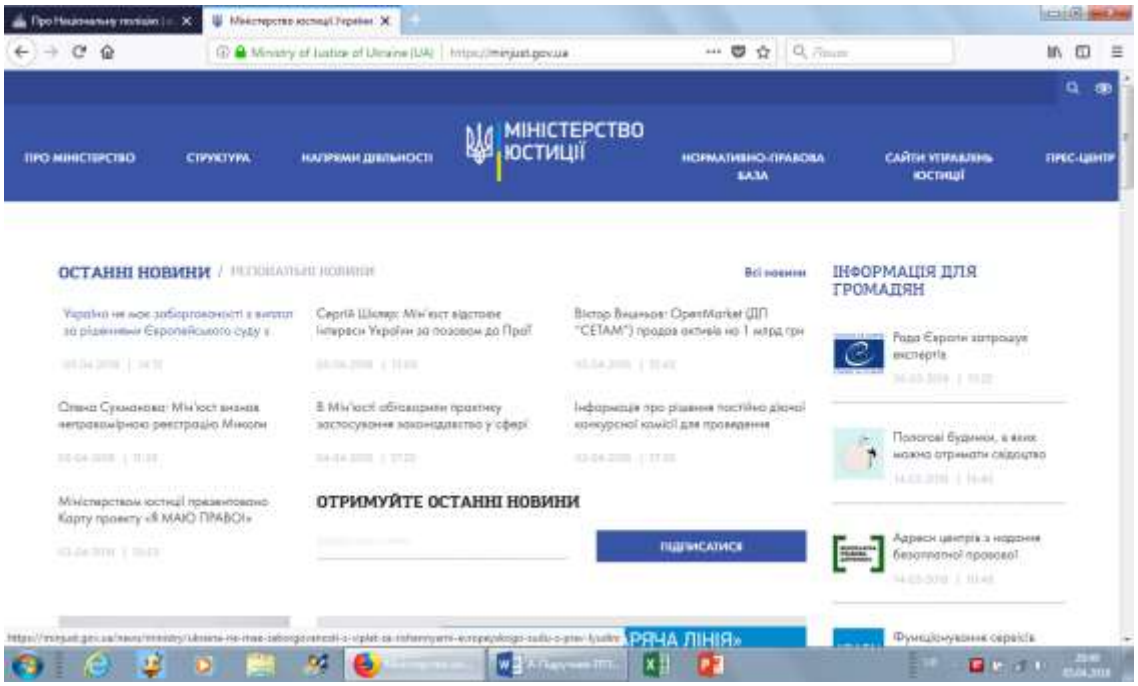


Рис. 1.6. Вебпортал Міністерства юстиції України (https://minjust.gov.ua/)

Міністерство юстиції України забезпечує формування та реалізацію державної правової політики, державної політики з питань банкрутства та використання електронного цифрового підпису, формування та реалізації державної політики у сфері безоплатної правової допомоги, організації примусового виконання рішень судів та інших органів (посадових осіб), пенітенціарної системи та служби пробації, державної реєстрації актів цивільного стану, державної реєстрації речових прав на нерухоме майно та їх обтяжень, державної реєстрації юридичних осіб, громадських формувань, що не мають статусу юридичної особи, та фізичних осіб-підприємців, реєстрації статуту територіальної громади м. Києва, державної реєстрації друкованих засобів масової інформації та інформаційних агентств як суб'єктів інформаційної діяльності і т. ін.

Мін'юст розробляє і реалізує політику в цілях забезпечення прозорого, швидкого та ефективного надання послуг кожній особі, забезпечуючи легкість ведення бізнесу та підвищуючи ступінь суспільної довіри і впевненості.

«Вебпортал Міністерства юстиції України» → *«Відкриті дані»* → ***«Інформація з Реєстрів у форматі відкритих даних»*** (https://minjust.gov.ua/information-from-register):

1. Реєстр громадських об'єднань.
2. Реєстр громадських формувань.
3. Єдиний реєстр нотаріусів.
4. Державний реєстр атестованих судових експертів.
5. Державний реєстр друкованих засобів масової інформації та інформаційних агентств як суб'єктів інформаційної діяльності.
6. Реєстр методик проведення судових експертиз.
7. Єдиний державний реєстр осіб, які вчинили корупційні правопорушення.
8. Єдиний реєстр підприємств, щодо яких порушено впровадження у справі про банкрутство.
9. Єдиний реєстр арбітражних керуючих (розпорядників майна, керуючих санацією, ліквідаторів) України.
10. Єдиний державний реєстр нормативно-правових актів.
11. Реєстр суб'єктів, які надають послуги, пов'язані з електронним цифровим підписом.
12. Електронний реєстр чинних, блокованих та скасованих посилених сертифікатів відкритих ключів засвідчувальних центрів та центрів сертифікації ключів.
13. Реєстр адміністративно-територіального устрою.
14. Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань.
15. Єдиний реєстр спеціальних бланків нотаріальних документів.
16. Єдиний державний реєстр осіб, щодо яких застосовано положення Закону України «Про очищення влади».

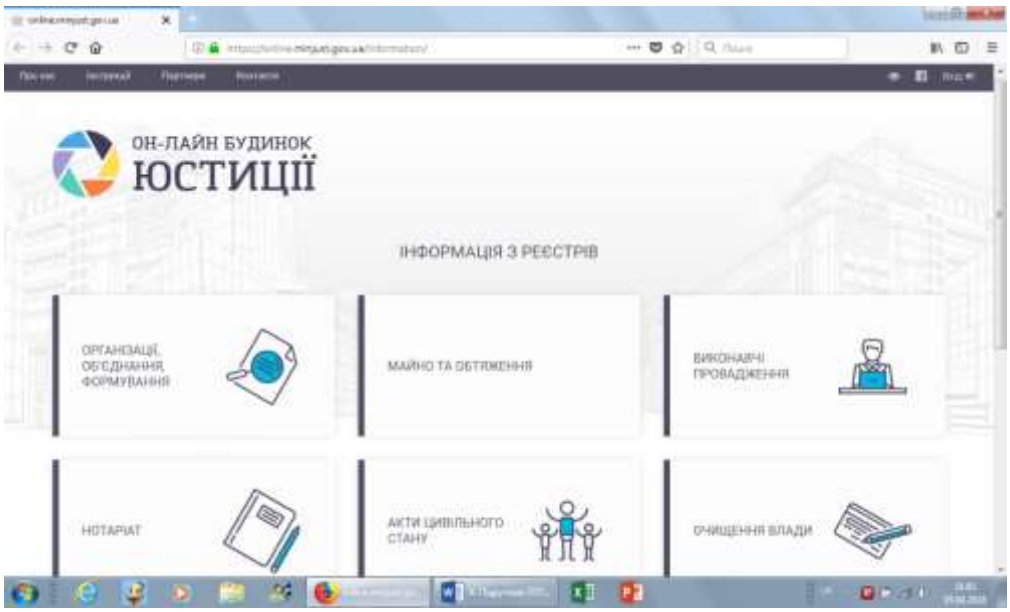


Рис. 1.7. Онлайн будинок юстиції

Вебпортал Міністерства юстиції України → «Онлайн сервіси» → ***«Інформація з реєстрів»*** (https://online.minjust.gov.ua/information/):

1. Організації, об'єднання, формування

– Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань

– Державний реєстр друкованих засобів масової інформації та інформаційних агентств

– Єдиний реєстр громадських формувань

– Реєстр громадських об'єднань

2. Майно та обтяження

– Державний реєстр речових прав на нерухоме майно

– Державний реєстр обтяжень рухомого майна

3. Виконавчі провадження

– Доступ для громадян та сторін виконавчого провадження

– Доступ для співробітників органів ДВС та приватних виконавців

– Єдиний реєстр боржників

4. Нотаріат

– Єдиний реєстр нотаріусів

– Єдиний реєстр спеціальних бланків нотаріальних документів

– Електронний реєстр апостилів

5. Акти цивільного стану

– Вебпортал звернень громадян

– Доступ для уповноважених осіб

6. Очищення влади

– Єдиний державний реєстр осіб, щодо яких застосовано положення Закону України «Про очищення влади»

7. Банкрутство

- Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство
- Єдиний реєстр арбітражних керуючих
- Система електронної звітності арбітражних керуючих

1.2.5. Єдиний державний реєстр судових рішень

Єдиний державний реєстр судових рішень (далі – ЄДРСР) – це автоматизована система збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень (рис. 1.8).

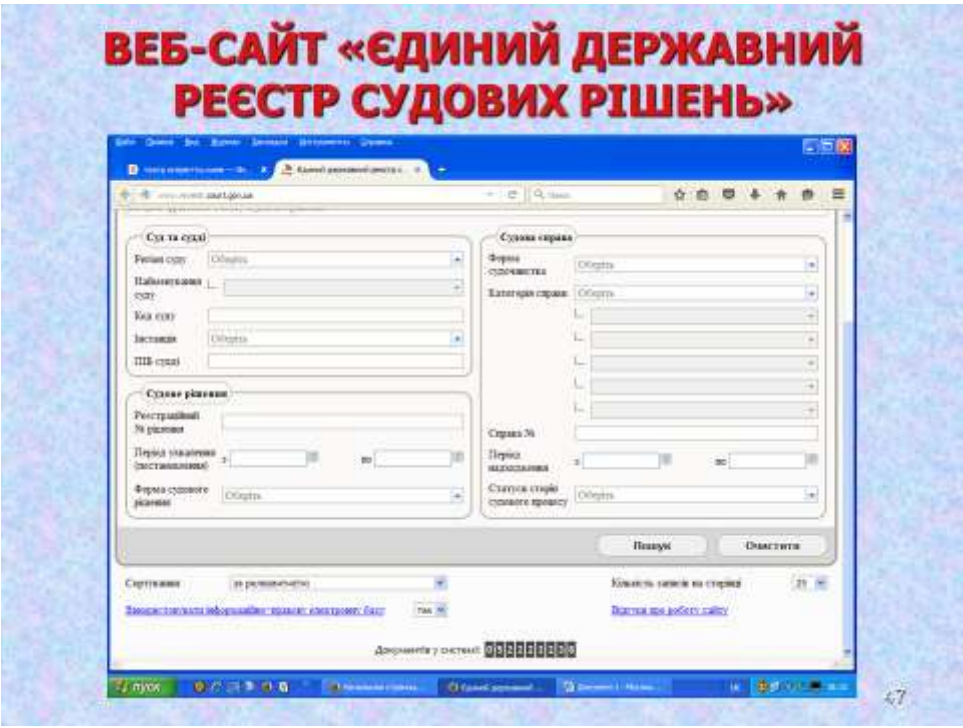


Рис. 1.8. Головна вебсторінка вебсайту «Єдиний державний реєстр судових рішень» (http://www.reyestr.court.gov.ua)

До ЄДРСР вносяться судові рішення Верховного Суду України, вищих спеціалізованих, апеляційних та місцевих судів – вироки, рішення, постанови, накази, ухвали, окремі ухвали (постанови) суду, що ухвалені (постановлені) судами у кримінальних, цивільних, господарських справах, у справах адміністративної юрисдикції, у справах про адміністративні правопорушення, крім судових рішень, які містять інформацію, що є державною таємницею.

Судові рішення, внесені до ЄДРСР, є *відкритими для безоплатного цілодобового доступу* на офіційному вебпорталі судової влади України відповідно до Закону України «Про доступ до судових рішень» від 22.12.2005 № 3262-IV [11].

База даних ЄДРСР містить інформацію *довідкового характеру*, яка станом на 23.02.2023 містить 115 059 512 документів.

1.2.6. Розшукові обліки на вебпорталі МВС України

На вебпорталі МВС України розміщено ***«Розшукові обліки»*** [79] (рис. 1.9, 1.10), які містять 11 типів пошукових запитів до баз даних. Даний пошуковий ресурс є обмеженою копією офіційних баз даних МВС України і періодично оновлюється.

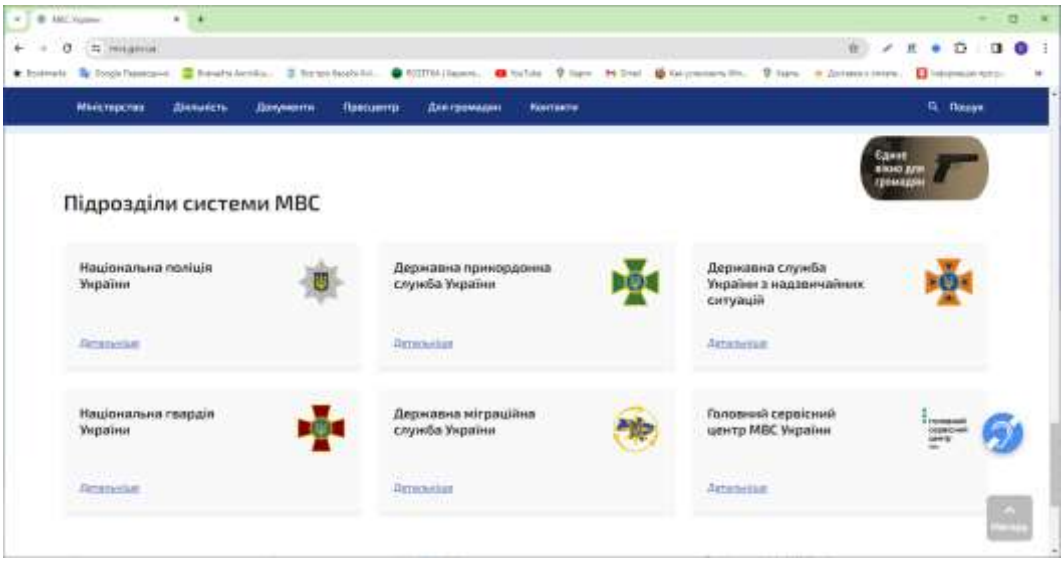


Рис. 1.9. Вебпортал Міністерства внутрішніх справ України (http://mvs.gov.ua/)

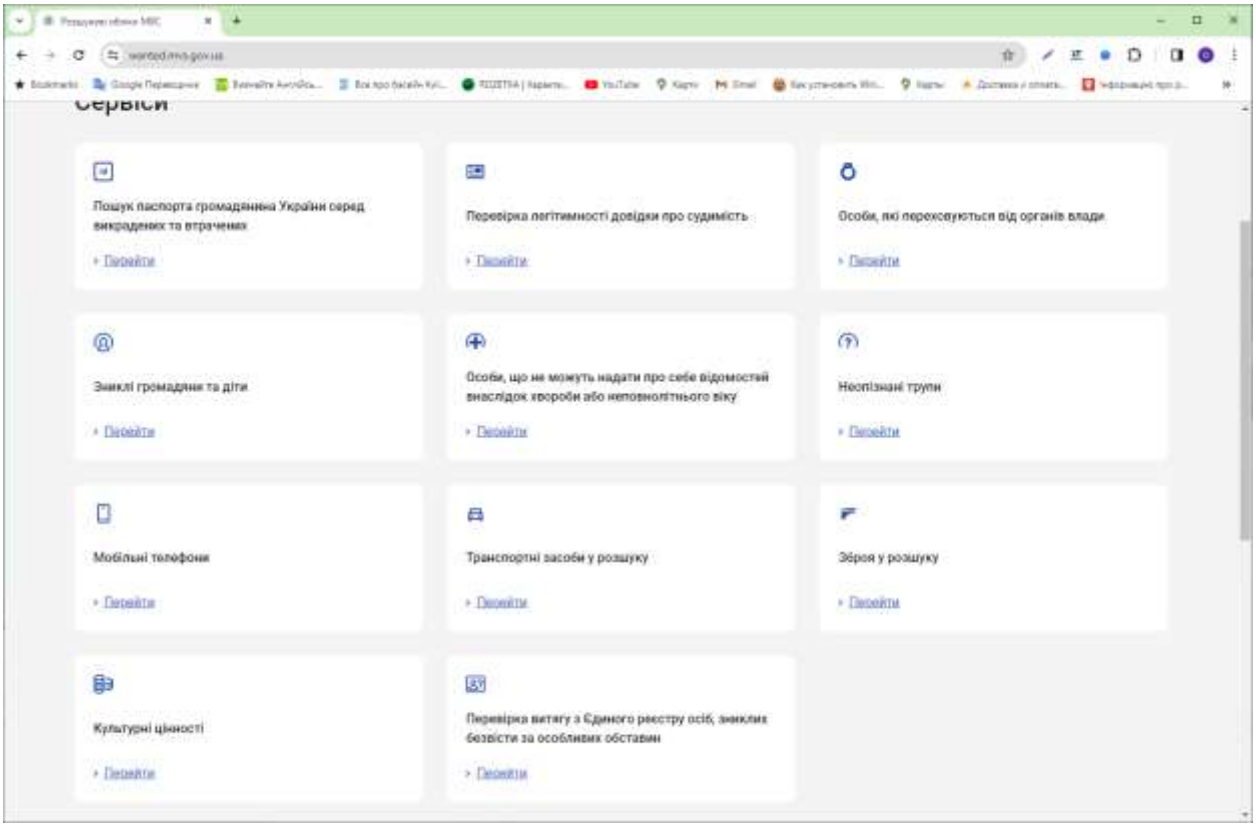


Рис. 1.10. Розшукові обліки на вебпорталі МВС України (https://wanted.mvs.gov.ua/)

Даний вебресурс призначений для надання допомоги органам та підрозділам Національної поліції:

1) зі встановлення місцезнаходження безвісті зниклих людей (*БД «Зниклі громадяни»*);

2) зі встановлення невпізнаних трупів (*БД «Невпізнані трупи»*);

3) з пошуку викрадених культурних цінностей (*БД «Культурні цінності»*);

4) з пошуку викрадених мобільних телефонів (*БД «Мобільні телефони»*);

5) з пошуку зброї, яка знаходиться у розшуку (*БД «Зброя у розшуку»*);

6) з пошуку транспортних засобів, які знаходяться у розшуку (*БД «Транспортні засоби у розшуку»*);

7) з розшуку тих осіб, хто переховується від органів влади (*БД «Особи, які переховуються від органів влади»*);

8) зі встановлення осіб, які втратили пам'ять (*БД «Особи, що не можуть надати про себе відомостей внаслідок хвороби або неповнолітнього віку»*);

9) зі встановлення легітимності довідки про судимість (*БД «Перевірка легітимності довідки про судимість»*);

10) з пошуку паспортів громадян України, які викрадені або втрачені (*БД «Пошук паспорта громадянина України серед викрадених та втрачених»*);

11) з перевірки витягу з Єдиного реєстру осіб, зниклих безвісти за особливих обставин (*БД «Перевірка витягу з Єдиного реєстру осіб, зниклих безвісти за особливих обставин»*).

На сайті також представлено детальну інформацію, куди громадянин може звернутися за телефоном «гарячої лінії» МВС України 15-36, або зателефонувавши 102. МВС та Національна поліція висловлюють вдячність за будь-яку допомогу.

1.2.7. Інформаційно-аналітична система «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості»

Відповідно до законодавста в Міністерстві внутрішніх справ у складі єдиної інформаційної системи МВС функціонує інформаційно-аналітична система «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості» [47].

Інформаційно-аналітична система «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості» (далі – ІАС) – це структурована автоматизована база даних, яка використовується для збирання, зберігання, обліку, пошуку, узагальнення, захисту, перевірки достовірності відомостей, перетворення та відображення інформації, забезпечення доступу до даних про притягнення особи до кримінальної відповідальності, відсутність (наявність) судимості або обмежень, передбачених кримінальним процесуальним законодавством України.

Джерелами автоматичного наповнення ІАС є такі інформаційні системи:

– Єдиний реєстр досудових розслідувань щодо осіб, яким повідомлено про підозру; осіб, щодо яких обрано запобіжний захід; наслідків досудового розслідування кримінальних правопорушень;

– Єдиний державний реєстр судових рішень щодо наслідків судового розгляду кримінальних проваджень;

– Єдиний реєстр засуджених та осіб, узятих під варту, щодо засуджених, ув'язнених та суб'єктів пробації;

– оцифровані архівні інформаційні масиви персонально-довідкового обліку МВС.

Об'єктами обліку ІАС (далі – об'єкти обліку) є:

– фізичні особи, які відповідно до Кримінального процесуального кодексу України набули статусу підозрюваного, обвинуваченого (підсудного), засудженого;

– фізичні особи, щодо яких застосовано примусові заходи медичного чи виховного характеру;

– фізичні особи, яких звільнено від кримінальної відповідальності згідно із статтями 44-49, 97 Кримінального кодексу України;

– фізичні особи, яких оголошено в розшук;

– громадяни України, яких засуджено судами інших держав;

– архівна інформація репресивних органів.

В ІАС обробляються такі **відомості про об'єкти обліку**:

– установчі дані: прізвище, власне ім'я, по батькові (за наявності), дата та місце народження;

– громадянство, стать, адреса задекларованого/зареєстрованого місця проживання (перебування), реквізити документів, що посвідчують особу, підтверджують громадянство України або спеціальний статус особи, унікальний номер запису в Єдиному державному демографічному реєстрі, реєстраційний номер облікової картки платника податку, дактилоскопічна формула (за наявності);

– повідомлення особі про підозру (пред'явлення обвинувачення);

– застосування щодо особи запобіжних заходів;

– оголошення особи у розшук;

– наслідки досудового розслідування кримінальних правопорушень (закриття кримінального провадження; звернення до суду з обвинувальним актом; з клопотанням про звільнення особи від кримінальної відповідальності; з клопотанням про застосування примусових заходів медичного або виховного характеру);

– судове рішення: дата, найменування суду, статті Кримінального кодексу України, вид та строк покарання, дата набрання законної сили;

– виконання покарання;

– здійснення Президентом України помилування щодо засудженого;

– застосування заходів пробації;

– засудження громадян України на території іноземних держав;

– зняття/погашення судимості.

Фізичні особи можуть отримати витяг про несудимість з ІАС, використавши застосунок «Дія» або подати запит в електронній формі та отримати довідку у

формі витягу через електронний сервіс https://vytiah.mvs.gov.ua, увійшовши до Особистого кабінету за допомогою кваліфікованого електронного підпису.

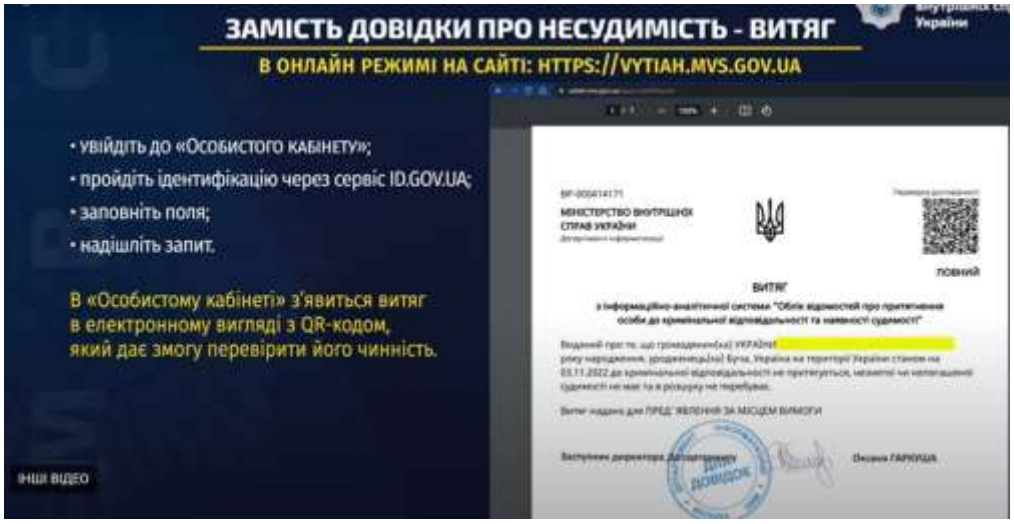


Рис. 1.11. Інформаційне повідомлення щодо порядку отримання витягу з ІАС

1.2.8. Банки даних Генерального секретаріату Інтерполу

Департамент міжнародного поліцейського співробітництва є структурним підрозділом апарату центрального органу управління поліції, який забезпечує планування, організацію, взаємодію та координацію дій структурних підрозділів апарату Національної поліції України, територіальних та міжрегіональних територіальних органів поліції (далі – органи та підрозділи поліції) та інших органів державної влади України щодо здійснення міжнародного співробітництва з компетентними органами іноземних держав та міжнародними організаціями з питань, що належать до компетенції поліції, Інтерполу та Європолу, а також реалізацію повноважень щодо здійснення представництва та забезпечення виконання зобов'язань України в Міжнародній організації кримінальної поліції – Інтерполі (далі – Інтерпол) та Європейському поліцейському офісі (Європолі) (далі – Європол), повноважень Національної поліції України як Національного центрального бюро Інтерполу (далі – НЦБ Інтерполу) та Національного контактного пункту Європолу в Україні (далі – НКП Європолу).

Департамент міжнародного поліцейського співробітництва відповідно до покладених на нього *завдань*:

– здійснює обмін інформацією з Генеральним секретаріатом Інтерполу, Європолом, правоохоронними органами та іншими органами державної влади України, а також з компетентними органами іноземних держав з питань протидії злочинності;

– організовує впровадження в діяльність Національної поліції України та інших органів державної влади України новітніх комунікаційних,

комп'ютерних та інших технологій, які розробляються та використовуються Інтерполом та Європолом;

– отримує в установленому порядку доступ до інформаційних систем та БД органів державної влади України, використовує їх у своїй діяльності;

– використовує інформаційні системи та банки даних Генерального секретаріату Інтерполу, Європолу, організовує та забезпечує надання в установленому порядку доступу до них уповноваженим органам державної влади України;

– забезпечує обмін інформацією у цілодобовому режимі;

– формує облікиористувачів, яким надано в установленому порядку доступ до банків даних Інтерполу, здійснює контроль за належним використанням такого доступу.

– забезпечує наповнення в установленому порядку банків даних Інтерполу та Європолу інформацією, наданою уповноваженим органами державної влади України;

– створює і використовує відповідно до законодавства України власні автоматизовані інформаційні системи;

– складає на підставі інформації правоохоронних органів та інших органів державної влади України звіти, інформаційно-аналітичні матеріали з питань протидії злочинності, надсилає їх до компетентних органів іноземних держав, Інтерполу та Європолу тощо.

Розглянемо банки даних Генерального секретаріату Інтерполу (https://www.interpol.int/How-we-work/Databases).

Відповідно до ст. 26 Статуту Інтерполу серед завдань Генерального секретаріату Інтерполу зазначається, що він:

1) виступає в якості міжнародного центру по боротьбі зі злочинністю;

2) діє як спеціалізований та інформаційний центр.

У зв'язку з цим, однією з ключових функцій Генерального секретаріату Інтерполу *є створення та забезпечення функціонування міжнародних банків даних інформації криміналістичного та розшукового характеру*.

Характерними особливостями цих банків даних є те, що інформація, яка в них міститься:

– вноситься до банків даних всіма країнами-членами Інтерполу (у даний час в Інтерполі 190 країн-членів);

– є доступною для правоохоронних органів всіх країн-членів Організації.

Указане дає підстави розглядати банки даних Інтерполу як *глобальний інструмент з протидії злочинност*і, зокрема, для попередження, розкриття та розслідування злочинів, розшуку осіб (підозрюваних, обвинувачених, підсудних, засуджених, безвісно відсутніх), автотранспорту, речей та предметів, ідентифікації осіб (які не можуть повідомити про себе ніяких відомостей, у т.ч. хворих та дітей, невпізнаних трупів) тощо.

Власником кожної одиниці/об'єкту інформації, що міститься в банках даних Інтерполу, є певна країна-член Організації, тобто відповідне національне центральне бюро (далі – НЦБ), що є ініціатором внесення інформації про об'єкт

до цього банку даних, або здійснювало обмін інформацією щодо відповідного об'єкту з іншими країнами (національними центральними бюро).

Інформаційне забезпечення Інтерполу станом на сьогодні містить велику кількість банків (баз) даних, а саме:

1. Банк «Повідомлення» – це міжнародні сповіщення про втікачів, підозрюваних у злочинах, осіб та організації, які підпадають під санкції Ради Безпеки ООН, потенційні загрози, зниклих безвісти осіб, трупи та злочинні методи. Деталі зберігаються в базі даних, відомій як Система кримінальної інформації INTERPOL.

2. Банк «Фізичні особи» місить бази:

– особисті дані та кримінальна історія людей, щодо яких подається запит на міжнародне поліцейське співробітництво;

– жорстоке поводження з дітьми та жертви. Зображення сексуальної експлуатації дітей використовує складне програмне забезпечення для порівняння зображень, щоб встановити зв'язки між жертвами, кривдниками та місцями. Метою є виявлення, місцезнаходження та затримання зловмисників, а також визволення постраждалих.

3. Банк «Криміналістика» містить відбитки пальців, профілювання ДНК і розпізнавання облич можуть відігравати вирішальну роль у розкритті злочинів, оскільки вони можуть виявити зв'язки між особами та/або місцем злочину. Не менш важливо, вони можуть допомогти довести невинуватість підозрюваного.

База «Відбитки пальців» – авторизовані користувачі в країнах-членах можуть переглядати, надсилати та перевіряти записи в базі даних відбитків пальців за допомогою зручної автоматичної системи ідентифікації відбитків пальців (AFIS).

База «ДНК» – містить профілі ДНК правопорушників, місць злочинів, зниклих безвісти та невпізнаних тіл. Ми не зберігаємо жодних номінальних даних, які пов'язують профіль ДНК з будь-якою особою.

База «Я – сім'я». Метою бази «I-Familia» є ідентифікація зниклих безвісти в усьому світі за допомогою зіставлення родинної ДНК. I-Familia допомагає возз'єднати близьких або закрити справи та дозволити сім'ям налагодити своє життя заново.

База «Розпізнавання обличчя» надає спеціальну платформу для зберігання та перехресної перевірки зображень з метою ідентифікації втікачів, зниклих безвісти та зацікавлених осіб.

4. Банк «Проїзні та офіційні документи». Прикордонні пункти є критично важливими для збереження національної безпеки. Бази даних допомагають виявляти та запобігати шахрайському використанню проїзних та адміністративних документів, тим самим обмежуючи пересування злочинців або незаконних предметів.

База «SLTD (проїзні та ідентифікаційні документи)» - містить інформацію про проїзні документи та документи, що посвідчують особу, про які було

повідомлено як про викрадені, втрачені, анульовані, недійсні або викрадені бланки

База «Викрадені адміністративні документи (SAD)» - містить записи про викрадені офіційні документи, які служать для ідентифікації об'єктів, наприклад, реєстраційні документи на транспортні засоби та сертифікати митного оформлення для імпорту/експорту.

База «Підроблені документи». Електронна бібліотечна документаційна система INTERPOL (FIELDS) надає поліцейським і прикордонникам візуальну інформацію про ключові маркери, які можуть вказувати на фальшивий або підроблений документ.

База «Порівняння справжніх і підроблених документів». Edison (Система електронної документації та інформації в мережах розслідувань) надає приклади справжніх проїзних документів, щоб допомогти ідентифікувати підроблені. Він містить зображення, описи та елементи захисту справжніх проїзних документів і документів, що посвідчують особу, виданих країнами та міжнародними організаціями.

5. Банк «Викрадене майно». Викрадені транспортні засоби, судна та твори мистецтва, ймовірно, переправлятимуться через кордон. Глобальні бази даних Інтерполу допомагають правоохоронним органам ідентифікувати вкрадені предмети та збільшують шанси на їх повернення.

База «Автомобілі». Ця база даних містить розширені ідентифікаційні дані всіх типів транспортних засобів (автомобілів, вантажівок, причепів, важкої техніки, мотоциклів) та запчастин, які можна ідентифікувати, про які було повідомлено як про викрадення.

База «Судна». База даних Stolen Vessels служить централізованим інструментом для відстеження та відстеження викрадених суден і двигунів.

База «Твори мистецтва». База даних «Твори мистецтва» містить описи та зображення культурних об'єктів, про які наші країни-члени та міжнародні партнери, такі як Міжнародна рада музеїв та ЮНЕСКО, повідомили як про викрадені. До нього входять предмети, награбовані під час кризових періодів в Афганістані, Іраку та Сирії.

6. Банк «Обіг вогнепальної зброї». Три потужні інструменти допомагають країнам-членам збирати та аналізувати інформацію, яку можна отримати зсередини та ззовні зброї, щоб запобігати та розкривати злочини, пов'язані з вогнепальною зброєю.

База «Ідентифікація вогнепальної зброї». Довідкова таблиця вогнепальної зброї INTERPOL – це інтерактивний онлайн-інструмент, який надає стандартизовану методологію для більш точної ідентифікації та опису вогнепальної зброї, щоб потім її можна було відстежити під час транскордонних розслідувань.

База «Розшук вогнепальної зброї». Система управління записами та розшуком незаконної зброї INTERPOL (iARMS) є єдиною глобальною правоохоронною платформою для підтримки транснаціонального відстеження незаконної, втраченої або викраденої вогнепальної зброї. Він покращує обмін

інформацією та співпрацю між правоохоронними органами щодо тероризму та інших злочинів, пов'язаних із вогнепальною зброєю.

База «Порівняння балістичних даних» Мережа балістичної інформації INTERPOL (IBIN) є єдиною великомасштабною міжнародною мережею обміну балістичними даними у світі. Вона надає розвідувальні дані правоохоронним органам шляхом централізованого зберігання та перехресного порівняння балістичних зображень, щоб знайти зв'язки між злочинами в різних країнах, які інакше могли б залишитися непоміченими.

7. Банк «Мережі організованої злочинності». Метою цих баз даних є покращення збору та обміну розвідданими, підтримка розслідувань і кращий аналіз злочинних мереж, що призводить до ідентифікації та арешту їхніх лідерів і фінансистів.

База «Морське піратство». База даних морського піратства зберігає розвідувальні дані про випадки піратства та збройного пограбування на морі, включаючи дані про осіб, номери телефонів, адреси електронної пошти, випадки піратства, місцезнаходження, підприємства та фінансову інформацію.

Рис. 1.12. Інформація щодо баз даних Інтерполу
(https://www.interpol.int/How-we-work/Databases/Our-19-databases)

Інформація вноситься в банки даних Генерального секретаріату Інтерполу: 1) *за зверненнями* НЦБ Інтерполу; 2*) автоматично* (на постійній основі), відповідними підрозділами Генерального секретаріату Інтерполу, які опрацьовують увесь масив інформації, що надходить від НЦБ Інтерполу про злочини, осіб, які їх вчинили тощо.

Отримання інформації або перевірка тих чи інших відомостей за банками даних Інтерполу здійснюється:

– безпосередньо*, в режимі on-line* – через інформаційно-комунікаційну систему Інтерполу I-24/7 (банки даних щодо осіб, транспортних засобів, документів, творів мистецтва);

– шляхом надсилання *запиту* до Генерального секретаріату Інтерполу (банки даних ДНК, порнографічних зображень, відбитків пальців).

Для забезпечення цільового використання правоохоронними органами держав-членів банків даних Інтерполу, їх функціонування організовано таким чином, що країна-власник інформації щодо об'єкта, розміщеного в банку даних Інтерполу, автоматично отримує повідомлення про факт перевірки цього об'єкта іншою державою (відповідно НЦБ Інтерполу, певним правоохоронним органом тощо). Отримання такого повідомлення для країни-власника інформації є підставою звернутись до країни, що перевіряла об'єкт в банку даних, для з'ясування підстав проведення відповідної перевірки, запитування відомостей про місцезнаходження об'єкта тощо.

Технології Інтерполу

Міжнародні банки даних Інтерполу – є одним із ключових інструментів в боротьбі з транснаціональною злочинністю. Інформаційне наповнення банків даних Інтерполу здійснюється правоохоронними органами всіх держав-членів Організації.

Доступ до цих банків даних забезпечується за допомогою ***інформаційно-комунікаційної системи Інтерполу І-24/7***. Розширення доступу до цієї системи всім без виключення правоохоронним органам України є одним з основних завдань Українського бюро Інтерполу і одним з основних аспектів політики діяльності Міжнародної організації кримінальної поліції – Інтерпол в цілому.

Інформаційно-комунікаційна система Інтерполу І-24/7 (Інтерпол 24 години на добу – 7 днів на тиждень) була впроваджена у діяльність Організації у 2002 році. Вона являє собою захищену від стороннього доступу мережу з обмеженим колом користувачів, що за своєю глобальністю не має аналогів у світі та є ефективним інструментом міжнародного співробітництва правоохоронних органів. Створення та впровадження в діяльність Інтерполу системи І-24/7 мало на меті вирішення двох основних *завдань*:

1) забезпечення *цілодобового оперативного обміну* інформацією національними центральними бюро Інтерполу держав-членів Організації між собою та з Генеральним секретаріатом Інтерполу;

2) надання *on-line доступу* підрозділам поліції та інших правоохоронних органів держав-членів Інтерполу до банків даних Генерального секретаріату Інтерполу.

Тобто обмін повідомленнями в системі І-24/7 є виключною компетенцією Генерального секретаріату та національних центральних бюро, які організовують взаємодію національних правоохоронних органів різних держав під час розслідування конкретних кримінальних справ, здійснюють міжнародний розшук осіб, викраденого транспорту, предметів тощо.

Національні правоохоронні органи держав-членів Інтерполу, такі, як поліція/міліція, підрозділи прикордонної служби та ін., мають можливість отримувати через систему І-24/7 доступ до банків даних Інтерполу.

Генеральний секретаріат Інтерполу не встановлює обмежень щодо кола правоохоронних органів, яким може бути наданий доступ до системи I-24/7. Навпаки, політикою Генерального секретаріату є надання доступу до системи якомога більшому колу користувачів у правоохоронних органах світу задля підвищення ефективності її використання. У багатьох країнах світу вже є повсякденним явищем наявність доступу до банків даних Інтерполу у поліцейських патрульних автомобілях та пунктах пропуску через державний кордон в аеропортах тощо. У деяких країнах на сьогодні система I-24/7 інтегрована з національними правоохоронними комунікаційними системами і є доступною для використання всім правоохоронцям, які безпосередньо здійснюють розкриття та розслідування злочинів.

1.2.9. Система «ЦУНАМІ»

Система централізованого управління нарядами патрульної служби поліції (скорочено – система «ЦУНАМІ») – комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами органів Національної поліції.

Для забезпечення належного захисту життя, здоров'я, прав і свобод киян та гостей столиці від протиправних посягань Головним управлінням (далі – ГУ) МВС України в м. Києві в 2008 року була впроваджена система «ЦУНАМІ». Роботі зі створення цієї системи передувала розробка ГУ МВС України в м. Києві Програми зміцнення законності, посилення боротьби зі злочинністю в місті Києві на 2007–2011 роки.

Метою створення «ЦУНАМІ» є вдосконалення процесу організації управління поліції, що сприятиме:

1) підвищенню ефективності діяльності нарядів поліції, які задіяні для підтримання публічної безпеки і порядку в системі єдиної дислокації, слідчо-оперативних груп, чергових частин (далі – ЧЧ);

2) скороченню часу реагування на повідомлення громадян про кримінальні правопорушення та події, припинення правопорушень та затримання злочинців по «гарячих слідах»;

3) покращанню контролю за своєчасністю та якістю реагування нарядів поліції на кримінальні та інші правопорушення, дотриманням законності під час виконання службових обов'язків працівників поліції.

Впроваджена «ЦУНАМІ» забезпечує користувачів необхідними інформаційними, технічними та аналітичними ресурсами для виконання функціональних обов'язків та прийняття ефективних управлінських рішень. Фактично управління всіма ресурсами органів поліції по реагуванню на злочини і пригоди перенесено з районних підрозділів в центр.

Організаційно система складається з двох рівнів:

1. До складу *міського рівня* організаційної структури входять:

– центр прийняття повідомлень – служба «102»;

– центр управління (чергові по місту, диспетчери-оператори системи);

– центр інформаційно-технічного супроводу системи.

2. До складу *районного рівня* організаційної структури входять:

– чергові частини районних управлінь;

– патрульні наряди районного управління, Департаменту патрульної поліції, Поліції охорони тощо;

– слідчо-оперативні групи;

– дільничні офіцери поліції.

Наведемо характеристику зазначених складових «ЦУНАМІ».

Центр прийняття повідомлень – це служба «102», яка вирішує завдання з прийняття та реєстрації повідомлень про кримінальні правопорушення та інші події на єдиній інформаційній базі.

Автоматизація служби «102» ЧЧ ГУ МВС України в м. Києві дозволила оператору служби заповнювати на комп'ютері формалізовану інформаційну картку (далі – ІК) події зі слів заявника. Система автоматично відслідковує навантаження на кожного оператора та видає аналітичну інформацію про прийом, оброблення та пропуски дзвінків операторами на термінал старшого зміни.

Завдяки інтеграції програмного забезпечення АТС «AWAYA» в систему «ЦУНАМІ» з'явилась можливість *оператором служби «102»* отримувати інформацію про особу та номер, з якого здійснюється дзвінок, ще до моменту підняття трубки, а саме:

– дані про власника телефонного номеру;

– кількість дзвінків, які раніше були здійснені з цього номеру;

– відслідковування повторних викликів по вже зареєстрованій події;

– географічне місцезнаходження абонента на електронній карті міста;

– попередження про дзвінки абонентів які внесені до окремого списку: психічно хворі, телефонні хулігани тощо.

Оператор здійснює первинну кваліфікацію події (в межах отриманої інформації по телефону), заповнює короткий зміст повідомлення, місце та час скоєння, прикмети злочинця, напрямок його руху (рис. 1.13). В залежності від кваліфікації події, оператору надаються відповідні інструкції – перелік питань, які він повинен задати заявнику. В найбільш відповідальних випадках система може автоматично підключити до розмови оперативного чергового по управлінню нарядами (створити конференцію) з метою негайного реагування нарядів по затриманню злочинців. В подальшому електронна картка «102» приєднується до БД «Єдиний облік» ІІПС МВС України, що перешкоджає укриттю кримінальних правопорушень на стадії кваліфікації їх в районних управліннях.

Заповнена оператором картка відразу надходить до диспетчера-чергового, відповідального за керування нарядами поліції в тому чи іншому районі столиці. Відповідне програмне забезпечення відображає інформацію про місце вчинення кримінального правопорушення (місце перебування заявника) на електронній карті м. Києва, розташованій у ЧЧ ГУ МВС України в м. Києві. Диспетчер-черговий направляє найближчі наряди поліції та керує іншими нарядами по розкриттю кримінального правопорушення по «гарячих слідах». За результатами реагування диспетчер ставить відповідні відмітки. Картка залишається на контролі, поки не буде отриманий повний звіт.

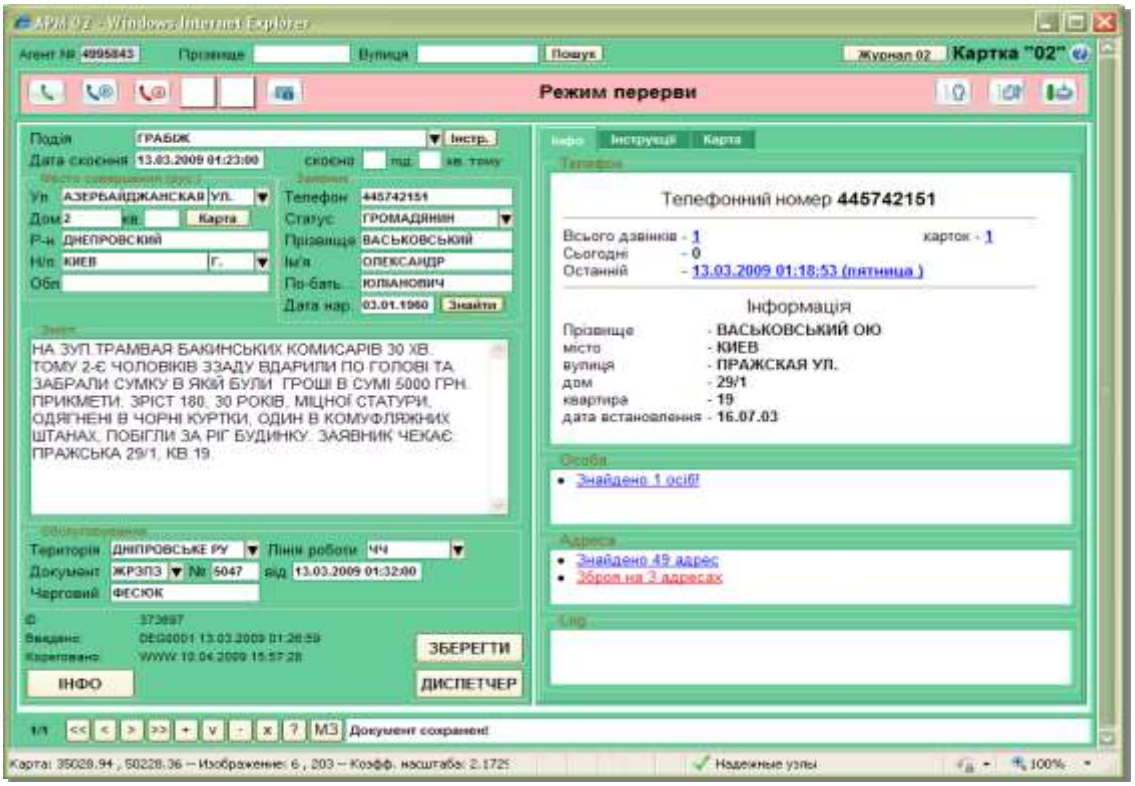


Рис. 1.13. Інформаційна картка «102»

Розглянемо *диспетчерський центр управління*. Висока оперативність реагування мобільних нарядів поліції на кримінальні правопорушення та інші події можлива лише за умови централізації керування нарядами на рівні Головного управління і створення з цією метою в ЧЧ ГУ МВС України в м. Києві диспетчерського центру (рис. 1.14).

Кожний оперативний черговий відповідає за один із районів міста Києва і керує нарядами поліції, у тому числі підрозділів патрульної поліції, поліції охорони тощо, які працюють у районі його обслуговування.

До *функцій диспетчерів-чергових*, відповідальних за організацію реагування на кримінальні правопорушення та пригоди в районах, входить:

– отримання інформації з служби «102» та відстеження на електронній карті місць учинення кримінальних правопорушень;

Рис. 1.14. Диспетчерський центр управління

визначення найближчих вільних нарядів поліції, які необхідно залучити до розкриття кримінального правопорушення по «гарячих слідах», залучення їх для виїзду до заявника, на місце події або в напрямку вірогідного переховування злочинця;

– управління нарядами поліції під час проведення пошукових заходів;

– здійснення моніторингу відеоінформації з камер відеоспостереження, встановлених у районі його обслуговування;

– відстеження результатів реагування на заяви та повідомлення громадян про кримінальні правопорушення, прийняті рішення тощо.

АРМ диспетчера ЧЧ Головного управління:

– відображає перелік подій, прийнятих оператором «102», які були вчинені в районі обслуговування (рис. 1.15);

– в разі визначення телефонного номера заявника відображає накопичені дані по цьому номеру (за якою адресою встановлено, кількість та зміст попередніх звернень);

– надає можливість зв’язатись з оператором «102», який прийняв виклик;

– надає можливість зв’язатись з заявником для уточнення даних по події;

– в разі отримання П.І.Б. заявника, надає всю наявну інформацію про особу з ІІПС МВС України;

– надає повну інформацію на адресу з ІІПС МВС України;

– інформує про повторність надходження інформації про подію;

– відображає дислокацію та стан роботи патрульних нарядів (рис. 1.15);

– забезпечує керування нарядами для реагування на прийняті кримінальні правопорушення та події;

– відслідковує послідовність реагування на подію з остаточною реєстрацію в «Єдиному обліку».

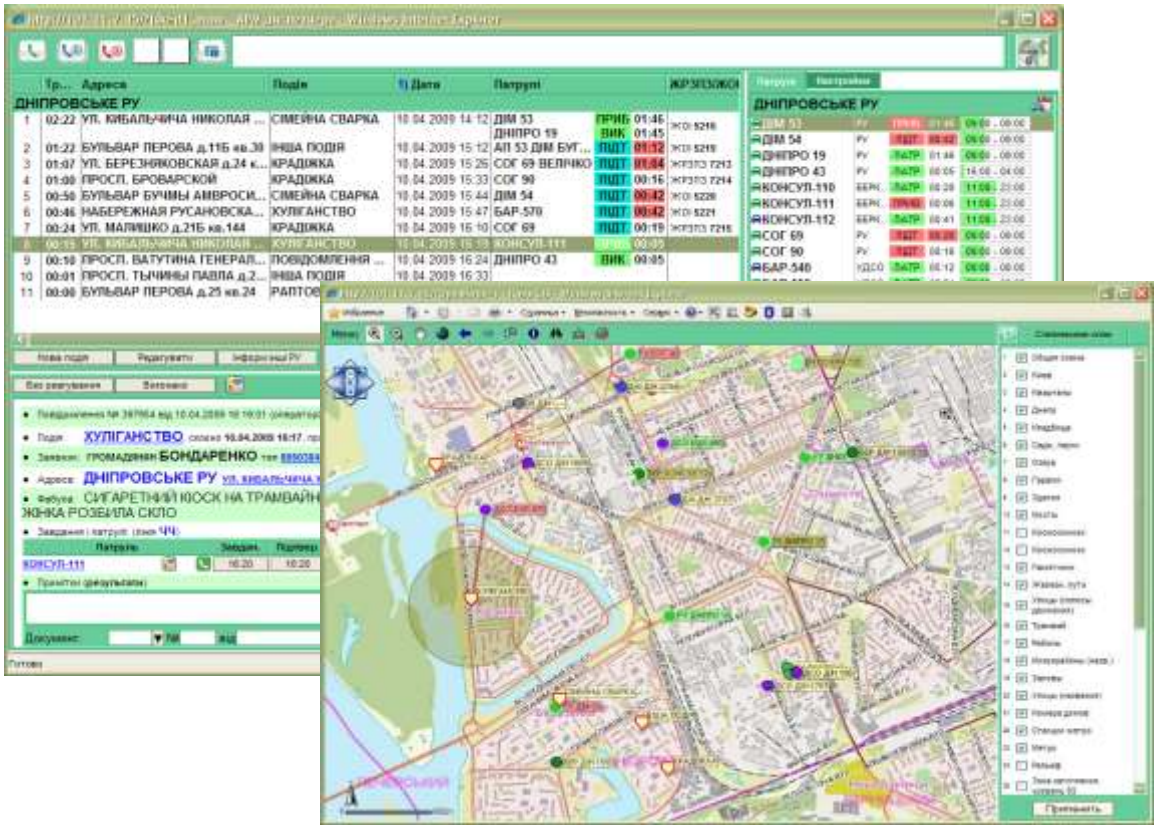


Рис. 1.15. Перелік подій, прийнятих оператором «102», дислокація та стан роботи патрульних нарядів на екранах комп’ютера АРМ диспетчера

1.2.10. Інтегрована інформаційно-пошукова система МВС України

Інтегрована інформаційно-пошукова система МВС України – це сукупність різних довідково-інформаційних та оперативно-розшукових обліків, які інтегровані в одну єдину систему. Інтеграція відомостей здійснюється за установчими даними на особу (ПІБ, дата та місце народження).

Станом на сьогодні означена система є складовою частиною ІІПНП (див. наступний підрозділ).

Метою створення ІІПС МВС України є об’єднання існуючих в МВС України інформаційних ресурсів в Єдиний інформаційно-аналітичний комплекс

із використанням сучасних ІТ, комп'ютерного та комунікаційного обладнання для підтримки оперативно-службової діяльності МВС, суттєвого зміцнення їх спроможності протидії та профілактики злочинності.

Основні завдання ІІПС МВС України:

1. Автоматизація процесів обліку отриманої інформації та обробки інформаційних запитів.
2. Контроль за своєчасністю і повнотою надання первинних документів.
3. Забезпечення надійного зберігання інформаційних обліків, їх систематизації та оперативного доступу до них.
4. Забезпечення комплексного захисту інформації та розмежування доступу до інформації.
5. Обмін інформацією між банками даних ІІПС відповідних рівнів.
6. Інформаційне забезпечення управлінської діяльності, підготовка аналітично-довідкових матеріалів.

Перелік *баз даних* Інтегрованої інформаційно-пошукової системи МВС України (рис. 1.16):

1. БД «Єдиний облік».
2. БД «Злочин».
3. БД «Доставлені».
4. БД «Контур».
5. БД «Особа».
6. БД «Розшук».
7. БД «Адміністративне правопорушення».
8. БД «Корупційне правопорушення».
9. БД «Мігрант».
10. БД «Угон».
11. БД «Річ».
12. БД «Втрачені документи».
13. БД «Кримінальна зброя».
14. БД «Зареєстрована зброя».
15. БД «Електронний рапорт».
16. БД «Пізнання».
17. БД «Антикваріат».
18. БД «Кримінальна статистика».
19. БД «ЄДРПОУ».
20. БД «Домашній арешт».

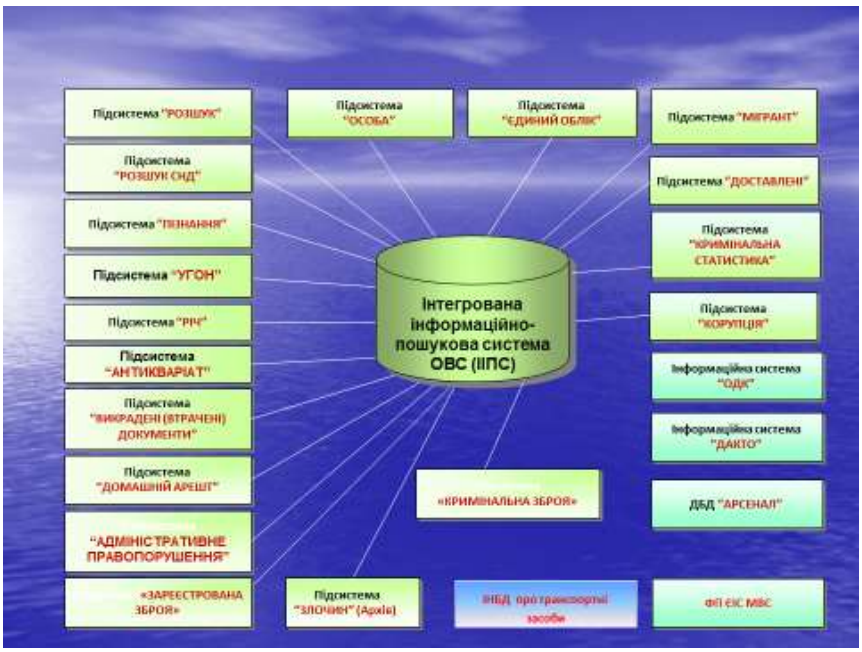


Рис. 1.16. Перелік баз даних Інтегрованої
інформаційно-пошукової системи МВС України

1.2.11. Інформаційний портал Національної поліції України

Інформаційно-комунікаційна система «Інформаційний портал Національної поліції України» (далі – система ІПНП) – сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення. Система ІПНП є складовою частиною Єдиної інформаційної системи МВС України [46].

Основними завданнями системи ІПНП є:

– інформаційно-аналітичне забезпечення діяльності Національної поліції України;

– забезпечення наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до ЄІС МВС;

– забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу;

– забезпечення електронної взаємодії з МВС та іншими органами державної влади.

Система ІПНП *призначена* для:

– формування інформаційних ресурсів ЄІС МВС;

– обробки інформації, яка утворена в процесі діяльності поліції;

– надання безпосереднього оперативного доступу до інформаційних ресурсів ЄІС МВС;

– генерації інтерфейсів та оброблення тимчасових наборів даних для здійснення інформаційної взаємодії органів (підрозділів) поліції з іншими

органами державної влади, органами правопорядку іноземних держав, міжнародними організаціями;

– здійснення пошукових та аналітичних функцій для використання інформації з інформаційних ресурсів (баз даних) поліції, МВС та інших органів державної влади в межах службової діяльності відповідно до рівня доступу і повноважень за запитом або регламентом;

– використання програмних компонентів геоінформаційних підсистем для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об'єкта в залежності від зміни його характеристик, зміни масштабу та деталізації картографічної інформації в інформаційних ресурсах;

– забезпечення автоматизації процесів управління силами та засобами поліції;

– забезпечення електронного документообігу в органах (підрозділах) поліції, обміну електронними документами з МВС;

– комплексного захисту інформації та розмежування доступу до інформації, що зберігається в базах даних системи ІПНП.

Складовими системи ІПНП є:

– центральний програмно-технічний комплекс;

– автоматизовані робочі місця користувачів;

– комунікаційна мережа доступу;

– комплексна система захисту інформації.

Інформаційними ресурсами системи ІПНП є інформація, що утворена в процесі діяльності поліції та використовується для формування:

– тимчасових наборів даних, що створюються в процесі діяльності поліції та використовуються для наповнення та підтримки в актуальному стані баз (банків) даних, які входять до ЄІС МВС та визначені статтею 26 Закону України «Про Національну поліцію»;

– баз даних у сфері управлінських відносин, необхідних для виконання покладених на поліцію повноважень;

– баз даних, необхідних для забезпечення щоденної діяльності поліції, у сфері трудових відносин, фінансового забезпечення, документообігу.

В інформаційних ресурсах системи ІПНП обробляється інформація, яка належить до державних інформаційних ресурсів. Така інформація не підлягає поширенню та передачі іншим особам, крім випадків, передбачених законодавством.

Бази даних поліції, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, *містять відомості*, зокрема, стосовно:

– повідомлень про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, що надійшли технічними каналами зв'язку;

– щодобових переліків та складу нарядів поліції та слідчо-оперативних груп, що заступають на чергування;

– завдань та орієнтувань, що доводились до нарядів поліції для реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події;

– звітування нарядів поліції за результатами реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, виявлення додаткових обставин на місці пригоди;

– пересувань нарядів поліції, які отримані із планшетних комп'ютерів (мобільних терміналів) та засобами GPS.

Користувачами системи ІПНП є посадові особи органів (підрозділів) поліції, яким надано право доступу до інформації в цій системі. Кожна дія користувача щодо отримання інформації з інформаційних ресурсів системи ІПНП фіксується у спеціальному електронному архіві.

На рис. 1.17 відображена структура інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», на рис. 1.18 – взаємодія ІПНП з деякими Центральними органами виконавчої влади, на рис. 1.19 – взаємодія ІПНП з деякими державними електронними інформаційними ресурсами.

Рис. 1.17. Структура інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»

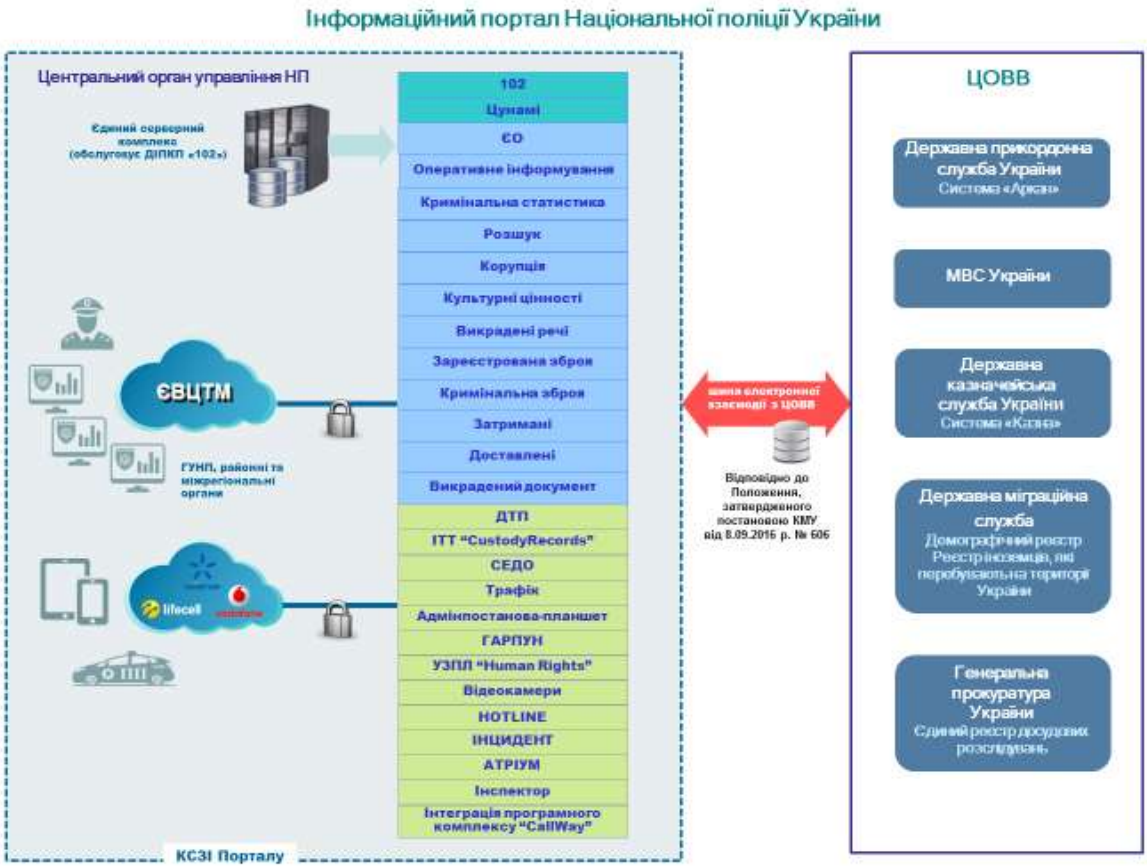


Рис. 1.18. Взаємодія ІПНП з деякими центральними органами виконавчої влади

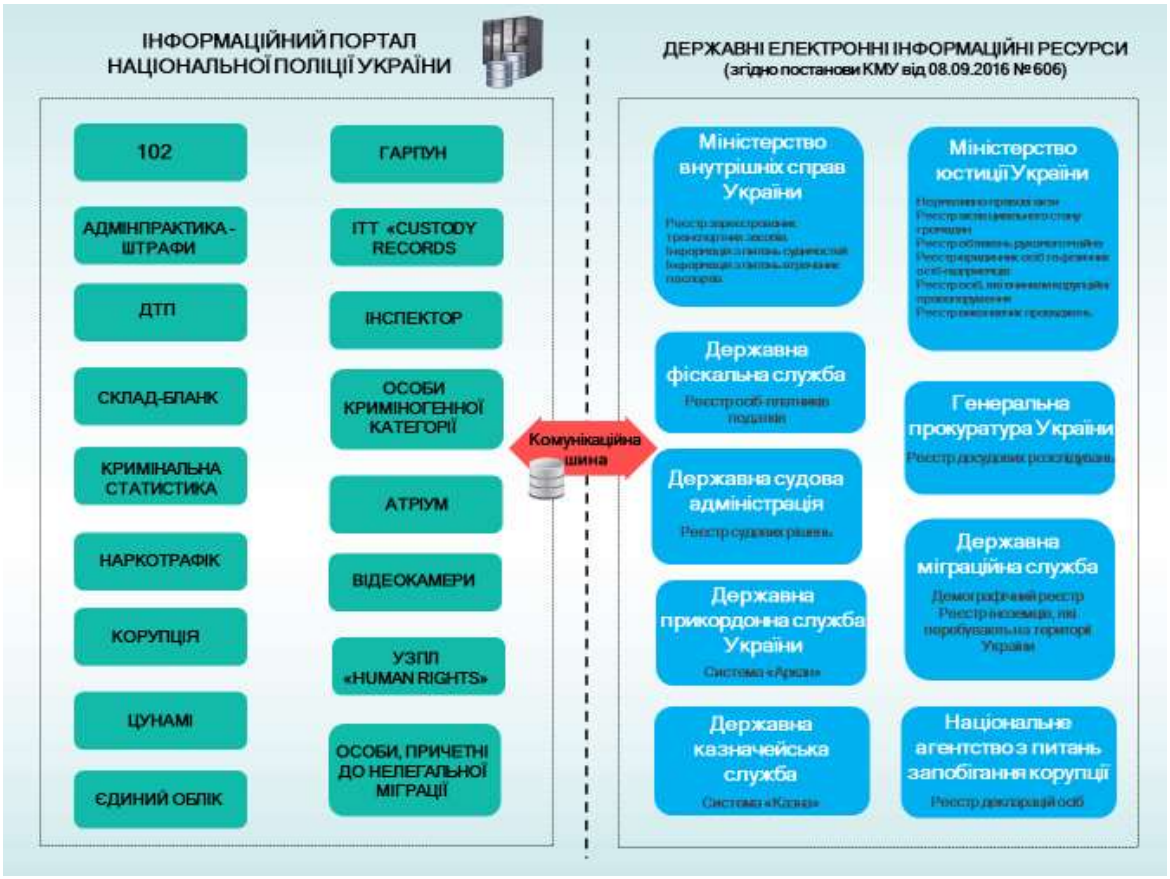


Рис. 1.19. Взаємодія ІПНП з деякими державними електронними інформаційними ресурсами

1.2.12. Єдиний реєстр досудових розслідувань

Єдиний реєстр досудових розслідувань (далі – ЄРДР) – створена за допомогою автоматизованої системи електронна база даних, відповідно до якої здійснюються збирання, зберігання, захист, облік, пошук, узагальнення даних, які використовуються для формування звітності, а також надання інформації про відомості ЄРДР, з дотриманням вимог КПК та законодавства, яким врегульовано питання захисту персональних даних (далі – ПД) та доступу до інформації з обмеженим доступом [36].

ЄРДР утворений та ведеться відповідно до вимог Кримінального процесуального кодексу (далі – КПК) України [28] з *метою забезпечення*:

– реєстрації кримінальних правопорушень (проваджень) та осіб, які їх учинили, обліку прийнятих під час досудового розслідування рішень та результатів судового провадження;

– оперативного контролю за додержанням законів під час проведення досудового розслідування;

– формування звітності про стан кримінальної протиправності та результати роботи органів досудового розслідування;

– аналізу стану та структури кримінальних правопорушень, вчинених у державі;

– інформаційно-аналітичного забезпечення державних органів, у тому числі правоохоронних та судових відповідно до вимог законодавства.

Власником і розпорядником Реєстру є держава в особі Офісу Генерального прокурора

Володільцем інформації, що обробляється в Реєстрі, є Офіс Генерального прокурора.

Офіс Генерального прокурора здійснює:

– розробку та удосконалення нормативно-правової бази для функціонування Реєстру;

– розробку засобів організаційного, методологічного та програмно-технічного ведення Реєстру;

– організацію взаємодії з іншими державними інформаційними ресурсами (системами, реєстрами та базами даних);

– виконання функцій адміністратора Реєстру (забезпечення належної роботи обладнання, технічне і технологічне створення та супроводження програмного забезпечення Реєстру, його адміністрування та моніторинг використання інформації, зберігання та захист даних Реєстру, надання та контроль права доступу тощо);

– навчання Реєстраторів щодо наповнення та користування Реєстром;

– інші функції,

Користувачами ЄРДР є:

– керівники прокуратур та органів досудового розслідування;

– прокурори;

– слідчі органів поліції, безпеки, органів, що здійснюють контроль за додержанням податкового законодавства, органів Державної кримінально-

виконавчої служби України та Державного бюро розслідувань, детективи Національного бюро;

– інші уповноважені особи органів прокуратури та досудового розслідування, які виконують функції з інформаційно-аналітичного забезпечення правоохоронних органів та ведення спеціальних обліків (оперативних, оперативно-облікових, дактилоскопічних тощо).

Внесення відомостей здійснюється шляхом фіксації Реєстратором інформації в ЄРДР та вибору даних у довідниках для заповнення документів первинного обліку про:

– кримінальне правопорушення;

– наслідки досудового розслідування кримінального правопорушення;

– заподіяні збитки, результати їх відшкодування та вилучення предметів злочинної діяльності;

– особу, яка вчинила кримінальне правопорушення та яка підозрюється у його вчиненні;

– рух кримінального провадження.

Установлені форми документів первинного обліку, довідників є єдиними для Реєстраторів усіх правоохоронних органів.

Облік кримінальних правопорушень, осіб, які їх учинили, проводиться за територіальним принципом їх вчинення (юрисдикцією місця вчинення кримінального правопорушення) або за визначенням прокурора відповідного рівня згідно з вимогами статті 218 КПК України.

Обмін інформацією, що міститься в ЄРДР та базах даних Міністерства внутрішніх справ, здійснюється відповідно до вимог чинного законодавства.

Обмін даними щодо осіб у кримінальних провадженнях, що містяться в ЄРДР та автоматизованій системі документообігу суду, облік та використання даних про результати судового провадження здійснюються відповідно до вимог чинного законодавства.

Відомості з ЄРДР надаються у вигляді витягу в порядку, встановленому КПК України.

Витяг з ЄРДР – документ, який засвідчує факт реєстрації в ЄРДР відомостей про кримінальне правопорушення.

Право доступу до відомостей, внесених до ЄРДР, *мають*:

– Держатель – у повному обсязі з урахуванням повноважень, якими наділені прокурори та керівники підрозділів Офісу Генерального прокурора України;

– Директор Національного бюро, перший заступник Директора Національного бюро, керівник Підрозділу детективів Національного бюро, керівник Управління внутрішнього контролю Національного бюро – у межах, визначених статтею 17 Закону України «Про Національне антикорупційне бюро України»;

– прокурори та керівники регіональних, місцевих та військових прокуратур – у межах кримінальних правопорушень, щодо яких слідчими

прокуратури та слідчими піднаглядних їм органів проводиться досудове розслідування;

– керівники органів прокуратури та досудового розслідування, слідчі органів прокуратури, поліції, безпеки, органів, що здійснюють контроль за додержанням податкового законодавства, органів Державної кримінально-виконавчої служби України, Державного бюро розслідувань, Національного бюро – у межах кримінальних правопорушень, щодо яких цими органами проводиться досудове розслідування та здійснюється контроль за додержанням вимог кримінального процесуального законодавства;

– користувачі – у межах наданих адміністратором прав доступу для отримання інформації про розпочаті досудові розслідування та прийняті під час досудового розслідування рішення, забезпечення ведення спеціальних обліків, проведення аналізу результатів діяльності правоохоронних органів.

На підставі внесених реєстраторами відомостей про кримінальні правопорушення та результати досудового розслідування Адміністраторами ЄРДР формується єдина звітність про кримінальні правопорушення, осіб, які їх учинили, та рух кримінальних проваджень. Форма, періодичність подання звітності та правила її формування визначаються нормативними актами за погодженням з центральним органом виконавчої влади у галузі статистики.

Прокурори, керівники органів досудового розслідування усіх рівнів забезпечують у відомствах контроль за своєчасним, повним та достовірним внесенням інформації до ЄРДР у строки, визначені КПК України.

Реєстратор є відповідальною особою за своєчасність, повноту та об'єктивність внесених до Реєстру відомостей згідно з чинним законодавством.

Реєстратори та користувачі відповідають за порушення вимог Положення про ЄРДР, втрату, пошкодження електронних ключів доступу та незаконне втручання в роботу ЄРДР згідно з чинним законодавством.

Питання для самоконтролю

1. Поняття системи інформаційного забезпечення юридичної діяльності.
2. Мета та завдання системи інформаційного забезпечення юридичної діяльності.
3. Принципи формування загальновідомчих та галузевих інформаційних підсистем, які складають основу системи інформаційного забезпечення юридичної діяльності.
4. Поняття інформації та інформаційних технологій.
5. Поняття основних видів інформаційної діяльності та видів інформації за змістом.
6. Який поділ інформації за порядком доступу? Класифікація інформації з обмеженим доступом.
7. Надати характеристику основних властивостей інформації.
8. Які існують формати дати? Особливості їх запису.
9. Формування поліцією інформаційних ресурсів відповідно до норм Закону України «Про Національну поліцію».

10. Використання поліцією інформаційних ресурсів відповідно до норм Закону України «Про Національну поліцію».

11. Класифікація основних видів обліків Міністерства внутрішніх справ України та Національної поліції.

12. Основні правові інформаційно-пошукові системи.

13. Реєстри вебпорталу Міністерства юстиції України.

14. Поняття Єдиного державного реєстру судових рішень.

15. Розшукові обліки на вебпорталі МВС України.

16. Поняття персонально-довідкового обліку МВС України.

17. Характеристика банків даних Генерального секретаріату Інтерполу.

18. Поняття інформаційно-комунікаційної системи Інтерполу I-24/7.

19. Автоматизовані робочі місця на вебпорталі Національної академії внутрішніх справ.

20. Загальна характеристика системи «ЦУНАМІ».

21. Характеристика Центру прийняття повідомлень – служби «102».

22. Характеристика Центр управління системи «ЦУНАМІ».

23. Поняття та мета створення Інтегрованої інформаційно-пошукової системи МВС України.

24. Основні завдання Інтегрованої інформаційно-пошукової системи МВС України.

25. Перелік баз даних Інтегрованої інформаційно-пошукової системи МВС України.

26. Поняття, основні завдання та структура інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України».

27. Загальна характеристика Єдиного реєстру досудових розслідувань.

Список використаних і рекомендованих джерел

Закони України

Основні

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР.
2. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII.
3. Про Національну поліцію : Закон України від 2 лип. 2015 р. № 580-VIII.

Додаткові

4. Про авторське право і суміжні права : Закон України від 23 груд. 1993 р. № 3792-XII.
5. Про бібліотеки і бібліотечну справу : Закон України від 27 січ. 1995 р. № 32/95-ВР.
6. Про видавничу справу : Закон України від 5 черв. 1997 р. № 318/97-ВР.
7. Про офіційну статистику : Закон України від 16 серп. 2022 р. № 2524-IX.
8. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII.
9. Про державну підтримку засобів масової інформації та соціальний захист журналістів : Закон України від 23 верес. 1997 р. № 540/97-ВР.
10. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI.
11. Про доступ до судових рішень : Закон України від 22 груд. 2005 р. № 3262-IV.
12. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16 листоп. 1992 р. № 2782-XII.

13. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5 жовт. 2017 р. № 2155-VIII.

14. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV.

15. Про захист від недобросовісної конкуренції : Закон України від 7 черв. 1996 р. № 236/96-ВР.

16. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 лип. 1994 р. № 80/94-ВР.

17. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI.

18. Про звернення громадян : Закон України від 2 жовт. 1996 р. № 393/96-ВР.

19. Про інформаційні агентства : Закон України від 28 лют. 1995 р. № 74/95-ВР.

20. Про Концепцію Національної програми інформатизації : Закон України від 4 лют. 1998 р. № 75/98-ВР.

21. Про науково-технічну інформацію : Закон України від 25 черв. 1993 р. № 3322-XII.

22. Про Національний архівний фонд та архівні установи : Закон України від 24 груд. 1993 р. № 3814-XII.

23. Про Національну програму інформатизації : Закон України від 1 груд. 2022 р. № 2807-IX.

24. Про Національну систему конфіденційного зв’язку : Закон України від 10 січ. 2002 р. № 2919-III.

25. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII.

26. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII.

27. Про електронні комунікації : Закон України від 16 груд. 2020 р. № 1089-IX.

28. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI.

29. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III.

30. Кодекс України про адміністративні правопорушення : Закон Української РСР від 7 груд. 1984 р. № 80731-X.

Підзаконні нормативно-правові акти

Основні

31. Про Стратегію сталого розвитку «Україна-2020» : Указ Президента України від 12 січ. 2015 р. № 5/2015.

32. Деякі питання документування управлінської діяльності : постанова Кабінету Міністрів України» від 17 січ. 2018 р. № 55).

33. Деякі питання електронної взаємодії державних електронних інформаційних ресурсів : постанова Кабінету Міністрів України від 8 верес. 2016 р. № 606.

34. Про затвердження Положення про Міністерство внутрішніх справ України : постанова Кабінету Міністрів України від 28 жовт. 2015 р. № 878.

35. Про затвердження Положення про Національну поліцію : постанова Кабінету Міністрів України від 28 жовт. 2015 р. № 877.

36. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення : наказ Офісу Генерального прокурора від 30 черв. 2020 р. № 298.

37. Порядок електронної інформаційної взаємодії Офісу Генерального прокурора та Міністерства внутрішніх справ України : наказ Офісу Генерального прокурора, МВС України від 22 листоп. 2021 р. № 371/846.

38. Про затвердження Інструкції з автоматизованого обліку адміністративних правопорушень : наказ МВС України від 4 лип. 2016 р. № 595.

39. Про затвердження Інструкції з оформлення документів у системі МВС України : наказ МВС України від 27 лип. 2012 р. № 650.

40. Про затвердження Інструкції з оформлення матеріалів про адміністративні правопорушення в органах поліції : наказ МВС України від 6 листоп. 2015 р. № 1376.

41. Про затвердження Інструкції про порядок ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події : наказ МВС України від 6 листоп. 2015 р. № 1377.

42. Про затвердження Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України : наказ МВС України від 26 груд. 2016 р. № 1351.

43. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення Єдиної інформаційної системи МВС : наказ МВС України від 20 жовт. 2017 р. № 870.

44. Про затвердження Положення про Єдину цифрову відомчу телекомунікаційну мережу МВС : наказ МВС України від 4 лип. 2016 р. № 596.

45. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України : наказ МВС України від 12 жовт. 2009 р. № 436 (втратив чинність 08.02.2022).

46. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС України від 3 серп. 2017 р. № 676.

47. Деякі питання ведення обліку відомостей про притягнення особи до кримінальної відповідальності та наявності судимості : наказ МВС України від 30 берез. 2022 р. № 207.

48. Про затвердження Інструкції з організації реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України : наказ МВС України від 16 лют. 2018 р. № 111.

49. Про затвердження Інструкції про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол : наказ МВС України, Офісу Генерального прокурора, Національного антикорупційного бюро України, Служби безпеки України, Державного бюро розслідувань, Міністерства фінансів України, Міністерства юстиції України від 17 серп. 2020 р. № 613/380/93/228/414/510/2801/5.

50. Про затвердження Переліку відомостей, що становлять службову інформацію в системі Національної поліції України : наказ Національної поліції України від 10 трав. 2016 р. № 385.

Додаткові

51. Про Єдину комп’ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю : Указ Президента України від 31 січ. 2006 р. № 80.

52. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних : постанова Кабінету Міністрів України від 21 жовт. 2015 р. № 835.

53. Про затвердження Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства : постанова Кабінету Міністрів України від 27 груд. 2017 р. № 1073.

54. Про затвердження Порядку ведення Єдиного державного реєстру судових рішень : постанова Кабінету Міністрів України від 25 трав. 2006 р. № 740.

55. Про затвердження Порядку використання комп’ютерних програм в органах виконавчої влади : постанова Кабінету Міністрів України від 10 верес. 2003 р. № 1433.

56. Про затвердження Порядку легалізації комп’ютерних програм в органах виконавчої влади : постанова Кабінету Міністрів України від 4 берез. 2004 р. № 253.

57. Про затвердження Концепції формування системи національних електронних інформаційних ресурсів : розпорядження Кабінету Міністрів України від 5 трав. 2003 р. № 259-р.

58. Про схвалення Концепції розвитку електронного урядування в Україні : розпорядження Кабінету Міністрів України від 20 верес. 2017 р. № 649-р.

59. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення : наказ Офісу Генерального прокурора від 30 черв. 2020 р. № 298.

60. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 7 лип. 2017 р. № 575.

61. Про затвердження Інструкції про порядок використання поліграфів у Національній поліції України : наказ МВС України від 13 листоп. 2017 р. № 920.

62. Про затвердження положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України : наказ МВС України від 29 лют. 2016 р. № 139.

63. Про затвердження Положення про територіальний сервісний центр МВС : наказ МВС України від 29 груд. 2015 р. № 1646.

64. Про затвердження порядку використання безконтактного електронного носія, який імплантовано в паспорт громадянина України : наказ МВС України від 16 лют. 2016 р. № 104.

65. Про організацію роботи із запитами на публічну інформацію в Національній поліції України : наказ МВС України від 7 лют. 2017 р. № 95.

66. Про затвердження Змін до Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС : наказ МВС України від 26 груд. 2023 р. № 1071.

67. Про затвердження Інструкції з діловодства в системі Національної поліції : наказ Національної поліції України від 20 трав. 2016 р. № 414.

68. Про затвердження Інструкції про порядок запису та збереження в цифровому вигляді заяв і повідомлень, які надходять за телефоном «102», або за допомогою інших засобів зв'язку до Національної поліції України : наказ Національної поліції України від 13 черв. 2017 р. № 574.

69. Про затвердження Положення про систему Інтернет у телекомунікаційній мережі Національної поліції України : наказ Національної поліції України від 21 лют. 2017 р. № 141.

Навчальна література

Основна

70. Кудінов В. А., Орлов Ю. Ю., Пакриш О. Є. Інформаційні технології в діяльності Національної поліції : навч. посіб. Київ, 2017. 100 с.

71. Кудінов В. А., Смаглюк В. М., Хахановський В. Г. Інформаційне забезпечення ОВС: навч. посіб. Київ, 2015. 108 с.

72. Кудінов В. А., Смаглюк В. М., Хахановський В. Г. Інформаційні технології в правозастосовній практиці : навч. посіб. Київ, 2015. 112 с.

73. Кудінов В. А., Смаглюк В. М., Хахановський В. Г. Інтегрована інформаційно-пошукова система органів внутрішніх справ України : навч. посіб. Київ, 2014. 112 с.

Додаткова

74. Інформатика в юридичній діяльності (частина 1) : підручник / [В. А. Іщенко, О. М. Грищак, В. А. Кудінов та ін.] / за заг. ред. В. А. Кудінова. Київ, 2016. 256 с.

75. Інформатика в юридичній діяльності (частина 2) : підручник / [В. А. Кудінов, І. М. Мельников, О. Є. Пакриш та ін.] / за заг. ред. В. А. Кудінова. Київ, 2017. 332 с.

Інтернет-ресурси

76. Президент України : [офіц. інтернет-представництво]. URL: http://www.president.gov.ua/ua.

77. Верховна Рада України : [офіц. вебпортал]. URL: http://www.rada.gov.ua.

78. Кабінет Міністрів України : [офіц. вебпортал]. URL: https://www.kmu.gov.ua/ua.

79. Міністерство внутрішніх справ України : [офіц. вебпортал]. URL: http://www.mvs.gov.ua.

80. Міністерство юстиції України : [офіц. вебпортал]. URL: https://minjust.gov.ua.

81. Національна академія внутрішніх справ : [офіц. вебпортал]. URL: http://www.naiau.kiev.ua.

82. Національна поліція України : [офіц. вебпортал]. URL: http://www.npu.gov.ua/uk.

83. Національна бібліотека ім. В. І. Вернадського : [офіц. вебпортал]. URL: http://www.nbuv.gov.ua.

РОЗДІЛ ІІ
НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАТИЗАЦІЇ ЮРИДИЧНОЇ ДІЯЛЬНОСТІ

2.1. Національне законодавство у сфері застосування інформаційних технологій у правозастосовній діяльності

Вирішення завдань підвищення ефективності та якості діяльності всіх ланок державного управління стосуються й органів, що здійснюють правозастосовну діяльність. Профілактика правопорушень, боротьба зі злочинністю, охорона громадського порядку та інші завдання, що вирішуються правоохоронними органами, потребують подальшого вдосконалення техніки і методів управління на основі сучасних досягнень науки та практики, розробки й впровадження комп'ютеризованих систем. Так само це стосується, зокрема, й судових органів.

Залежно від призначення тієї чи іншої правової норми в регулюванні функціонування складових елементів системи державного управління інформаційною сферою ці норми можливо об'єднати у такі групи:

– норми, що закріплюють цілі, основні завдання та напрями діяльності держави в інформаційній сфері. Ця програмно-цільова група норм, до яких належать, зокрема, норми, закріплені в статтях 3, 10, 17 Конституції України, в Законі України «Про інформацію», у розділах IV, VI Закону України «Про Концепцію Національної програми інформатизації» від 4 грудня 1998 р., Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 9 січня 2007 р. та ін., має цілеспрямовуюче значення для функціонування всієї системи державного управління інформаційною сферою;

– норми, що визначають систему суб'єктів державного управління інформаційною сферою та їх адміністративно-правовий статус.

Законами України можуть визначатися окремі повноваження органів загальної компетенції стосовно управління інформаційною сферою. Зокрема, ст. 21 Закону України «Про Кабінет Міністрів України» від 21 грудня 2006 р. серед його повноважень визначає проведення державної політики у сфері інформатизації, сприяння становленню єдиного інформаційного простору та ін.

Важливе місце в зазначеній групі норм посідають також норми, закріплені в підзаконних нормативно-правових актах (далі – НПА), передусім ті з них, що містяться в актах Президента України, Кабінету Міністрів України (далі – КМУ), якими визначається адміністративно-правовий статус міністерств, інших центральних органів виконавчої влади, що здійснюють державне управління в інформаційній сфері (наприклад, постанова КМУ «Про затвердження Положення про Міністерство транспорту та зв'язку України» від 6 червня 2006 р. № 789).

Норми, що регулюють порядок взаємодії суб'єктів державного управління інформаційною сферою з керованими ними суб'єктами інформаційних відносин в процесі реалізації прямих і зворотних управлінських зв'язків між ними. До цієї групи належать, передусім, норми, що детально регламентують процедури застосування різних методів державного управління в інформаційній сфері, визначають форми їх реалізації. Такі норми закріплені, наприклад, в статтях 23–37 Закону України «Про телебачення і радіомовлення», які регламентують процедуру здійснення такого методу управління, як ліцензування в галузі телебачення і радіомовлення.

В Законі України «Про друковані засоби масової інформації (пресу) в Україні» від 16 листопада 1992 р. врегульований порядок здійснення обов'язкової державної реєстрації друкованих засобів масової інформації. Законом України «Про державну таємницю» в ст. 22 регламентовано порядок надання допуску громадян до державної таємниці. Застосування низки заходів адміністративного примусу врегульовано нормами Кодексу України про адміністративні правопорушення.

В цих законах та інших нормативно-правових актах визначаються і вимоги до форми правових актів управління, що приймаються при застосуванні зазначених методів.

До цієї ж групи можна віднести й норми, що містяться в Інструкції Національної ради України з питань телебачення і радіомовлення про порядок здійснення перевірок телерадіоорганізацій та провайдерів програмної послуги України, затвердженій рішенням Національної ради України з питань телебачення і радіомовлення від 24 січня 2007 р. № 69, якою регламентована процедура проведення зазначеним органом перевірок з метою одержання необхідної інформації про функціонування суб'єктів підвідомчої йому галузі управління, тобто врегульована процедура забезпечення зворотного зв'язку в процесі державного управління цією галуззю.

Окремі норми визначають адміністративно-правовий статус суб'єктів інформаційних відносин. Так, ст. 7 Закону України «Про електронні комунікації» визначає повноваження Генерального штабу Збройних Сил України у сфері користування радіочастотним спектром, ст. 7 Закону України «Про електронні комунікації» визначає повноваження центрального органу виконавчої влади у сферах електронних комунікацій та радіочастотного спектра.

Основні принципи формування та комплексного використання інформаційних систем правоохоронних органів України визначаються Конституцією України та чинним інформаційним законодавством, на основі якого формується відомча та галузева підзаконна нормативно-правова база. Враховані також міжнародні принципи формування та використання інформаційних систем кримінального судочинства, розроблені Організацією Об'єднаних Націй у 1992 році.

Керівництвом правоохоронних органів обумовлюється спеціальна нормативно-правова, методологічна та технологічна сумісність системи інформаційного забезпечення.

Формування інформаційних підсистем, які складають основу інформаційно-аналітичного забезпечення правоохоронних органів, здійснюється згідно з такими *принципами*: функціонального призначення; нормативно-правового забезпечення; фактичності даних; доцільності впровадження та експлуатації; нарощування та розвитку; гармонізації законодавства України із європейським правом.

Під час створення, впровадження та функціонування інформаційно-аналітичних систем правоохоронної діяльності враховувались такі групи нормативно-правових документів:

– закони України;

– міжнародні нормативні акти;

– укази Президента України;

– постанови Кабінету Міністрів України;

– накази та розпорядження міністерств та відомств правоохоронних органів, рішення колегій;

– накази керівництва головних управлінь та управлінь в областях.

Серед законів України слід виділити такі: «Про інформацію», «Про Національну програму інформатизації», «Про авторське право і суміжні права», «Про електронні комунікації», «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про антикорупційне бюро України», «Про офіційну статистику», «Про Основні засади розвитку інформаційного суспільства в Україні», «Про дорожній рух», «Про державну таємницю», «Про захист інформації в інформаційно-комунікаційних системах», «Про корупцію», Кримінальний і Кримінальний процесуальний кодекси України.

В Законі України «Про Національну програму інформатизації» наведено такі важливі терміни та поняття: база даних; база знань; геоінформаційні системи; засоби інформатизації; інформатизація; інформаційно-комунікаційна технологія; інформаційний продукт; інформаційний ресурс тощо, які широко використовуються у правозастосовній діяльності. Одним із основних завдань Національної програми інформатизації є створення загальнодержавних систем інформаційно-аналітичної підтримки діяльності органів державної влади та органів місцевого самоврядування. Відповідно до ст. 6 зазначеного Закону органи державної влади в межах їх компетенції здійснюють такі функції у процесі інформатизації:

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

– встановлення стандартів, норм і правил використання засобів інформатизації;

– 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 оброблення інформації;

– забезпечення підготовки фахівців з питань інформатизації та інформаційних технологій;

– організацію сертифікації програмних і технічних засобів інформатизації;

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

– забезпечення інформаційної безпеки держави.

Крім того, відповідно до розділу 7 Закону України від 4 лютого 1998 р. № 75/98-ВР «Про Концепцію Національної програми інформатизації» реалізація проектів програми забезпечить підвищення рівня ефективності боротьби з правопорушеннями, корупцією, організованою злочинністю на основі створення першої черги інтегрованої інформаційно-аналітичної системи правоохоронних органів України та міжвідомчого інформаційно-аналітичного комплексу аналізу і прогнозування рівня злочинності та правопорушень.

Особливо важливим нормативно-правовим документом в сфері інформатизації боротьби зі злочинністю став Указ Президента України «Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю» від 31 січня 2006 р. № 80/2006, метою якого було покращення координації оперативно-розшукових, правових та інформаційних заходів правоохоронних органів щодо боротьби зі злочинністю, підвищення рівня роботи в цій сфері.

У продовження цього Указу була прийнята постанова КМУ «Про затвердження Державної програми інформаційно-комунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю» від 8 квітня 2009 р. № 321, яка до втрати своєї чинності (на підставі постанови КМУ від 22 квітня 2013 р. № 315) відіграла свою важливу роль.

Крім того, слід виділити, зокрема, такі постанови Кабінету Міністрів України:

– «Про затвердження Порядку підключення до глобальних мереж передачі даних» від 12 квітня 2002 р. № 522;

– «Про затвердження Концепції технічного захисту інформації в Україні» від 8 листопада 1997 р. № 1126;

– «Про затвердження Положення про технічний захист інформації в Україні» від 9 вересня 1994 р. № 632;

– «Про створення інтегрованої міжвідомчої автоматизованої системи обміну інформацією з питань контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон «Аркан»»: наказ Адміністрації Державної прикордонної служби України, СБ України, МВС України, МЗС України, Служби зовнішньої розвідки України, Держмитслужби, ДПА України, Міністерства праці та соціальної політики України від 3 квітня 2008 р. № 284/287/214/150/64/175/266/75;

– «Про затвердження Порядку ведення Єдиного державного реєстру судових рішень» від 25 травня 2006 р. № 740.

Зрозуміло, що крім зазначених НПА, створення та функціонування інформаційно-аналітичної системи правоохоронних органів має ґрунтуватися на відомчих наказах, розпорядженнях, рішеннях Колегій та інструкціях, а також на спільних наказах правоохоронних та державних органів України, зокрема, на таких наказах та розпорядженнях МВС України:

– «Про створення дворівневої комп'ютеризованої інформаційної підсистеми щодо обробки статистичних даних органів внутрішніх справ УВС областей та МВС (шифр «Статистика 2», статистика на рівні МВС), «Статистика 3» (статистика на рівні УВС області)» – 1975 р.;

– «Про організацію і тактику розшуку злочинців, що переховуються, безвісті зниклих громадян та встановлення невпізнаних осіб та заходи щодо вдосконалення організації їх розшуку» (наказ МВС України від 9 травня 1992 р.);

– «Про створення Міжвідомчого банку даних по обліку інформації про незаконний обіг наркотичних речовин та причетних до нього осіб» (шифр «Наркобізнес»)» (наказ МВС України від 1995 р.);

– «Про порядок ведення персонального оперативно-довідкового та дактилоскопічного обліків в органах внутрішніх справ України» (наказ МВС України від 2 березня 1995 р.);

– «Про створення в ОВС України підрозділів оперативного інформування» (наказ МВС України від 16 травня 1995 р. № 302);

– «Про створення комп'ютеризованої інформаційної підсистеми щодо обліку криміногенних осіб та номерних речей (шифр «Профілактика-Розшук)» (наказ МВС України від 1996 р.);

– «Про створення єдиної системи централізованого номерного обліку вогнепальної зброї в системі МВС України» (наказ МВС України від 30 квітня 1996 р. № 290);

– «Про створення єдиного автоматизованого банку даних втрачених і викрадених паспортів» (лист МВС України від 8 квітня 1998 р. № 1897/ШТ);

– «Про затвердження Інструкції про порядок ведення та використання в роботі бази даних викраденого в країнах СНД автомототранспорту підрозділами Державтоінспекції» (наказ МВС України від 1995 р. № 99, наказ МВС України від 3 квітня 1998 р. № 252);

– «Про впровадження у діяльність органів внутрішніх справ України комп'ютерної системи збору та передачі інформації «Електронна пошта»» (наказ МВС України від 14 травня 1998 р. № 343);

– «Про проект створення інформаційної підсистеми обліку осіб, оголошених у регіональний, державний та міждержавний розшук (розпорядження МВС України від 30 січня 1998 р.). Подальший розвиток ІПС «Розшук» забезпечував наказ МВС України від 31 грудня 2000 р. № 590 «Про внесення змін та доповнень до Інструкції про організацію і тактику розшуку зниклих злочинців, безвісти пропалих громадян та встановлення невідомих осіб»;

– «Про заходи щодо удосконалення єдиної інформаційної мережі ОВС України» (розпорядження МВС України від 12 березня 1998 р. № 45);

– «Про вдосконалення системи ідентифікації безвісти зниклих та невпізнаних трупів громадян в органах внутрішніх справ» (розпорядження МВС України від 26 жовтня 2000 р. № 276);

– «Про затвердження Положення про єдину цифрову відомчу телекомунікаційну мережу МВС» (наказ МВС України від 4 липня 2016 р.);

– «Про підвищення ефективності функціонування автоматизованої інформаційної системи розшуку викрадених транспортних засобів – «Угон»»;

– «Про створення Єдиної системи централізованого номерного обліку вогнепальної зброї в системі МВС України – АІС "Арсенал"»;

– «Про підвищення ефективності функціонування автоматизованих інформаційних систем обліку викрадених, втрачених державних номерних знаків та реєстраційних документів – АІПС «Номерний знак», «Документ», «Довідка-рахунок»»;

– «Про Концепцію розвитку системи інформаційного забезпечення ОВС України»;

– «Інструкція про оперативно-довідкові та дактилоскопічні обліки в ОВС та органах (установах) кримінально-виконавчої системи України»;

– «Про першочергові заходи щодо створення Центру та підрозділів технічного захисту інформації в системі МВС України»;

– «Про організацію і виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України»;

– «Про затвердження Інструкції про створення Єдиної автоматизованої системи номерного обліку вогнепальної (стрілецької) зброї, яка зберігається й використовується в МВС, на об'єктах дозвільної системи та перебуває в особистому користуванні громадян»;

– «Про вдосконалення реагування на повідомлення про злочини, інші правопорушення і події та забезпечення оперативного інформування в органах і підрозділах внутрішніх справ України»;

– «Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України»;

– «Про затвердження Інструкції з організації функціонування Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України».

Крім того, певний інтерес становлять розпорядження МВС України «Про вдосконалення інформаційного забезпечення органів внутрішніх справ», «Про запровадження новітніх інформаційних технологій в діяльність органів внутрішніх справ України», а також рішення Колегії МВС України «Про затвердження Програми інформатизації ОВС України».

З точки зору інформаційної безпеки та захисту інформації в інтегрованому банку даних також певний інтерес становить наказ Державної служби України з питань технічного захисту інформації «Про затвердження Інструкції щодо умов і правил здійснення діяльності у галузі технічного захисту інформації та контролю за їх дотриманням».

Як зазначалось вище, у державних органах влади України, зокрема у правоохоронних органах, створена та функціонує низка різноманітних інформаційних баз даних та автоматизованих інформаційних систем, які вже об'єднані (або ведуться роботи щодо їх об'єднання) в інтегровані банки даних.

Так, у 1994 р. в Адміністрації Державної прикордонної служби України було впроваджено інтегровану інформаційно-комунікаційну систему «Гарт», користувачами якої є Адміністрація Державної прикордонної служби України та інші міністерства й відомства.

У 2000 р. у цьому відомстві було впроваджено банк даних викрадених транспортних засобів (так звана БД-13), який є складовою системи «Гарт» та міжвідомчої системи «Аркан».

У 2007 р. було створено базу даних «Відомості про осіб, які перетнули державний кордон України», яка також є складовою систем «Гарт» та «Аркан».

У 2008 р. була введена в експлуатацію інтегрована міжвідомча автоматизована система обміну інформацією з питань контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон – «Аркан».

Абонентами системи є Адміністрація Державної прикордонної служби України, Служба безпеки України, МВС України, МЗС України, Служба зовнішньої розвідки України, Держмитслужба, Державна податкова адміністрація України, Міністерство праці та соціальної політики України.

Система «Аркан» призначена для своєчасного, достовірного та функціонально повного інформаційно-аналітичного забезпечення діяльності суб'єктів системи стосовно здійснення ними заходів із запобігання і недопущення в'їзду в Україну або виїзду з України осіб, яким згідно із законодавством не дозволено в'їзд в Україну або яких тимчасово обмежено в праві виїзду з України, у тому числі й згідно з дорученнями правоохоронних органів, розшуку в пунктах пропуску через державний кордон осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, припинення протиправної діяльності фізичних і юридичних осіб, які незаконно переправляють мігрантів в Україну або транзитом переміщують їх через територію України, посилення контролю за додержанням правил в'їзду, виїзду, перебування в Україні іноземців та осіб без громадянства, а також виконання інших завдань у правоохоронній сфері відповідно до законодавства.

До складу системи «Аркан» входять такі бази даних:

– СБ України: відомості про осіб, яким цим відомством заборонено в'їзд в Україну; стосовно яких є доручення СБ України; відомості про транспортні засоби, стосовно яких є доручення СБ України;

– Служба зовнішньої розвідки України: відомості про осіб, стосовно яких є доручення СЗРУ;

– Міністерство внутрішніх справ України: відомості про осіб, яким МВС заборонено в'їзд в Україну; стосовно яких є доручення МВС; відомості про втрачені, викрадені та оголошені недійсними документи, що дають право на

виїзд з України та в'їзд в Україну; відомості про транспортні засоби, що перебувають у розшуку; про фізичних осіб, які перебувають у розшуку; про транспортні засоби, зареєстровані в Україні; про викрадені предмети культурної спадщини; про транспортні засоби, стосовно яких є доручення МВС України;

– Державна прикордонна служба України: відомості про осіб, яким органами охорони держкордону заборонено в'їзд в Україну; про осіб, стосовно яких виконано доручення правоохоронних органів, у тому числі СБУ і МВС; про вилучені, втрачені, викрадені та оголошені недійсними документи, що дають право на виїзд/в'їзд в Україну; про затримані транспортні засоби, які перебувають у розшуку; про документи, видані установами МЗС і МВС, в яких виявлено несправності під час здійснення паспортного контролю; про візи, видані установами МЗС, в яких виявлено несправності під час здійснення паспортного контролю; відомості про осіб, які перетнули державний кордон; про осіб, яким органами держкордону відмовлено у перетинанні державного кордону; про осіб, затриманих за організацію незаконного переміщення через державний кордон; про осіб, стосовно яких органами дізнання Державної прикордонної служби порушено кримінальні справи; про іноземців та осіб без громадянства, які не виїхали з України після закінчення строку перебування в Україні; про транспортні засоби, стосовно яких виконано доручення СБУ та МВС;

– МЗС України: відомості про втрачені, викрадені та оголошені недійсними документи громадян України для виїзду за кордон, видані МЗС, дипломатичними представництвами та консульськими установами України за кордоном; про документи, що дають право на в'їзд та виїзд з України, оформлені МЗС та дипломатичними представництвами та консульськими установами України за кордоном; про іноземців та осіб без громадянства, яким оформлено візи для в'їзду в Україну; про іноземців та осіб без громадянства, яким оформлено дозволи на перебування в Україні;

– Державна митна служба України: інформація про митне оформлення транспортних засобів, які перетинають митний кордон; про перетинання вантажами митного кордону; про порушників митного законодавства;

– ДПА України: відомості про юридичних та фізичних осіб – підприємців, які перебувають на податковому обліку; про осіб, стосовно яких є доручення ДПА.

У 2008 р. у МВС України було створено Державну інформаційну систему реєстраційного обліку фізичних осіб та їх документування.

У 2007 р. в Міністерстві юстиції України створено Державний реєстр актів цивільного стану громадян.

У 2004–2007 рр. в Укрзалізниці було створено автоматизовані системи управління «Експрес-2», «Експрес-УЗ» (Південно-Західна залізниця), «Експрес-УЗМ» (Львівська залізниця), Єдину автоматизовану систему управління пасажирськими перевезеннями (АСК ПП УЗ). Продаж проїзних документів відбувався виключно з використанням особистих даних. Слід зазначити, що подібні автоматизовані системи у колишньому СРСР були досить ефективними

у боротьбі зі злочинністю (зокрема, системи «Аеропорт», «Аеропорт-2»). З 2010 р. залізничні квітки знову продаються із введенням особистих даних. На наш погляд, необхідно відновити таку реєстрацію на авіатранспорті, а також поширити її на інші пасажирські перевезення.

У 2003 р. НЦБ Інтерполу, а також ГУМВС, УМВС України були підключені до інформаційно-пошукової системи «I-24/7» Інтерполу.

Крім того, у Державному митному комітеті України існує Центральна база даних електронних копій вантажних митних декларацій; у Міграційній службі функціонує автоматизована інформаційна система (далі – ІС) «Біженець». Відповідно до Закону України від 22 грудня 2005 р. № 3262-IV «Про доступ до судових рішень» у Державному підприємстві «Інформаційні судові системи» функціонує Єдиний державний реєстр судових рішень, доступ до якого відкритий через Інтернет.

База даних «Банкрутство» функціонує відповідно до Положення про порядок формування та ведення єдиної бази даних про підприємства, щодо яких порушено провадження у справі про банкрутство.

У МВС України в 2003 р. впроваджено ІІПС «АРМОР». Функціонують також спеціалізована біометрична система «АРГУС», Інтегрований національний банк даних про транспортні засоби. Слід зазначити, що останнім часом у МВС України було розроблено низку проектів створення автоматизованих інформаційних систем та баз даних, зокрема, Положення про ІІПС ОВС України та Інструкція з організації її функціонування.

Нормативно-правова база в галузі інформаційної діяльності забезпечує інтеграцію і сумісність баз даних, регулює процеси збирання, накопичення та передачі інформації в системі правоохоронних органів, затверджує правила щодо виконання технологічних процесів роботи з інформаційними банками даних, з визначенням відповідних термінів проходження інформації, вимог до оформлення даних (повнота, достовірність, актуальність тощо), використання інформації у службовій діяльності та персоналізує відповідальність за дотримання цих правил.

2.2. Міжнародні документи у сфері нормативно-правового регулювання інформаційних технологій у правозастосовній діяльності

У вирішенні питань формування та використання інформаційних систем та мереж країни світу базуються на узгодженості (адаптації, гармонізації) їх нормативно-правового забезпечення із міжнародними стандартами держав – членів Ради Європи та Європейського Союзу, які визначають стандартні принципи обробки ПД в автоматизованих системах.

Згідно з Конвенцією № 108 Ради Європи «Про захист осіб у зв’язку з автоматизованою обробкою персональних даних» від 28 січня 1981 р., положення якої отримали розвиток у Директивах Європейського Парламенту та Ради Європи 95/46/ЄС «Про захист осіб у зв’язку з обробкою персональних

даних і вільним обігом цих даних» від 24 жовтня 1995 р. та 97/66/ЄС «Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі» від 15 грудня 1997 р., це потребує застосування у національному законодавстві наступних базових принципів, які передбачають забезпечення щодо:

– **якості даних.** ПД, що піддаються автоматизованій обробці:

- отримують та обробляють сумлінно та законно;
- зберігаються для визначених і законних цілей та не використовуються у спосіб, несумісний з цими цілями;
- мають бути адекватними, відповідними і не надмірними з точки зору цілей, для яких вони зберігаються;
- мають бути точними та в разі необхідності мають поновлюватися;
- зберігаються у форматі, який дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для цілі, для якої такі дані зберігаються;

– **захисту особливих категорій даних.** Персональні дані, що свідчать про расову приналежність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій. Це правило застосовується також до ПД, що стосуються засудження у кримінальному порядку;

– **безпеки даних.** Для захисту ПД, що зберігаються у файлах даних для автоматизованої обробки, вживаються відповідні заходи безпеки, спрямовані на запобігання випадковому чи несанкціонованому знищенню або випадковій втраті, а також на запобігання несанкціонованому доступу, зміні або поширенню;

– **додаткових гарантій для суб'єкта даних.** Будь-якій особі надають можливість:

- встановлювати існування файлу персональних даних для автоматизованої обробки, його головні цілі, а також особу та постійне місце проживання чи головне місце роботи контролера файлу;
- отримувати через розумні проміжки часу та без надмірної затримки або витрат підтвердження або спростування факту зберігання персональних даних, що її стосуються, у файлі даних для автоматизованої обробки, а також отримувати такі дані у доступній для розуміння формі;
- вимагати у відповідних випадках виправлення або знищення таких даних, якщо вони оброблялися всупереч положенням внутрішнього законодавства, що запроваджують основоположні принципи, визначені у Конвенції № 108 Ради Європи від 28.01.1981 р.;
- використовувати засоби правового захисту в разі невиконання передбаченого у пунктах b і c цієї статті прохання про підтвердження або у відповідних випадках про надання, виправлення або знищення ПД.

У загальному плані наведеним принципам повинні відповідати усі діючі інформаційні підсистеми, а також ті, що створюються чи мають бути створені.

Міжнародне законодавство у сфері інформатизації

Серед міжнародних нормативно-правових документів, що стосуються регулювання інформаційних відносин та відносин в сфері інформатизації, слід виділити такі:

- Загальна декларація прав людини (ООН, 1948 р.);
- Статут Ради Європи (Лондон, 5 травня 1949 р.);
- Конвенція Ради Європи «Про захист прав людини та основоположних свобод» (від 1950 р.);
- Конвенція Ради Європи (від 7 червня 1968 р., редакція від 14 липня 1993 р.);
- Конвенція Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (№ 108 від 28 січня 1981 р.);
- Конвенція Ради Європи «Про взаємну допомогу у кримінальних справах» (від 20 квітня 1959 р.);
- Додатковий Протокол до Конвенції Ради Європи від 20 квітня 1959 р. «Про взаємну допомогу у кримінальних справах» (від 17 березня 1978 р.);
- Додатковий Протокол до Конвенції Ради Європи № 108 від 28 січня 1981 р. «Про захист осіб у зв'язку з автоматизованою обробкою ПД щодо органів нагляду та транскордонних потоків даних» (від 8 листопада 2001 р.);
- Другий Додатковий Протокол від 8 листопада 2001 р. до Конвенції Ради Європи від 20 квітня 1959 р. «Про взаємну допомогу у кримінальних справах»;
- Конвенція Ради Європи «Про кіберзлочинність» (№ 185 від 23 листопада 2001 р.);
- Рекомендації Ради Європи «Про захист персональних даних у автоматизованих базах медичних даних» (№ К (81)1 від 23 січня 1981 р.);
- Рекомендації Ради Європи «Про доступ до інформації, що знаходиться у розпорядженні державних органів» (№ К (81) 19 від 25 листопада 1981 р.);
- Рекомендації Ради Європи «Про захист ПД, що використовуються для наукових досліджень та статистики» (№ К (83) 10 від 23 вересня 1983 р.);
- Рекомендації Ради Європи «Про практичне застосування положень Конвенції про взаємну правову допомогу з кримінальних справ щодо судових доручень про перехоплення телекомунікаційних повідомлень» (№ К (85) 10 від 28 червня 1985 р.);
- Рекомендації Ради Європи «Про регулювання використання персональних даних у секторі поліції» (146 № К (87) 15 від 17 вересня 1987 р.);
- Рекомендації Ради Європи «Про передачу третім особам персональних даних, які знаходяться в розпорядженні державних органів» (161 № К (91) 10 від 9 вересня 1991 р.);
- Рекомендації Ради Європи «Про проблеми кримінально-процесуального права, пов'язані з інформаційними технологіями» (165 № К (95) 13 від 11 листопада 1995 р.);

- Рекомендації Ради Європи «Про захист осіб у зв'язку з обробкою даних у інформаційних магістралях» (168 № К (99) 5 від 23 лютого 1999 р.);
- Рекомендації Ради Європи «Про висвітлення у засобах масової інформації виборчих компаній» (172 № К (99)15 від 9 листопада 1999 р.);
- Рекомендації Ради Європи «Про права журналістів не розголошувати їх джерела інформації» (175 № К (2000)7 від 8 березня 2000 р.);
- Рекомендації Ради Європи «Про європейську політику доступу до архівів» (190 № К (2000)13 від 13 липня 2000 р.);
- Рекомендації Ради Європи «Про доступ до офіційних документів» (203 № К (2002)2 від 21 лютого 2002 р.);
- Конвенція Європейського Союзу «Про Європол» (від 1995 р.);
- Акт Ради Європейського Союзу «Про правила щодо конфіденційності інформації Європолу» (1998/С26/02 від 3 листопада 1998 р.);
- Акт Ради Європейського Союзу «Про правила щодо аналізу файлів Європолу» (1998/С26/01 від 3 листопада 1998 р.);
- Акт Ради Європейського Союзу «Про правила щодо отримання інформації Європолом від третіх сторін» (1999/С 26/03 від 3 листопада 1998 р.);
- Акт Ради Європейського Союзу «Про правила щодо врегулювання передачі персональних даних Європолом до третіх держав та третім органам» (1999/С88/01 від 12 березня 1999 р.);
- Конвенція Європейського Союзу «Про взаємну правову допомогу з кримінальних справ» (від 29 травня 2000 р.);
- Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист осіб у зв'язку з обробкою ПД і вільним обігом цих даних» (від 24 жовтня 1995 р.);
- Директива 96/9/ЄС Європейського Парламенту і Ради «Про правовий захист баз даних» (від 11 березня 1996 р.);
- Директива 96/19/ЄС Комісії ЄС «Про внесення поправок до Директиви 90/388/ЄЕС «Про забезпечення повної конкуренції на ринках телекомунікацій» (від 13 березня 1996 р.);
- Директива 97/13/ЄС Європейського Парламенту і Ради «Про спільну базу для загальних дозволів та індивідуальних ліцензій в сфері телекомунікаційних послуг» (від 10 квітня 1997 р.);
- Директива 97/66/ЄС Європейського Парламенту і Ради «Про обробку ПД і захист прав осіб у телекомунікаційному секторі» (від 15 грудня 1997 р.);
- Директива 99/93/ЄС Європейського Парламенту і Ради «Про систему електронних підписів, що застосовується в межах Співтовариства» (від 13 грудня 1999 р.);
- Директива 2000/31/ЄС Європейського Парламенту і Ради «Про правові аспекти інформаційних послуг щодо електронної комерції на внутрішньому ринку» (від 8 червня 2000 р.);
- Директива 2002/58/ЄС Європейського Парламенту і Ради «Про обробку ПД та захист таємниці у секторі телекомунікацій» (від 12 липня 2002 р.);

- Резолюція Ради Європейського Союзу «Про законне перехоплення телекомунікаційних повідомлень» (від 17 січня 1995 р.);
- Резолюція Ради Європейського Союзу «Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг» (від 20 червня 2001 р.);
- Регламент Європейського Парламенту і Ради № 45/2001 «Про захист фізичних осіб, що стосується обробки ПД установами і органами Спільноти і щодо вільного переміщення таких даних» (від 18 грудня 2000 р.);
- Декларація Комітету міністрів Ради Європи «Про європейську політику в галузі нових інформаційних технологій» (від 7 травня 1999 р.);
- Хартія Глобального інформаційного суспільства (рекомендації країн «вісімки» щодо принципів і напрямків формування і розвитку інформаційного суспільства, Окінава, 2000 р.);
- Організація Об'єднаних Націй: Конгрес з попередження злочинності, пов'язаної з використанням комп'ютерних мереж (Відень, 2000 р.).

2.3. Правові інформаційно-пошукові системи

Для громадян єдиним джерелом отримання інформації з правових питань завжди була консультація юриста. При цьому професійна діяльність юриста завжди була пов'язана з опрацюванням значних обсягів правових відомостей з різних галузей права, аналізом нестандартних правових ситуацій, що виникають під час кваліфікації правопорушень, зокрема, кримінальних, різноманітних суперечливих з точки зору чинного законодавства ситуацій.

Обсяг правових відомостей настільки великий, що для оперативного доступу до них, їх систематизації, своєчасного і коректного використання юристами та звичайними громадянами все більш актуальним стає застосування спеціалізованих програмно-технічних засобів – правових інформаційно-пошукових систем [2; 7; 10; 12; 18; 19; 21].

2.3.1. Загальна характеристика правової інформаційної системи

Відомо, що юридична діяльність здебільшого пов'язана з пошуком, аналізом, обробкою, використанням, зберіганням та поширенням актуальної правової інформації. З розвитком інформаційних систем вони стали активно застосовуватися в юридичній діяльності [10–21].

Інформаційні системи, як правило, розглядаються як сукупність організаційних і технічних засобів для збереження та опрацювання інформації з метою забезпечення інформаційних потреб користувачів. ІС є середовищем, складовими елементами якої є комп'ютери, програмні продукти, БД, люди, засоби зв'язку тощо [10; 12; 15].

Інформаційний ресурс – це сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо) [6].

Основна мета інформаційних систем – це організація зберігання, обробки та передавання інформації на основі автоматизації інформаційних процесів у різних сферах людської діяльності [13, с. 58].

Виділяють ***три етапи розвитку інформаційних систем***:

1. *Автоматизовані системи керування* – обмежуються розв'язанням деяких функціональних управлінських завдань, зокрема, бухгалтерського обліку.

2. Використання *централізованої БД*, яка за допомогою системи керування базою даних обслуговує всі прикладні програми.

3. Концепція єдиної централізованої керованої бази моделей – блоків обчислень, спільних для багатьох прикладних програм. Такі системи одержали назву *системи підтримки прийняття рішень*.

З розвитком ІТ та засобів комунікацій на Заході в 60-х роках XX ст. почали активно використовувати ІС в юридичній діяльності.

У 1967 році в Бельгії була розроблена електронна картотека *«CREDOC»*. Вона містила документи внутрішнього і міжнародного права. Для того, щоб отримати з неї відомості, потрібно було звернутися в спеціальне інформаційне бюро.

В 1967 році почалась розробка однієї з найвідоміших повнотекстових ІС США *(«LEXIS»*), в якій є всі судові прецеденти США, а також нормативно-правові акти штатів та федерального значення, включаючи повний текст Конституції США. Згодом в «*LEXIS*» було додано законодавство Великобританії та англійські судові прецеденти. Сьогодні ця система доступна в мережі Інтернет (*«LEXIS-NEXIS»*).

Всі *електронні картотеки* мають той *недолік*, що вони не дають змоги ознайомитись з повним текстом документа. Тому були створені більш зручні *повнотекстові системи*, які дозволяли не тільки швидко знаходити в інформаційних масивах необхідний документ, але й працювати з його змістом.

Сучасні інформаційні системи ***вирішують наступні задачі***:

1) здійснення пошуку, обробки та зберігання інформації, яка накопичується протягом тривалого періоду часу;

2) зберігання структурованих даних;

3) створення процедур та технічних засобів для їх реалізації, за допомогою яких можна автоматизувати процес пошуку інформації;

4) аналіз та прогнозування різних видів інформації. Вивчають потоки інформації з метою їх мінімізації, стандартизації та адаптування для ефективної обробки в рамках інформаційних систем;

5) дослідження способів представлення та зберігання інформації, розробка спеціальних прийомів кодування інформації, анотування об'ємних документів та їх реферування;

6) створення мереж зберігання, обробки та передачі інформації, що включать бази даних, термінали обробки та засоби зв'язку.

Правові інформаційні системи є одним із різновидів ІС, тому для них характерні ті самі ***властивості***, що й для будь-якої ІС, зокрема [12; 18; 22; 28]:

– структура й функціонування системи визначається поставленими перед нею цілями і завданнями;

– ІС є впорядкованою сукупністю елементів, які є підсистемами та характеризуються функціональною самостійністю, якісною відособленістю;

– функціонування будь-якої інформаційної системи полягає у прийомі, створенні, зберіганні, передачі, обробки і видачі інформації;

– система має зручний інтерфейс для взаємодії користувача з системою, що дає можливість формулювати складні запити у зручній для користувача формі;

– єдність системи та взаємозв'язок її складових частин – наявність підсистем, єдиної файлової БД, єдиних стандартів та протоколів та єдиного управління в межах однієї системи;

– зв'язок з оточуючим середовищем щодо обміну ресурсами та, водночас, відособленість від нього, тобто відносна відокремленість від тих фактів середовища, що не впливають на досягнення поставленої мети.

Однак є певні ***особливості***, які характеризують виключно ***правові інформаційні системи***. Вони містять [11; 12; 22; 28]:

– нормативно-правові акти органів державної влади та органів місцевого самоврядування;

– відомчі нормативні акти, судових прецедентів, актів нотаріальних органів;

– різного роду довідкові матеріали в юридичних документах;

– статистичні відомості в галузі права;

– наукові дослідження, проведені на основні аналізу правових актів;

– накази та розпорядження посадових осіб підприємств, установ та організації тощо.

Основною метою правових інформаційних систем є надання користувачеві повної, достовірної та актуальної правової інформації [5].

Правові інформаційні системи можна ***класифікувати*** за такими напрямками:

1. *За рівнем або сферою діяльності* – державні, територіальні, галузеві, підприємств або установ та окремих технологічних процесів.

2. *За рівнем автоматизації процесів управління* – інформаційно-пошукові системи, інформаційно-довідкові системи (далі – ІДС), інформаційно-керівні системи, інтелектуальні інформаційні системи, системи підтримки прийняття рішень.

3. *За ступенем централізації обробки інформації* – централізовані ІС, децентралізовані ІС, інформаційні системи колективного використання.

4. *За ступенем інтеграції функцій* – багаторівневі ІС з інтеграцією за рівнями управління (підприємство – об'єднання, об'єднання – галузь та ін.), багаторівневі ІС з інтеграцією за рівнями планування.

Для ІПС (ІДС) характерні два етапи функціонування: 1) збір та зберігання інформації; 2) пошук та видача інформації користувачу.

В залежності від ***режиму організації пошуку*** ІПС (ІДС) поділяються на:

1. *Документальні* – в них реалізується пошук в інформаційному фонді документів чи текстів у відповідності з отриманим запитом з подальшим наданням користувачу цих документів чи їх копій. Вся обробка отриманої інформації в документальних ІПС здійснюється користувачем.

2. *Бібліографічні* – характеризуються тим, що пошук ведеться в інформаційному фонді вторинних джерел.

3. *Бібліотечні* – пошук ведеться в інформаційному фонді, що складається з первинних документів.

4. *Фактографічні* – реалізують пошук та видачу фактів, документів та текстів, що містять відомості, які можуть задовольнити запит користувача. Основною їх відмінністю є те, що вони надають користувачу не конкретний документ, а в певній мірі опрацьовану інформацію.

Таким чином, ***правова інформаційна система*** – це організаційно-технічна система, яка забезпечує вироблення рішень на основі автоматизації інформаційних процесів у правовій сфері життя суспільства.

Правові ІПС надають можливість користувачам отримати широкий доступ до НПА України та інших документів [4; 8; 10]. Вони можуть входити до різних автоматизованих робочих місць юриста, бухгалтера, менеджера, банкіра тощо. Ними можуть користуватися всі, хто бажає отримати інформацію чи консультативну юридичну допомогу.

Використання правових ІПС в юридичній діяльності дозволяє ***одержати наступні результати*** [10; 12; 17; 20]:

1) інтенсифікація пошукових процесів шляхом одержання за одиницю часу більших обсягів правових матеріалів і створення умов для їх більш глибокого аналізу та документального оформлення на персональному комп’ютері;

2) економія часу, засобів і ресурсів при здійсненні пошуку необхідної інформації, відстеженні всіх змін і доповнень у чинних правових актах;

3) широкі можливості для ведення аналітичної роботи з документами;

4) зростання результативності прийнятих рішень, що пов’язано з підвищенням швидкості реагування на зміни законодавчої бази;

5) підвищення якості професійної діяльності юристів.

Найбільш відомими на українському ринку правовими ІПС є: «Ліга: Закон» (платна) , «Нормативні акти України» (далі – НАУ) (платна), «Законодавство України» (безкоштовна) .

2.3.2. Єдина інформаційно-правова платформа «Ліга: Закон»

Продукти компанії «Ліга: Закон» забезпечують швидкий доступ до законодавчої бази України, заощаджують час при здійсненні пошуку необхідної нормативної інформації, допомагають у прийнятті ефективних рішень, мають зручний інструментарій для роботи з документами, надають можливість ведення аналітичної роботи та доступ до періодичних видань з оглядами питань

оподаткування, бухгалтерського обліку, підприємницької діяльності та іншою бізнес і довідковою інформацією; надають можливість створення власних статистичних добірок і звітів у будь-якому тематичному розрізі та у часі; надають можливість отримати швидку консультацію у фахівців Центру «Ліга» тощо [10; 23; 26].

Компанія «Ліга: Закон» розробила спеціальну хмарну платформу для запуску всіх своїх продуктів.

Переваги хмарної платформи:

– *Єдине середовище*. Виконує роль єдиного інформаційного поля для різних ключових підрозділів та співробітників організацій. Це єдині принципи роботи із інформацією, єдиний пошук та класифікатори, єдина система взаємних прямих і зворотних посилань між різними типами інформації.

– *Для щоденної роботи.* Незамінний і надійний інструмент для повсякденної роботи керівників, юристів, бухгалтерів, фахівців у сфері управління персоналом, викладачів, студентів у правовому полі України.

– *Хмарні технології.* Забезпечують цілодобову підтримку безперебійної діяльності бізнесу, підприємців, підприємств державного сектору, громадських організацій та об'єднань.

– *Мобільність.* Інноваційні технологічні рішення й адаптивний дизайн платформи дозволяють отримувати користь для бізнесу з різних мобільних пристроїв. Щоб користуватися платформою, достатньо доступу до Інтернету рівня 2G.

Сьогодні продукти компанії «Ліга: Закон» об'єднують понад 160 тисяч користувачів, а також Адміністрацію Президента України, Кабінет Міністрів України, різні міністерства й інші органи виконавчої державної влади і місцевого самоврядування, банки, посольства, іноземні представництва, компанії, а також численні комерційні структури [23].

ІПС «Ліга: Закон» складається з програмної оболонки, яка забезпечує пошук документів, та інформаційного ядра – текстових БД нормативних документів. Станом на сьогодні вона містить понад 1,7 млн різних документів. Система оснащена різними наборами сервісів та інструментів.

Сучасні ***продукти компанії*** «Ліга: Закон» (https://ligazakon.net/?role=all):

I. *Інформаційно-правові системи «Ліга: Закон»*.

II. *Періодичні видання та довідники*.

III. *Сервіси моніторингу та аналізу*.

IV. *Сервіси електронної звітності та документообігу*.

I. Інформаційно-правові системи «Ліга: Закон» [26]

Системи «Ліга: Закон» – найповніше джерело систематизованої та достовірної правової інформації зі зручними інструментами для пошуку. Дають змогу швидко знайти й проаналізувати правову інформацію на будь-який момент часу, оцінити ситуацію та прийняти правильне рішення.

Класифікація систем «Ліга: Закон»:

1. **«*Гранд*»** – система для ключових підрозділів великого підприємства (бухгалтерії, юридичного департаменту та кадрового відділу), яка також містить електронні видання «БУХГАЛТЕР&ЗАКОН» та «ЮРИСТ&ЗАКОН».

2. **«*Прайм*»** – система для підприємства, зокрема керівника, бухгалтера («Ситуації для бухгалтера», «Консультації» та ін.), кадровика («Ситуації для кадровика», «Інструкції та шаблони») і юриста («Судова практика», «Коментовані кодекси» та ін.).

3. **«*Бухгалтер проф*»** – система для невеликого підприємства, що містить правову інформацію для бухгалтера: «Форми та бланки», «Ситуації для бухгалтера», «Консультації», «Калькулятори» та ін.

4. **«*Юрист проф*»** – система для юридичної компанії та юриста: «Коментовані кодекси», «Європейське законодавство», «Мистецтво оборони», «Судові прецеденти та практика» та ін.

5. **«*Юрист*»** – спеціалізована система для юриста й адвоката: «Термінологічний словник», «Законопроекти», «Ситуації для юриста», повне «Законодавство України», «Довідники» та ін.

Класифікація інформаційно-правових систем «Ліга: Закон» за об'єктом призначення:

– **Загальні модулі**: «Законодавство України», «Правова картина дня», «Новації», «Влада України», «Типові договори та шаблони», «Банкрутство», «Довідники».

– **Керівнику**: «Ситуації для бізнесу», «Галузі економіки».

– **Кадровику**: «Ситуації для кадровика», «Інструкції та шаблони для кадровика».

– **Юристу**: «Термінологічний словник», «Календар юриста», «Законопроекти», «Ситуації для юриста», «Судова практика», «Коментовані кодекси», «Європейське законодавство», «Мистецтво оборони», «Судові прецеденти», «Калькулятор штрафів».

– **Бухгалтеру**: «Калькулятор індексації зарплати», «Калькулятор відпусток», «Календар бухгалтера», «База податкових знань», «Форми та бланки», «Ситуації для бухгалтера», «Консультації», «Судова практика для бухгалтера», «Бухгалтерські проводки».

– **Електронні видання**: «БУХГАЛТЕР&ЗАКОН», «ЮРИСТ&ЗАКОН».

Модуль *«**Законодавство України**»* містить такі документи:

– прийняті Верховною Радою України (далі – ВРУ) з 1990 року;

– прийняті Президентом України з 1990 року;

– прийняті КМУ з 1991 року;

– зареєстровані Міністерством юстиції України, прийняті міністерствами та іншими органами державної виконавчої влади з 01 січня 1993 року;

– прийняті законодавчими та виконавчими органами влади СРСР, УРСР, які не втратили чинності на сьогодні;

– усі чинні кодекси України;

– роз'яснення, листи, накази та інструкції Державної фіскальної служби;

– постанови, листи Національного банку України, Міністерства фінансів України;

– чинні в Україні міжнародні угоди, конвенції та інші документи міжнародного права, починаючи з 1815 року;

– документи про кадрові перестановки, нагородження, про перейменування, зміну кордонів населених пунктів і територіальних одиниць тощо.

II. Періодичні видання та довідники [26]

1. **«ЮРИСТ&ЗАКОН»**

Електронне видання для юриста містить аналітичні матеріали з практичними рекомендаціями експертів «ЛІГА: ЗАКОН» і практикуючих юристів. Тексти доповнено таблицями, інфографікою, відео. *Періодичність виходу*: щотижня. *Мовні версії*: українською та російською мовами. Термінові статті доступні ще до виходу номера. *Можливості «ЮРИСТ&ЗАКОН»*:у фокусі видання завжди найгарячіші теми, експертні думки та консультації провідних юристів компаній, адвокатів, а також держорганів з найактуальніших питань правозастосування; отримання аналітики та практики застосування права: аналіз, алгоритми дій, практичні рекомендації та висновки; у кожному номері – експертні думки, оцінки й коментарі представників органів влади та відомих юристів, аналіз свіжої судової практики й найбільш важливих тем з юридичних форумів; гіперпосилання у статтях дають можливість переходу зі сторінок видання до нормативно-правової бази, судових рішень. Зручний пошук за підшивкою номерів і тематиками дає змогу швидко знайти потрібну інформацію; усім користувачам доступний архів номерів за попередні 2 роки.

2. **«БУХГАЛТЕР&ЗАКОН»**

Електронне видання для бухгалтерів великих і середніх підприємств, бухгалтерів, які ведуть бухоблік у декількох підприємствах, аудиторів, юристів, бізнес-консультантів, що включає аналітичні матеріали з практичними рекомендаціями експертів «ЛІГА: ЗАКОН». Режим читання максимально наближений до друкованих видань. Тексти доповнено таблицями. *Періодичність виходу*: журнал виходить щотижня. Термінові статті доступні ще до виходу номера. *Мовні версії*: українською та російською мовами. *Можливості «БУХГАЛТЕР&ЗАКОН»*: у центрі уваги завжди “гарячі” теми, які опрацьовують експерти, спілкуючись із бухгалтерами різних підприємств і вивчаючи найпопулярніші теми бухгалтерських форумів; практичні рекомендації щодо виконання бухгалтерських завдань на щодень; рекомендації юриста для бухгалтера; огляд та аналіз судової практики щодо податкових спорів з практичними висновками; добірки матеріалів для бухгалтерів бюджетних організацій; можливість швидко знайти необхідний матеріал у підшивці номерів видання та тематичних рубриках; відразу зі статті видання можна переходити за посиланнями на нормативно-правовий акт, що заощаджує час на їхній пошук і дає можливість глибше проаналізувати матеріал; сервіс «Обране» дає можливість зберігати добірки потрібних статей і коментарів, необхідних у повсякденному професійному житті; у передплатників є можливість поставити запитання до редакції видання або авторові конкретної статті (протягом 2-х тижнів з дня виходу номера) й одержати на нього відповідь; миттєва доставка: номер доступний на комп’ютері читача відразу

після випуску; усім комерційним користувачам доступний архів видання з липня 2014 р.

3. **«ВІСНИК МІЖНАРОДНИХ СТАНДАРТІВ ФІНАНСОВОЇ ЗВІТНОСТІ»** (далі – МСФЗ)

Всеукраїнське спеціалізоване періодичне видання про практику застосування МСФЗ. У виданні представлено огляд нових і переглянутих МСФЗ, аналізуються типові помилки у складанні фінансової звітності, розглядаються питання складання інтегрованої звітності та розвитку бізнесу. *Періодичність виходу***:** один раз на місяць. *Мовні версії***:** українською та російською мовами. *Можливості видання «Вісник МСФЗ» (в Україні)*: корисний інструментарій з освоєння та практичного застосування положень МСФЗ – постійний спеціальний додаток "Довідник МСФЗ", де систематизована необхідна інформація для формування професійних суджень; формат електронного видання дає змогу не лише оперативно знайомитися з новинами та головними подіями у сфері МСФЗ, а й завжди мати під рукою архів документів зі зручними функціональними можливостями роботи з ним; крім висвітлення практичних питань застосування МСФЗ, кожен випуск містить цікаву інформацію із суміжних галузей. Наприклад, про особливості ведення бізнесу й оподаткування у різних країнах світу (Китай, Ізраїль, Італія, Великобританія, Сінгапур, Австрія тощо); безпосередньо зі статті видання можна переходити за посиланнями на нормативні акти, стандарти, що заощаджує час на їх пошук і дає можливість глибше проаналізувати матеріал; миттєва й гарантована доставка – відразу після випуску номер доступний читачу.

4. **«ІНТЕРАКТИВНА БУХГАЛТЕРІЯ»**

Щоденне електронне видання для бухгалтерів, фінансистів, юристів, власників бізнесу, керівників, кадровиків, викладачів і студентів облікових та фінансових дисциплін. Обсяг видання не можна оцінити у звичайних паперових сторінках, адже масштаб інформації не обмежений і залежить лише від інформаційних потреб користувачів. Усі матеріали зв'язані гіперпосиланнями з базою НПА від «ЛІГА: ЗАКОН». «Інтерактивна бухгалтерія» – це не просто видання, а сукупність додаткових сервісів для користувача, таких як «Особистий асистент», «Мої документи», персональні консультації. *Періодичність виходу*: щодня в робочі дні. *Мовні версії*: українською та російською мовами. *Можливості «Інтерактивної бухгалтерії»*: моніторинг законодавства 24 години на добу. Читачі першими довідаються про зміни в законодавстві та нормативних документах; аналітика та роз'яснення актуальних тем; актуальна база необхідних нормативних документів від компанії «ЛІГА: ЗАКОН»; сотні консультацій, наданих представниками Державної фіскальної служби, Мінсоцполітики, Пенсійного фонду України, Держказначейства, Держфінінспекції, соціальних фондів та інших органів влади; професійні персональні консультації; бланки, форми, довідники (усі необхідні для роботи документи); «Особистий асистент» допоможе знайти потрібний нормативний

документ, бланк звітності або первинний документ, підібрати аналітичні матеріали на тему, що цікавить; сервіс «Мої документи» дає змогу створювати особисті каталоги й добірки статей, коментарів та інших документів, необхідних їм у повсякденному професійному житті.

ІІІ. Сервіси моніторингу та аналізу [26]

1. **«CONTR AGENT»**

Система дає змогу за кілька хвилин перевірити свого партнера й одержати про нього таку інформацію: форма власності; основний вид діяльності; П. І. Б. директора; контактні дані; стан підприємства; оголошення про банкрутство; судові рішення, у яких згадано контрагента; податковий борг підприємства; про планові перевірки; аналітика фінансової благонадійності контрагента й інформація про санкції, запроваджені щодо нього.

Система надає можливість поставити підприємство на моніторинг: «CONTR AGENT» перевірятиме обрані компанії в різних базах, надасть оперативну інформацію про події, пов'язані з банкрутством або судовими рішеннями щодо обраних контрагентів, на пошту та в інтерфейсі користувача.

2. **«VERDICTUM»**

Система аналізу судових рішень «VERDICTUM» – спеціалізований багатофункціональний продукт для підприємств, діяльність яких періодично чи постійно пов'язана з необхідністю захисту своїх інтересів у суді. Продукт потрібний фахівцям, які бажають бути в курсі судової практики щодо спірних питань законодавства. Містить інноваційні пошукові алгоритми та інструменти опрацювання, аналізу й класифікації текстів, що значно спрощують роботу в багатомільйонному масиві судових рішень. *Періодичність оновлень*: щодня. *Можливості «VERDICTUM»*: допоможе сформувати власну правову позицію та продемонструє позиції судів у тотожних справах чи щодо суперечливих моментів законодавства; це інструмент, який у декілька разів скоротить час на пошук і добирання судової практики завдяки унікальним алгоритмам пошуку та вбудованим фільтрам; дає змогу за лічені секунди, використовуючи 14 різних параметрів, добирати справи за схожими критеріями для аналізу й прийняття рішень; показує хронологію проходження справи різними інстанціями; дає змогу працювати з НПА, згаданими в текстах рішень, завдяки інтеграції в платформу «ЛІГА: ЗАКОН».

3. **«SMS МАЯК»**

Фізичним і юридичним особам сервіс дасть можливість відстежувати зміни статусу будь-якого об'єкта нерухомості за номером у Державному реєстрі речових прав на нерухоме майно, а також поінформує в разі його зміни (без зазначення суті зміни).

Власникові нерухомого майна сервіс дасть змогу отримувати повідомлення про будь-які реєстраційні дії щодо його нерухомого майна на ранніх стадіях. «SMS-Маяк» сповістить про факт подання, суть заяви на зміну статусу об'єкта, а також про прийняття рішення щодо зміни статусу.

IV. Сервіси електронної звітності та документообігу [26]

«REPORT»

Онлайн-сервіс створення, подання й зберігання електронної звітності для компаній різних сфер діяльності та приватних підприємців на будь-якій системі оподаткування. *Періодичність оновлень*: щодня. *Мовні версії*: українською мовою. *Можливості «REPORT»*:

– Економія часу та матеріальних ресурсів.

– Простий, зручний і функціональний інтерфейс.

– Безпека передачі даних за допомогою сертифікованого сервісу.

– Форми відповідають затвердженому формату контролюючих органів України.

– Працює онлайн з усіма ОС без додаткових інсталяцій.

– Захищений хмарний архів зберігання.

– Підказки при заповненні форм.

– Імпорт документів (звітів, квитанцій).

– Дає змогу подавати звітність за 5 платниками податків у межах одного доступу.

– Безкоштовна технічна підтримка, консультація та навчання по роботі із сервісом.

– Автоматичне оновлення сервісу й останніх форм звітів.

2.3.3. Правова система «Нормативні акти України»

Дещо з історії та особливості комп'ютерних правових систем НАУ

Перша комп'ютерна правова система «Нормативні акти України» була розроблена у вересні 1991 року на замовлення Верховної Ради України. Тоді ще DOS-версія системи вміщувалася на 5 дискетах і містила кілька тисяч законодавчих актів. Але вже тоді були закладені основи побудови структури бази даних, функціональні можливості, які притаманні системам НАУ і сьогодні [10; 25].

З того часу продукт зазнав багато модифікацій: розширювався інформаційний склад бази даних, розроблялося нове програмне забезпечення під більш сучасні платформи операційних систем, були випущені системи НАУ з базами законодавства в перекладах англійською мовою, з базою судових рішень.

На сьогоднішній день правові системи НАУ мають заслужену репутацію, як надійний довідковий та аналітичний інструмент для юристів та інших фахівців, що використовують в роботі законодавство України – керівників підприємств, бухгалтерів, кадровиків і т. ін.

Це стало можливим завдяки постійному розвитку «трьох китів» – ***трьох складових будь-яких правових систем***, без яких вони були б малоефективні:

1. *Інформаційне наповнення* – це повна законодавча база України (близько 550 тис. документів):

– регіональне законодавство (документи обласних рад і держадміністрацій);

– перспективне законодавство (тексти законопроектів ВРУ);
– судова практика;
– аналітичні та довідкові документи (консультації, нормативні таблиці, бланки звітності, типові документи, каталог оголошень про банкрутство, словник законодавчих термінів, довідник органів влади та ін.);
– інтегрована з законодавством України база судових рішень;
– база перекладів законодавства англійською мовою.

2. *Пошук інформації* – це 6 різних видів пошуку:

1) експертний пошук (враховує форми слів, синоніми, близькі слова, компонує знайдені документи за релевантністю запиту);
2) пошук за реквізитами (враховує 10 параметрів, дозволяє провести попередній підрахунок);
3) пошук за словами в тексті;
4) пошук за контекстом у назві;
5) пошук за контекстом в тексті (шукає цифрові та символьні контексти);
6) пошук за датою/інтервалом дат.

Існують додаткові пошуки серед знайдених документів: фільтрація потрібної інформації; навігація по структурі знайденого списку документів за видавниками; 3 види сортування в знайденому списку.

3. *Обробка інформації* – це загальні дані про документ (реквізити, опублікування, історія внесених змін, коментарі):
– навігація по структурі документа;
– пошук слів або контекстів всередині тексту;
– перегляд минулих і майбутніх редакцій;
– пошук змін в тексті документа;
– автоматичне порівняння редакцій на будь-яку дату змін;
– зв’язки документа (інші НПА, судова практика, законопроекти, терміни, консультації, бланки та ін.);
– перехід в інші документи по гіперпосиланням в тексті;
– добірка судових рішень до документу або його статті;
– відсилання із судових рішень на норми права постатейно, з урахуванням діючої дати;
– зв’язки судових рішень в процесі проходження по інстанціям;
– поставка документу або судового рішення на контроль змін;
– маркер і закладки в тексті;
– виведення на друк;
– експорт в Word, буфер, файл, у власну БД тощо.

Причини появи в 2007 році продукту «МЕГА-НАУ»

З червня 2006 року почав функціонувати Єдиний державний реєстр судових рішень, і користувачі отримали доступ до значного обсягу інформації. Оскільки вільне відтворення текстів судових рішень, в тому числі в електронних БД, було прописано у Законі України «Про доступ до судових рішень», природним чином виникла ідея створення вибіркової бази судових рішень, орієнтованої на аналіз судової практики та інтегрованої із

законодавчою базою України. Крім «звичного» багаторічного забезпечення користувачів законодавчою базою України, розробники НАУ поставили мету надати практикуючим юристам унікальний інструмент для аналізу та узагальнення судової практики.

З урахуванням зауважень і побажань в ***продукті «МЕГА-НАУ»*** були реалізовані наступні ***новації*** [25]:

– *офлайн доступ (без підключення до інтернету)* – база даних судових рішень, як і нормативно-правова база, працює в офлайн варіанті, тобто встановлюється на сервері/комп'ютері всередині організації. Це гарантує всім без обмеження кількості користувачам постійний доступ до інформації, а також забезпечує надійний зв'язок (інтеграцію) цих баз даних;

– *деревовидна структура бази* – для чіткої візуалізації, полегшення навігації і пошуку судові рішення структуровані у вигляді дерева за розділами Суди / Дата / Номер;

– *додаткові види пошуку* – пошук за реквізитами розширений параметрами «Позивач», «Відповідач». Для параметра «Суддя» сформований список суддів;

– *зв'язки судових рішень (історія проходження)* – проаналізувати судову практику (визначити "долю" рішення) допомагає опція зв'язків з іншими судовими рішеннями в процесі проходження інстанціями, а також з рішеннями, що посилаються одне на одне;

– *зв'язки з НПА* – інтеграція з нормативно-правою базою дозволяє з тексту рішення миттєво за гіперпосиланням відкривати текст НПА з позиціонуванням на конкретній статті і з урахуванням редакції документу на дату прийняття рішення;

– *добірки судових рішень до статей НПА* – одночасно з цим надана можливість з тексту НПА постатейно робити добірки судових рішень, в тексті яких є посилання на дану статтю;

– *контроль рішень* – судові рішення в «МЕГА-НАУ» можна поставити на контроль, що дозволяє відстежувати появу нових рішень, пов'язаних з контрольованим;

– *власна база рішень* – знайдені рішення можна зберігати в окремій базі. Це дозволяє користувачам створювати власні аналітичні добірки з урахуванням спеціалізації діяльності;

– *сервіс «Моніторинг контрагентів»* – наявність в нормативній базі інформаційного розділу «Каталог оголошень про банкрутство» і база судових рішень надали можливість розробити додатковий сервіс «Моніторинг контрагентів». Він дозволяє контролювати за кодом ЄДРПОУ «судову біографію» та ризики банкрутств клієнтів, постачальників, підрядчиків та інших осіб, з якими веде справи організація;

– *сервіс «Машина часу» (для нормативно-правової бази)* – унікальний сервіс, який дозволяє переносити не просто окремі документи, а всю нормативно-правову базу у минуле. Склад документів, їх статус та поточна

редакція встановлюються на вказану користувачем дату. Документи, які набули чинності після цієї дати, не відображаються. Відповідно налаштовуються зв'язки та гіперпосилання документів.

Оскільки продукт з самого початку розроблявся не як аналог реєстру, а в якості інструменту для аналітичної роботи, було прийнято рішення відсіювати малоінформативні для аналізу судової практики документи (наприклад, ухвали про перенесення / скасування засідання, численні однотипні судові рішення тощо), значний обсяг яких надходить переважно з місцевих судів першої інстанції. Така фільтрація дозволяє зменшити обсяг надходження документів приблизно на 70 %, що істотно прискорює пошуки необхідних рішень і полегшує обслуговування (оновлення інформації) бази даних.

Переваги продукту «МЕГА-НАУ» [25]:

1. *Понад 12 мільйонів документів.*

«МЕГА-НАУ» унікальна не тільки за обсягом інформації – понад 11 млн. судових рішень і 850 тис. нормативних актів, але і системою зв'язків, що інтегрує судові рішення та нормативні акти в єдиний аналітичний комплекс, а динаміка проходження справ різними судовими інстанціями дозволяє ретельно підготуватися до судового засідання.

Надана законодавча та консультативно-довідкова інформація дозволяє забезпечити потреби також бухгалтерів, кадровиків та інших фахівців підприємства. Кількість користувачів в локальній мережі не обмежується.

2. *Інтелектуальний пошук*.

Для роботи з великою кількістю інформації розроблено експертний пошук з урахуванням форм слів, синонімів, близьких слів, перевіркою запиту на помилки та відсортуванням результатів пошуку за релевантністю.

3. *Унікальні сервіси:*

– «Моніторинг контрагентів».

– «Машина часу».

– «Майбутні редакції документів».

4. *Незалежність і мобільність*.

Робота «МЕГА-НАУ» не залежить від зовнішніх умов і наявності Інтернету – система працює швидко і безперебійно на будь-якому комп'ютері, а для великих підприємств дозволяє використовувати одну систему для всіх підрозділів – мережевий варіант розрахований на необмежену кількість осіб.

Зручність і унікальність «МЕГА-НАУ» ще й у тому, що система легко встановлюється на зовнішній USB-носій або планшет під Windows 8.

5. *Конфіденційність*.

«МЕГА-НАУ» забезпечує абсолютну конфіденційність роботи тому, що працюєте з базами, що встановлені на сервері Вашої організації, на відміну від інших систем, які пропонують доступ до власних серверів через Інтернет. Відомо, що запит, зроблений в Інтернеті, залишається там назавжди. Зацікавлені особи можуть перевірити Ваші пошукові запити, наприклад, які справи і якого судді Ви шукаєте.

6. *Зручність та технологічність.*

Легкість в опануванні та використанні системи. Помірні вимоги до ресурсів комп'ютера. Простий супровід системи, що не потребує спеціального персоналу.

Розглянемо сучасні ***продукти «МЕГА-НАУ» ТОВ «Інформтехнологія»*** (http://www.nau.ua) (рис. 2.1):

I. *«НАУ-ЕКСПЕРТ».*

II. *«МЕГА-ПРЕЦЕДЕНТ».*

III. *«IPLEX.ПРОФІ.XL».*

Рис. 2.1. Продукти «МЕГА-НАУ» (http://www.nau.ua)

I. «НАУ-ЕКСПЕРТ» (система перевірена часом!) [25]

«НАУ-ЕКСПЕРТ» – універсальна правова система, що завоювала досить велику популярність у користувачів. Це обумовлено тим, що інформаційний склад бази розрахований на найширшу категорію спеціалістів (керівники підприємств, юристи, бухгалтери, менеджери з персоналу) та інше:

– *Актуальна правова інформація* – повна нормативно-правова база, судова практика, аналітика, консультації, погляди, роз'яснення, моніторинги і довідники, бланки звітності, типові документи, зразки правочинів та цивільно-правових договорів, та багато іншого.

– *Багаторічний досвід* – 30 років на ринку, супровід тисяч користувачів, участь у міжнародних проектах та державних замовленнях.

– *Надійні програми* – невимогливі до ресурсів комп'ютера, надійна система контролю оновлень інформації в НАУ, безперебійна робота в мережі без обмеження кількості користувачів.

– *Інформаційний склад* («Нормативно-правові акти»; «Регіональна база»; «Судова практика»; «Консультації»; «Проекти законів»; «Словник термінів»; «Бланки документів»; «Каталог банкрутств»; «Зведені таблиці»; «Довідник органів влади»).

– *Технічні вимоги* (Windows NT, 2000, XP, Vista, 7; оперативна пам'ять від 512 Мбайт; процесор від Pentium 4; дисковий простір від 6 Гбайт) (для USB-версії: USB-носій обсягом від 8 Гбайт; порт стандарту USB 2.0; файлова система USB-носія – NTFS).

– *Унікальні сервіси, які надає тільки «НАУ-ЕКСПЕРТ»*: 1) надтонкий контекстний пошук (реалізований тільки в «НАУ»); 2) «Машина часу» – дозволяє переносити всю нормативно-правову базу у минуле (склад документів, їх статус і поточна редакція встановлюються на вказану дату); 3) USB-версія «НАУ» – всю систему можна записати на флешку або на USB-диск і працювати на будь-якому комп'ютері.

II. «МЕГА-ПРЕЦЕДЕНТ» (відібрана судова практика!) [25]

Правова система «МЕГА-Прецедент» – це інноваційний аналітичний продукт, що не має аналогів. Система розроблена з урахуванням побажань користувачів: юридичних фірм та приватно практикуючих юристів. Вона призначена для ґрунтовної підготовки юриста чи адвоката до судового засідання.

Переваги «МЕГА-Прецедент»:

– *Обрана судова практика*. До складу «МЕГА-Прецедент» увійшла професійна добірка найбільш вагомих судових рішень, яка складається з понад 1 400 000 судових рішень, що пройшли шлях від нижчих до вищих судових інстанцій та мають власну історію. В історії справи відображаються інші рішення, на які є посилання з поточного. Крім того, судові рішення мають прямі та зворотні зв'язки з НПА. Це дозволяє проаналізувати судову практику та обрати єдиний вірний шлях для вирішення власної судової справи.

– *Компактність*. Поєднання значного обсягу вагомої судової практики з компактними техніко-економічними показниками – система займає небагато місця на диску, швидко оновлюється, а також допускає роботу необмеженого числа користувачів у локальній мережі.

– *Мобільність*. Система може бути встановлена на USB-носій (флешку), а отже працювати та оновлюватись на будь-якому комп'ютері.

– *Інформаційний склад* («Судові рішення», які обираються за об'єктивними критеріями; «Аналітично-правова база «НАУ-Експерт»»).

– *Технічні вимоги* (Microsoft Windows NT / 2000 / XP / 2003 Server / Vista/ Linux; оперативна пам'ять: від 500 Мбайт (для Vista від 1 Гбайт); процесор: не нижче за Pentium IV 3 Ггц; дисковий простір від 10 Гбайт) (для USB-версії:

USB-носій обсягом від 16 Гбайт; порт стандарту USB 2.0; файлова система USB-носія – NTFS).

ІІІ. «ІРLEX.ПРОФІ.XL» (надсучасна правова система!) [25]

«ІРLEX.ПРОФІ.XL» – це програми і бази даних законодавства України.

Переваги «ІРLEX.ПРОФІ.XL» за функціональністю:

– *Актуально без зусиль* – всі бази знаходяться на серверах компанії, тому завжди актуальні та повні. У користувача на пристрої – тільки невеличка програма. Для роботи потрібен Інтернет.

– *Судову базу включено* – до складу системи входить база судових рішень з суттєво розвиненими сервісами.

– *Встановлюється і працює всюди* – з системою можна працювати на всіх власних пристроях: комп'ютері, планшеті, смартфоні.

– *Працюють на всіх популярних платформах* (Windows, Linux, MacOS, Android, iOS).

– *Мобільне законодавство* (для юриста, бухгалтера, керівника). Станом на сьогодні кількість встановлень понад 350 000.

– *Легкість в роботі* (встановити за 1 хв.; підключитися за 2 хв.; навчитися за 3 хв.).

– *Потужність в роботі* (сотні готових рішень, аналогів не існує).

Переваги «ІРLEX.ПРОФІ.XL» з точки зору користувачів:

– *Юристи* – «Контроль змін» («Актуальна правова база», «Календар редакцій», «Моніторинг законопроектів», «Регіональні акти»), «Судова практика» («База судових рішень», «Правові позиції Верховного суду України», «Калькулятори штрафів і зборів», «Приклади позовних заяв»), «Договірна робота» («Перевірка юросіб та ФОП», «Зразки та приклади договорів», «Моніторинг контрагентів»).

– *Бухгалтери* – «Консультації» («Журнал Дебет-Кредит», «Податкові запитання-відповіді», «Оперативна аналітика», «Огляд судової практики»), «Інструменти» («Калькулятори зарплати, відпусток», «Бланки звітності», «Календар бухгалтера»), «Довідники» («Курси, індекси, норми», «Проводки», «Стандарти бух обліку»).

– *Керівники* – універсальність (забезпечення всього персоналу правовою базою в офісі на звичайних комп'ютерах та поза межами офісу на мобільних пристроях), надійність (мобільні системи на порядок безпечніші ніж онлайн-сервіси та значно стабільніші ніж офлайнові системи), ефективність (дуже висока якість системи в поєднанні зі спеціальними корпоративними тарифами забезпечує до 300 % рентабельності на рік).

2.3.4. Інформаційно-пошукова система «Законодавство України»

ІПС «Законодавство України» є сучасним і простим засобом для роботи з правовою інформацією [3; 9; 10; 12; 24]. Система має потужний пошуковий апарат та різноманітні засоби відображення документів, кількість яких станом на 14.03.2024 містить 274 781 документів.

Вона містить: 1) документи органів влади України (Президента України, ВРУ, КМУ, Конституційного Суду України, Верховного Суду України, міністерств та відомств); 2) міжнародні угоди; 3) деякі нормативні документи органів влади; 4) документи регіонального законодавства [30].

Актуалізація БД здійснюється щоденно. База даних «Законодавство України» має інформаційний характер і не є офіційним друкованим виданням. Вона використовується згідно із Положенням про вебресурси ВРУ [30].

Вкладка «Законодавство» офіційного вебпорталу інформаційно-пошукової системи «Законодавство України» містить розділи: «Законодавство України»; «Пошук за реквізитами»; «Надходження законодавства»; «Міжнародні документи»; «Популярні документи»; «Первинні законодавчі акти»; «Розподіл за комітетами ВР»; «Анотації англійською мовою»; «Термінологія законодавства» тощо (рис. 2.2) [24].

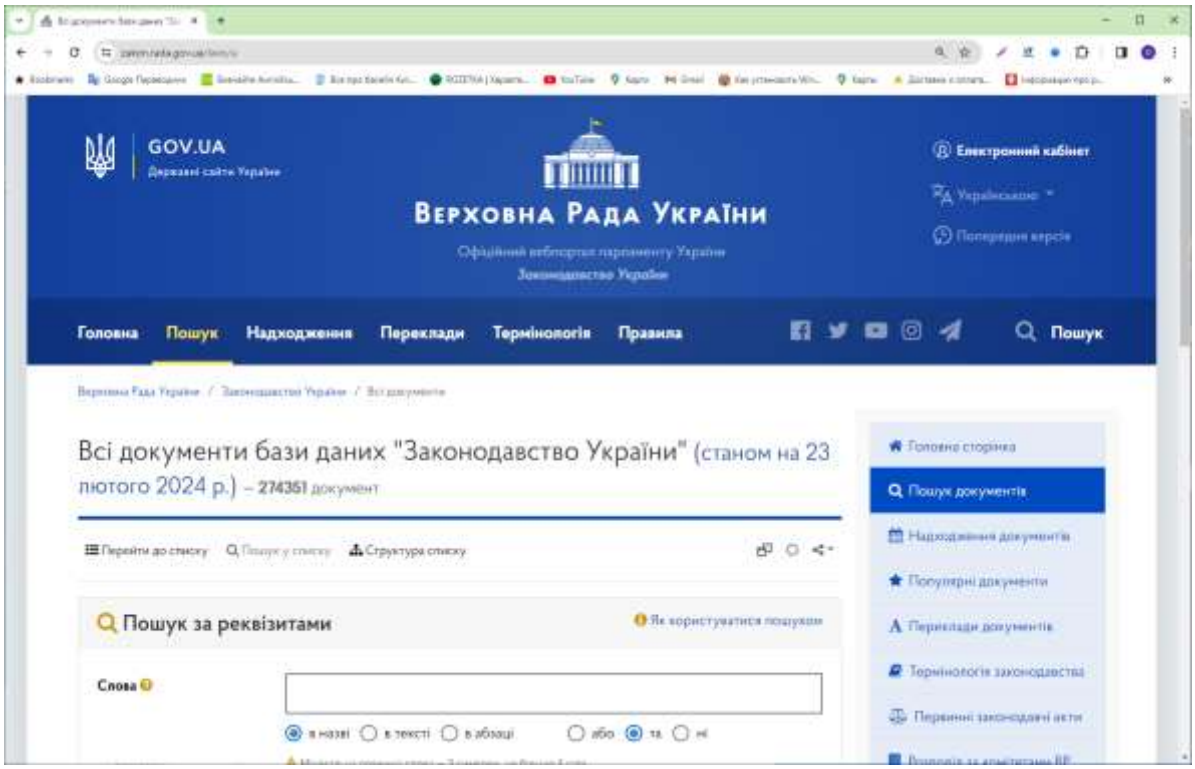


Рис. 2.2. Вебсторінка «Законодавство» офіційного вебпорталу ІПС «Законодавство України» (http://zakon.rada.gov.ua/laws/a)

Унікальним інформаційним ресурсом ІПС є постійно актуалізований *термінологічний словник законодавства України* (станом на 23.02.2024 містить 95 876 термінів), які згруповані за алфавітом (рис. 2.3). Найбільше термінів містять: «П» (8004), «С» (4964), «В» (4190).

Станом на 23.02.2024 ІПС «Законодавство України» містить 274351 документ.

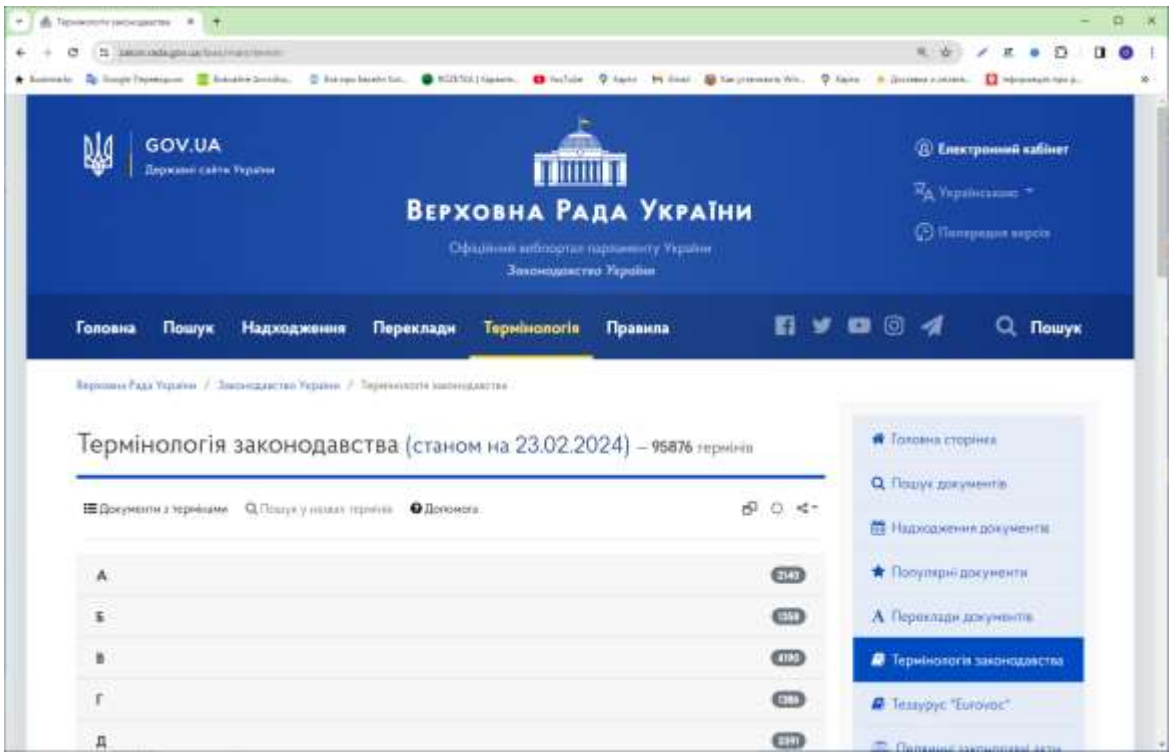


Рис. 2.3. Вебсторінка «Термінологія законодавства» офіційного вебпорталу ІПС «Законодавство України» (http://zakon.rada.gov.ua/laws/main/term)

Головна сторінка розділу **«Законодавство України»** містить підрозділи:

– ***«Види документів:»*** Кодекси України – 46; Закони України – 7 707; Постанови – 86 274 (станом на 23.02.2024)

– ***«Структура бази даних:»*** "*Видавники документів*" (ВРУ – 28 747; Президент України – 45 982; КМУ – 83 814 (станом на 23.02.2024).

– ***«Універсальний пошук:»*** (пошукова система дозволяє швидко знайти документи, як за реквізитами, так і за контекстом).

Використовуючи підрозділи «Групи документів:», «Структура бази даних:» головної сторінки розділу «Законодавство України» можна по списках здійснювати пошук необхідних документів.

Крім того, існує можливість з головної сторінки розділу **«Законодавство України»** перейти до рубрик меню: «Пошук документів»; «Найновіші надходження»; «Нові надходження»; «Популярні документи»; «Анотації документів»; «Документи за видавниками»; «Міжнародні документи»; «Первинні законодавчі акти»; «Документи комітетів ВР»; «Довідкова інформація»; «Замовлення надходжень»; «Термінологія законодавства»; «Альтернативний пошук» тощо.

Розглянемо можливості розділу «Пошук за реквізитами» (рис. 2.4) [27].

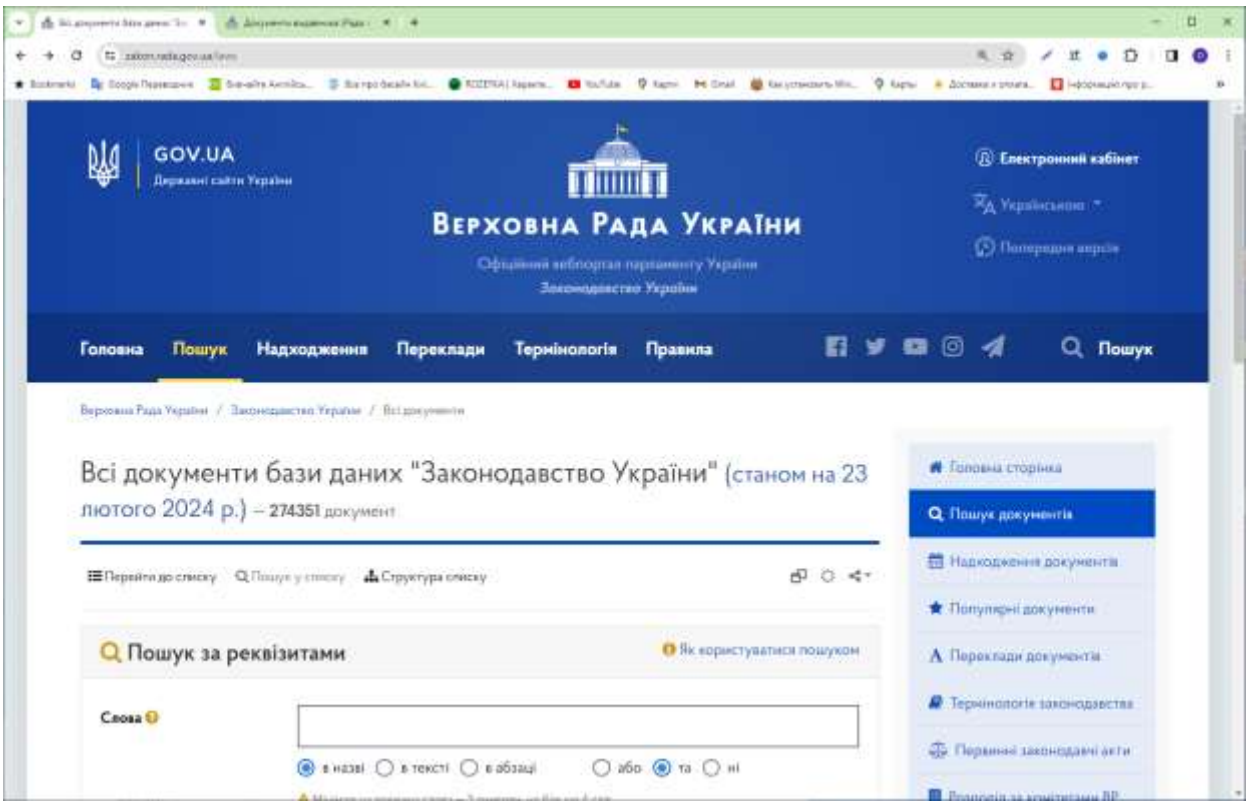


Рис. 2.4. Вебсторінка «Пошук за реквізитами» офіційного вебпорталу ІПС «Законодавство України» (http://zakon.rada.gov.ua/laws)

Вебсторінка «Пошук за реквізитами» містить такі *інформаційні поля* (рис. 2.6): «Слова», «Видавники», «Види документа», «Дата прийняття», «Номер документа», «Р. номер Мін'юсту», «Інше».

Розглянемо ***можливості інформаційних полів*** вебсторінки «Пошук за реквізитами» ***для пошуку документів*** [27].

Для пошуку документів *за словами* необхідно ввести одне або декілька слів у поле, що знаходиться праворуч від назви «**Слова**». Під «словом» розуміється слово або його початкова частина. Пошук виконується в документі «**в назві**», «**в тексті**», або одночасно і в назві, і в тексті («**всюди**»). При пошуку за декількома словами вони поєднуються одним з таких логічних сполучників: «**або**», «**та**», «**ні**».

Вимоги до пошукового запиту:

1) в словах тільки українські (або рос.) літери, мінімальна довжина слова **3** символи;

2) слова розділяються проміжками;

3) можна вводити початок слова (наприклад: **юрид***) або слово точно (**юрист!**);

4) за умовчанням встановлено логічний сполучник «**та**», але можна використовувати такі сполучники:

– «**та**» – всі вказані слова повинні бути в тексті (наприклад: **+юридична! +діяльність!**);

– «**або**» – будь-яке з вказаних слів може бути в тексті (наприклад: **~угод* ~догов***)

– «**ні**» – ні одне з вказаних слів не повинно бути в тексті (наприклад: **-внесення* -змін!**)

При пошуку слід враховувати, що деякі документи в базі даних є російськомовними, проте назви документів завжди подаються тільки українською мовою. Таким чином, при пошуку за назвою слід завжди вводити слова українською мовою.

Для уточнення пошукового запиту можна вказати додаткові реквізити, такі як: «Видавник», «Тип документа», «Дата прийняття», «Номер документа», «Р. номер Мін'юсту».

Реквізити в полі «**Видавник**» та «**Тип документа**» вибираються зі *списку*, що знаходиться праворуч. За умовчанням пошук виконується за всіма видавниками та всіма типами документів.

Якщо *відома дата прийняття документа* або необхідно знайти документи *за певний часовий проміжок*, то введіть відповідні дані у поле «**Дата прийняття**» Дані можна вводити за допомогою переліків років, місяців та чисел або за допомогою календарика, який викликається натисканням білої стрілочки, що знаходиться праворуч.

Якщо дата вводиться неповністю (наприклад, введено тільки рік, а місяця і числа немає), то пошук, природно, проводиться за присутньою частиною дати (наприклад, за вказаний рік). За умовчанням, невказані частини дати в зворотному порядку, починаючи з року, встановлюються поточними. Необхідно відмітити, що завдяки сформованому індексу за датою документів, пошук по всій базі даних майже миттєвий!

Якщо в полі поряд з датою встановлено значення «**дорівнює**», то виконується пошук документів, що були прийняті одного року, місяця або конкретного дня. Крім цього, можна виконати пошук документів, які були прийняті до вказаної дати включно (значення «**аніше за**»), знайти документи, які були прийняті після вказаної дати включно (значення «**пізніше за**»).

Пошук за *номером документа* або *номером його реєстрації в Мін'юсті* найшвидший і найточніший. При такому пошуку не обов'язково вводити номер повністю – достатньо знати його фрагмент.

За допомогою спеціального списку, який знаходиться ліворуч, можна вибрати один із режимів пошуку: **«починається»**, **«дорівнює»**, **«входження»**. За умовчанням пошук відбувається за входженням фрагмента номера. Відповідно, в разі, якщо відомий тільки початок номера, то необхідно вказати *«починається»*. Якщо номер відомий точно, то встановіть значення *«дорівнює»*.

Кожний список документів, що утворюється при роботі з інформаційно-пошуковою системою «Законодавство України» можна розкласти за *структурою* (посилання знаходиться в верхній частині сторінки під заголовком списку та позначено), яка поділяється на такі *основні групи*: «Видавники документів»; «Міжнародні видавники»; «Види документів»; «Роки прийняття»; «Стан документів» [24; 27].

Для списків *«Нових надходжень»* (за 30 останніх днів – 558 документа), *«Найновіші надходження»* (на 23 лютого 2024 р. – 16 документів), *«Документи за видавниками»*, *«Міжнародні документи»* також існує можливість подивитися кількість документів на кожну з присутніх тем тематичного класифікатора [24; 27].

Структура списку документів – дуже корисна інформаційна функція системи. Одразу можна побачити кількість документів для кожного елемента в кожній підгрупі та відкрити цей список без використання пошукової форми просто натиснувши мишкою на будь-який підсвічений елемент (видавник, тип або рік). Крім того, якщо структура виконується на всій базі або на великому списку документів, групи видавників або тем документів можуть складатися з великої кількості елементів. Тому зроблено пошук у структурі за будь-якою частиною слів елементів. Якщо набрати деякі слова (наприклад **«міністерство»**) в пошуковій формі під списком структури та натиснути кнопку, то знайдені елементи будуть виділені іншим кольором та перемістяться в верхню частини своєї підгрупи [27].

«Альтернативний пошук» головної сторінки розділу «Законодавство України» – контекстний пошук в документах з сайту ВРУ можна здійснювати за допомогою відомих пошукових механізмів, таких як Google, Яndex або Мета. Але *цей пошук відрізняється від вбудованого*: пошукові запити треба набирати повністю, не скорочуючи слів. Вирази будуть враховувати всі комбінації слів згідно із морфологією та близькості між ними. Сортування результатів також відрізняється – найбільш точні за запитом документи будуть знаходитись вгорі списку. Всі результати будуть відкриті у новому вікні.

«Популярні документи» головної сторінки розділу «Законодавство України» дозволяє переглянути популярні документи [24]. Наприклад:

1. Статистика за документами (*візити*) (кількість документів за період 01-13 квітня 2018 р. – 122 735) надає список таких популярних документів:

1) Цивільний процесуальний кодекс України (Закон від 18.03.2004 № 1618-IV) – 20 327.

2) Цивільний кодекс України (Закон від 16.01.2003 № 435-IV) – 20 079.

3) Кримінальний процесуальний кодекс України (Закон від 13.04.2012 № 4651-VI) – 18 146.

4) Кримінальний кодекс України (Закон від 05.04.2001 № 2341-III) – 15 076.

5) Податковий кодекс України (Закон від 02.12.2010 № 2755-VI) – 12 330.

6) Конституція України (Закон від 28.06.1996 № 254к/96-ВР) – 12 171.

7) Кодекс законів про працю України (Закон від 10.12.1971 № 322-VIII) – 12 052.

8) Кодекс України про адміністративні правопорушення (статті 1-212-21) (Закон від 07.12.1984 № 8073-X) – 11 975.

9) Кодекс адміністративного судочинства України (Закон від 06.07.2005 № 2747-IV) – 9 845.

10) Про виконавче провадження (Закон від 02.06.2016 № 1404-VIII) – 8 631.

11) Земельний кодекс України (Закон від 25.10.2001 № 2768-III) – 8 249.

12) Про запобігання корупції (Закон від 14.10.2014 № 1700-VII) – 7 817.

2. Статистика за документами (*сторінки*) (кількість документів за період 01-13 квітня 2018 р. – 122 735) надає список таких популярних документів:

1) Податковий кодекс України (Закон від 02.12.2010 № 2755-VI) – 302 758.

2) Цивільний кодекс України (Закон від 16.01.2003 № 435-IV) – 191 038.

3) Кримінальний процесуальний кодекс України (Закон від 13.04.2012 № 4651-VI) – 177 641.

4) Цивільний процесуальний кодекс України (Закон від 18.03.2004 № 1618-IV) – 165 651.

5) Кримінальний кодекс України (Закон від 05.04.2001 № 2341-III) – 104 429.

6) Кодекс України про адміністративні правопорушення (статті 1-212-21) (Закон від 07.12.1984 № 8073-X) – 91 452.

7) Кодекс адміністративного судочинства України (Закон від 06.07.2005 № 2747-IV) – 71 230.

8) Господарський процесуальний кодекс України (Закон від 06.11.1991 № 1798-XII) – 53 531.

9) Кодекс законів про працю України (Закон від 10.12.1971 № 322-VIII) – 49 742.

10) Земельний кодекс України (Закон від 25.10.2001 № 2768-III) – 47 024.

11) Господарський кодекс України (Закон від 16.01.2003 № 436-IV) – 37 847.

12) Про виконавче провадження (Закон від 02.06.2016 № 1404-VIII) – 33 495.

13) Конституція України (Закон від 28.06.1996 № 254к/96-ВР) – 30 567.

14) Кодекс України про адміністративні правопорушення (статті 213-330) (Закон від 07.12.1984 № 8073-X) – 29 191.

15) Про запобігання корупції (Закон від 14.10.2014 № 1700-VII) – 27 159.

16) Сімейний кодекс України (Закон від 10.01.2002 № 2947-III) – 23 339.

Друк документів розділу «Законодавство України» за допомогою веббраузера має суттєві *обмеження* [27]. Основним з них є неможливість вибрати шрифт тексту документа та його розмір. Крім того, деякі веббраузери старих версій некоректно здійснюють друкування документів, а стандартний для Windows браузер Internet Explorer взагалі не показує документи розміром більше за кілька мегабайтів.

Тому рекомендується спочатку зберегти текст документа у файл, а потім відкрити його за допомогою стороннього редактора (наприклад, програми *Microsoft Word* чи *Open Office*) та здійснити друк відповідно до вказаних налаштувань. Якщо необхідно роздрукувати невелику частину документа, то можна спочатку виділити фрагмент тексту документа (мишкою, клавішами

Ctrl-A тощо) та зберегти у буфері обміну (комбінація клавіш *Ctrl-C*), після чого скопіювати збережений фрагмент тексту до редактора (*Ctrl-V*).

З урахуванням вищезазначеного для ***друкування документів*** рекомендується наступний *порядок дій* [27]:

– відкрити текст необхідного документа для перегляду;

– якщо текст документа представлено в текстовому форматі (кожний рядок як абзац), необхідно лівою кнопкою мишки натиснути на іконці  ;

– натиснути лівою кнопкою мишки на іконці  (Текст для друку);

– зберегти текст документа у файл, вибравши функцію *«Зберегти як»* та вибравши тип документа: *«Вебсторінка, повністю»* або *«Вебархив (єдиний файл)»*;

– знайти збережений файл та, натиснувши на ньому правою кнопкою мишки, вибрати пункт меню *«Відкрити з допомогою»*, наприклад, програми *Microsoft Word*.

Якщо ж здійснювати друк документів за допомогою механізмів, наявних у веббраузерах, рекомендується використовувати останні версії наступних браузерів: Google Chrome; Mozilla FireFox; Opera.

Особливості використання ІПС «Законодавство України» [29]:

1. Для отримання достовірної інформації при роботі зі сторінкою рекомендується користуватися *сучасними браузерами*: Internet Explorer версії 6.0+, Mozilla Firefox 2.0 та Opera 9 (обов'язково в параметрах безпеки браузера треба дати дозвіл на виконання javascript та отримання cookies). Старі браузери підтримуються частково – можливі деякі розбіжності та проблеми з відображенням шрифтів, таблиць, стилями та javascript.

2. Деякі документи занадто великі для нормального перегляду їх в повному обсязі у вікні браузера, тому вони *поділені на частини* – "сторінки" розміром приблизно по 60 Кбайт. Це прискорює відкриття документів та зменшує навантаження на сервер. Переглянути весь текст можна натиснувши "*Текст для друку*" у заголовку вікна тексту або картки.

3. Для *збереження документа в текстовому вигляді* необхідно його відкрити, натиснути  (*Текст для друку*), виділити текст всього документа (*Ctrl-A*) та скопіювати виділений текст в буфер обміну (*Ctrl-C*), перейти у будь-який текстовий редактор, вставити текст з буфера обміну (*Ctrl-V*) та зберегти його, як *«Текстовий файл* (*.txt)». Є можливість за допомогою автоматичного конвертора перетворити форматований документ у більш зручний текст для роботи. Для цього використовується кнопка , яка розташована в тексті документа на панелі інструментів.

4. ІПС працює на кількох незалежних серверах-дзеркалах (*zakon* та *zakon1*). Інформація в БД не відрізняється. Для стабільної роботи між ними відбувається рівномірне балансування навантаження. Коли на якомусь сервері проводяться регламентні роботи, користувачів автоматично переадресують на інший доступний сервер. Тому краще заходити з головної адреси.

5. В списках документів та в пошуковій формі представлено *скорочені назви видавників* для зменшення розміру сторінок. Повні назви видавників можна побачити в режимі «Структура списку».

6. Для того, щоб для документа подивитись *список пов'язаних з ним документів* потрібно відкрити картку або натиснути на відповідну іконку  чи пункт меню в верхньому меню вікна документа. Ще не всі документи мають визначені списки пов'язаних з ними документів, деякі списки – неповні. Нові зв'язки поступово додаються.

7. Для того, щоб побачити *проекти законів* в картці документа ВРУ (починаючи з 3 скликання) є посилання на картку законопроекту, яка має таку іконку  . Крім того, є спеціальний розділ «Законотворчість – Законопроекти» в головному меню сайту Верховної Ради України.

8. В списках документів показується багато реквізитів, тому для зручності визначення додаткової інформації щодо стану документів або їх популярності використовується *інший шрифт* та *колір* або *інші позначки*. Червоним кольором показано документи, які не набрали чинність, темно-сірим – які втратили. Виділено також картки, що знаходяться у розділі «Популярні документи».

9. Є деякі *особливості в пошуку документів*, які потрібно враховувати:

– шукайте слова в назвах документів тільки українською;

– в назвах немає слів «Закон про» або «одекс про» тощо, назви зразу починаються зі слова «Про» (наприклад, «Про мови»), а тип документа краще вказувати через спеціальне поле в картці;

– не заповнюйте зразу всі відомі Вам реквізити про документ, достатньо хоча б в одному помилитись, і результат буде нульовий;

– при контекстному пошуку не вказуйте широковживані слова (наприклад «про», «від», «України»), документів де вони зустрічаються багато;

– крім того, якщо вказуєте початкову частину слова, то включайте корінь слова повністю (наприклад, «дод вар» погано, краще «додан вартість»);

– використовуйте пошук на списках (декілька важливих списків знаходяться на головній сторінці) та користуйтесь «структурою списку».

10. На сайті «Законодавство України» використовується *система захисту від перевантаження*, що, зокрема, спричиняють програми автоматичного скачування великого об'єму інформації [30]:

– Надмірне використання ресурсів сервера з одного IP блокується системою на деякий час! Обмежена кількість сторінок, що відкриваються IP-адресою за хвилину. Не рекомендується перевантажувати сервер запитами, бо це потягне за собою закриття доступу на кілька хвилин. Після повторних та багаторазових блокувань доступ до сайту автоматично припиняється на більший час (3 доби).

– Складний контекстний пошук може бути перерваний за тайм-аутом через 10 сек. Якщо таке трапиться, оптимізуйте запит та спробуйте знову звернутися до сервера. Повідомлення про невдалий пошук частіше з'являється під час пікового навантаження (в період з 10 до 13 та з 14 до 17 годин).

– Тимчасові списки документів, що формуються під час пошуку, зберігаються в кеші запитів на сервері. Кількість файлів списків обмежена, тому вони можуть бути вилучені, а під час перегляду сторінок цього списку з'явиться повідомлення, що тимчасовий список не знайдено.

Таким чином, ІПС «Законодавство України» має такі ***інформаційні можливості***:

1. *Робота з документами* (пошук документів за реквізитами, ключовими словами, юридичним класифікатором, конкретними словами з підсвічуванням їх у знайдених текстах; друк документів або їх частин на будь-якому принтері; копіювання текстів / збереження документів у файл тощо).

2. *Сервісні функції* (перекладач українсько-російський або українсько-російсько-англійський; формування списків користувача; перегляд, сортування, виведення на друк або в файл списку знайдених документів тощо).

3. *Аналітичні функції* (аналіз статистики всієї бази або списків у необхідному розрізі; перегляд структури документа; контроль документів на предмет внесення змін; перегляд редакцій документів тощо).

Питання для самоконтролю

1. Головні нормативно-правові документи, що регулюють застосування інформаційних технологій у правозастосовній діяльності.
2. Основні міжнародні документи в сфері нормативно-правового регулювання інформаційних технологій у правозастосовній діяльності.
3. Роль та значення інформаційного права в сфері нормативно-правового регулювання інформаційних технологій у правозастосовній діяльності.
4. Становлення інформаційного законодавства України в сфері регулювання інформаційних технологій.
5. Нормативно-правові акти, де визначені поняття «інформація», «інформаційна технологія», «інформатизація».
6. Базові закони в сфері інформації та інформатизації.
7. Проблеми та перспективи національного законодавства в сфері регулювання інформаційних технологій.
8. Учасники правовідносин під час створення та використання інформаційних технологій у правозастосовній діяльності.
9. Досвід правового регулювання в сфері інформаційних технологій в країнах ЄС.
10. Основні напрями правового регулювання відносин, що пов'язані з Інтернет.
11. Поясніть значення термінів «інформаційна система», «інформаційний ресурс», «правова інформаційна система».
12. Основна мета, етапи розвитку та задачі інформаційних систем.
13. Основна мета та властивості правових інформаційних систем.
14. Класифікація правових інформаційних систем.
15. Основні результати використання правових інформаційно-пошукових систем в юридичній діяльності.

16. Загальна характеристика Єдиної інформаційно-правової платформи «Ліга: Закон».

17. Класифікація інформаційно-правових систем «Ліга: Закон».

18. Періодичні видання та довідники компанії «Ліга: Закон».

19. Сервіси моніторингу та аналізу, електронної звітності та документообігу компанії «Ліга: Закон».

20. Загальна характеристика ІПС «Нормативні акти України».

21. Новації та переваги продукту «МЕГА-НАУ» «Інформтехнології».

22. Поняття та переваги систем «НАУ-ЕКСПЕРТ», «МЕГА-Прецедент», «IPLEX.ПРОФІ.XL».

23. Загальна характеристика ІПС «Законодавство України».

24. Основні можливості пошуку документів в інформаційно-пошуковій системі «Законодавство України».

25. Можливості вебсторінки «Пошук за реквізитами» інформаційно-пошукової системи «Законодавство України» для пошуку документів.

26. Особливості використання ІПС «Законодавство України».

Практичні завдання до розділу ІІ

Практичне заняття № 2 (Час виконання: 2 години**)**

Мета заняття: поглибити практичні навички здобувачів щодо використання інформаційно-пошукових систем у сфері законодавства.

Завдання 1: Ознайомтесь з правилами роботи з базою ІПС «Законодавство України» (https://zakon.rada.gov.ua/laws/main/rules).

Які є *обмеження* в доступі до БД «Законодавство України»?

Завдання 2: Надайте відповіді на наступні питання шляхом копіювання тексту з відповідних законів/нормативних актів:

1. Законодавче визначення понять «*інформація*», «*види інформації за змістом*», «*інформація з обмеженим доступом*» (див. Закон України «Про інформацію»).

2. Що таке «*база даних*», «*електронні інформаційні ресурси*», «*засоби інформатизації*», «*інформаційно-комунікаційні технології*», «*цифрова технологія*»? (див. Закон України «Про Національну програму інформатизації»).

3. Що таке «*згода суб'єкта персональних даних*», «*обробка персональних даних*», «*персональні дані*» ? (див. Закон України «Про захист персональних даних»).

4. Які повноваження поліції у сфері інформаційно-аналітичного забезпечення? (див. Закон України «Про Національну поліцію»).

5. Зробити витяг п. 6 нормативно-правового акту за такими даними: *Видавник* «Кабінет Міністрів України»; *Дата прийняття* «листопад 2018 року»; *Номер документа* – «1024».

6. Зробити витяг п. 2 розділу 1 наказу МВС України № 676 від 03.08.2017.

7. Яку інформацію можна отримати з банків даних Інтерполу? (див. спільний наказ № 613/380/93/228/414/510/2801/5 від 17.08.2020).

8. Визначення терміну «*поліцейський*». Де і у яких нормативно-правових актах це зазначено? (див. «Термінологія законодавства» на вебпорталі ВРУ).

9. Визначення терміну «*інформаційна технологія*». Де і у яких нормативно-правових актах це зазначено? (див. «Термінологія законодавства» на вебпорталі ВРУ).

10. Визначення терміну «*катування*». Де і у яких нормативно-правових актах це зазначено? (див. «Термінологія законодавства» на вебпорталі ВРУ).

Завдання 3. Здійсніть результативний пошук двох осіб з двох різних інформаційно-розшукових обліків, розміщених на сайті mvs.gov.ua. Фотографії та реквізити знайдених осіб скопіюйте у вище створений файл docx.

Завдання 4. За допомогою інтернет посилання https://generator-online.com/qrcode/ згенеруйте QR код для однієї з вибраних осіб (що містить текстові реквізити особи) та скопіюйте ці коди у вище створений файл docx. За допомогою власного смартфона прочитайте інформацію, що міститься у QR коді в зашифрованому вигляді.

Список використаних і рекомендованих джерел

До п. 2.1, 2.2

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. *Урядовий кур'єр.* 1996. № 129–130.
2. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII.
3. Про науково-технічну інформацію : Закон України від 25 черв. 1993 р. № 3322-XII.
4. Про Національну програму інформатизації : Закон України від 1 груд. 2022 р. № 2807-IX.
5. Про Концепцію Національної програми інформатизації : Закон України від 4 лют. 1998 р. № 75/98-ВР.
6. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 лип. 1994 р. № 80/94-ВР.
7. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI.
8. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI.
9. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII.
10. Про основи національної безпеки України : Закон України від 19 черв. 2003 р. № 964-IV.
11. Про електронні комунікації : Закон України від 16 груд. 2020 р. № 1089-IX.
12. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV.
13. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5 жовт. 2017 р. № 2155-VIII.
14. Про авторське право і суміжні права : Закон України від 23 груд. 1993 р. № 3792-XII.
15. Про інформаційні агентства : Закон України від 28 лют. 1995 р. № 74/95-ВР.
16. Про телебачення і радіомовлення : Закон України від 21 груд. 1993 р. № 3759-XII.
17. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26.
18. Кодекс України про адміністративні правопорушення : Закон Української РСР від 7 груд. 1984 р. № 80731-X. *Відомості Верховної Ради Української РСР.* 1984. Додаток до № 51. Ст. 1122.
19. Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних : Указ Президента України від 24 верес. 2001 р. № 891.

20. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 лип. 2009 р. № 514.

21. Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю : Указ Президента України від 31 січ. 2006 р. № 80.

22. Про затвердження Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю : постанова Кабінету Міністрів України від 8 квіт. 2009 р. № 321.

23. Про електронний обмін службовими документами в органах виконавчої влади : постанова Кабінету Міністрів України від 17 лип. 2009 р. № 733.

24. Про затвердження Концепції технічного захисту інформації в Україні : постанова Кабінету Міністрів України від 8 жовт. 1997 р. № 1126.

25. Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади : постанова Кабінету Міністрів України від 10 верес. 2003 р. № 1433.

26. Про затвердження Порядку легалізації комп'ютерних програм в органах виконавчої влади : постанова Кабінету Міністрів України від 4 берез. 2004 р. № 253.

27. Про затвердження Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах : постанова Кабінету Міністрів України від 29 берез. 2006 р. № 373.

28. Про затвердження Концепції формування системи національних електронних інформаційних ресурсів : розпорядження Кабінету Міністрів України від 5 трав. 2003 р. № 259-р.

29. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України : наказ МВС України від 12 жовт. 2009 р. № 436 (втратив чинність).

30. Інформатизація управління в органах внутрішніх справ / [В. Г. Хахановський, П. П. Підюков, В. М. Смаглюк та ін.] ; за заг. ред. Я. Ю. Кондратьєва. Київ : НАВСУ, 2003. 215 с.

31. Системна інформатизація законотворчої та правоохоронної діяльності : монографія / [кер. авт. кол. М. Я. Швець ; за ред. В. В. Дурдинця та ін.]. Київ : Навч. кн., 2005. 639 с.

32. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / [В. М. Бутузов, В. Д. Гавловський, Л. П. Скалозуб та ін.] ; за ред. Б. В. Романюка, Є. Д. Скулиша. Київ, 2011. 404 с.

33. Сайти з законодавства. URL: www.rada.gov.ua ; http://www.nau.kiev.ua.

34. Національна академія внутрішніх справ : [офіц. вебпортал]. URL: http://www.naiau.kiev.ua.

До п. 2.3

Законодавчі та підзаконні нормативно-правові акти України

Основні

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР.

2. Про Єдиний державний реєстр нормативних актів : Указ Президента України від 27 черв. 1996 р. № 468/96.

3. Про затвердження Програми інформатизації законотворчого процесу у Верховній Раді України на 2012–2017 роки : постанова Верховної Ради України від 5 лип. 2012 р. № 5096-VI.

4. Про Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні» : постанова Верховної Ради України» від 3 лип. 2014 р. № 1565-VII.

Додаткові

5. Про внесення змін до Закону України «Про інформацію» : Закон України від 13 січ. 2011 р. № 2938-17.

6. Про Національну програму інформатизації : Закон України від 1 груд. 2022 р. № 2807-IX.

7. Про стратегію сталого розвитку «Україна-2020» : Указ Президента України від 12 січ. 2015 р. № 5/2015.

8. Про Рекомендації парламентських слухань на тему: «Про стан та законодавче забезпечення розвитку науки та науково-технічної сфери держави» : постанова Верховної Ради України від 11 лют. 2015 р. № 182-VIII.

9. Про Перелік автоматизованих систем інформаційно-технологічного забезпечення діяльності Верховної Ради України : розпорядження Голови Верховної Ради України від 1 лип. 2003 р. № 663.

Навчальна та наукова література

Основна

10. Кудінов В. А., Орлов Ю. Ю., Пакриш О. Є. Інформаційні технології в діяльності Національної поліції : навч. посіб. Київ, 2017. 100 с.

11. Кудінов В. А., Смаглюк В. М., Хахановський В. Г. Інформаційні технології в правозастосовній практиці : навч. посіб. Київ, 2015. 112 с.

12. Хахановський В. Г., Чукаєва А. В. Інформаційне право : підручник / за заг. ред. С. С. Чернявського. Київ, 2015. 216 с.

Додаткова

13. Ананьєв О. М., Бєлий О. І. Інформаційні системи і технології правової інформації : навч. посіб. Львів, 2013. 303 с.

14. Брикайло Л. Ф. Інформаційні технології пошуку, підготовки та обробки документів у юриспруденції: система «Ліга-Закон» : навч. посіб. Київ, 2008. 102 с.

15. Денісова О. О. Інформаційні системи і технології в юридичній діяльності : навч. посіб. Київ, 2004. 307 с.

16. Зацеркляний М. М. Інформаційні технології у правозастосовній діяльності. Харків, 2010. 332 с.

17. Інформатика в юридичній діяльності (частина 1) : підручник / [В. А. Іщенко, О. М. Грищак, В. А. Кудінов та ін.] / за заг. ред. В. А. Кудінова. Київ, 2016. 256 с.

18. Інформатика в юридичній діяльності (частина 2) : підручник / [В. А. Кудінов, І. М. Мельников, О. Є. Пакриш та ін.] / за заг. ред. В. А. Кудінова. Київ, 2017. 332 с.

19. Інформаційні технології в юридичній діяльності: базовий курс : навч. посіб. / [О. В. Співаковський, М. І. Шерман, В. М. Стратонов та ін.]. Херсон, 2012. 220 с.

20. Іщенко О. М., Черних С. П., Аршинов І. А. Від арифмометра до високих технологій (до 40-ї річниці створення інформаційної служби МВС України). Запоріжжя, 2012. Т. 1. 472 с.

21. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посіб. / [В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін.] / за заг. ред. В. Г. Іванова. Харків, 2010. 237 с.

22. Швець М. Я. Віхи становлення правової інформатики. *Віче*. 2012. № 18. С. 31–32.

23. Шерман М. І. Правова інформаційно-пошукова система «Ліга-Закон. Юрист» як засіб комп'ютерної підтримки навчання правових дисциплін. *Науковий часопис Національного педагогічного університету ім. М. П. Драгоманова*. 2011. Вип. 11 (18). С. 46–51. (Серія 2 «Комп'ютерно-орієнтовані системи навчання»).

Інтернет-ресурси

24. Верховна Рада України : [вебпортал]. URL: http://portal.rada.gov.ua.

25. Інформаційно-пошукова система «Нормативні акти України» : [вебпортал]. URL: http://www.nau.ua.

26. Ліга: Закон : [вебпортал]. URL: http://www.ligazakon.ua/ua.

27. Допомога «Як користуватись пошуком». URL: http://zakon2.rada.gov.ua/laws/main/help.

28. Журнал «Правова інформатика». URL: http://www.bod.kiev.ua/jurnal/index.htm.

29. Питання, що часто виникають, та відповіді на них. URL: http://zakon2.rada.gov.ua/laws/main/faq.

30. Правила роботи з базою даних «Законодавство України». URL: http://zakon2.rada.gov.ua/laws/main/rules.

РОЗДІЛ ІІІ
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В НАУКОВО-ПЕДАГОГІЧНІЙ ДІЯЛЬНОСТІ

3.1. Створення наукових і навчальних презентацій засобами Microsoft PowerPoint

Термін ***мультимедіа*** (лат. multum (багато) + medium (середовище, носій)) – комбінування різних форм представлення інформації (тексту, графіки, звуку, відео, анімації) та її обробки в єдиному об'єкті (файлі, носієві).

З точки зору використання комп'ютерної техніки це поняття можна визначити таким чином:

Мультимедіа – це комплекс апаратних і програмних засобів, що дозволяють користувачеві працювати в діалоговому режимі з даними різних видів (графіка, текст, звук, відео), організованими у вигляді єдиного інформаційного середовища. Наприклад, в одному об'єкті-контейнері (англ. container) може міститися текстова, аудіо, графічна та відео інформація, а також, можливо, способи інтерактивної взаємодії з нею.

Під терміном ***презентація*** (від англ. presentation – представлення, подання, показ) найчастіше розуміють суспільне представлення чогось недавно створеного, нового, ще невідомого аудиторії (наприклад, підприємства, нового продукту, проекту, товару тощо).

Під час виступу, для кращого сприймання аудиторією матеріалу, що презентується, як правило, використовують допоміжні матеріали: таблиці, плакати, малюнки, фотографії, відеофільми та іншу наочність. У наш час із цією метою почали застосовувати ***мультимедійні комп'ютерні презентації*** (надалі їх будемо називати просто презентаціями), створені за допомогою спеціальних програм.

Однією з таких програм є програма ***Microsoft PowerPoint*** – складова частина пакету Microsoft Office.

Презентація, створена за допомогою Microsoft Power Point, – це набір слайдів, що зберігаються у файлі спеціального формату. Слайд (від англ. to slide – повзти) може містити текст, графічні об'єкти (фотографії, таблиці, рисунки, діаграми, відеозаписи), звук, анімацію, елементи керування (кнопки, гіперпосилання). Презентацію можна демонструвати на екрані монітора або за допомогою мультимедійного комплексу (комп'ютер, проектор, аудіообладнання, екран чи інтерактивна дошка).

Презентації використовують під час доповідей на службових нарадах, лекціях, конференціях, семінарах, захистах проектів та наукових робіт. Якісно підібраний та оформлений матеріал значно підвищує інтерес слухачів та сприяє кращому розумінню та засвоєнню матеріалу.

Забезпечення сучасного рівня підготовки фахівців вимагає постійного удосконалення навчального процесу. Педагоги-новатори завжди

впроваджували новітні технології для підвищення ефективності та якості навчання. І якщо ви ставите перед собою амбітні завдання:

– істотно поліпшити якість навчального матеріалу;

– значно підвищити інтерес студентів до предмета;

– суттєво поліпшити розуміння і запам’ятовування навчального матеріалу;

– збільшити обсяг матеріалу, що викладається, при незмінній кількості або при зменшенні лекційних годин;

– підвищити свій рейтинг в очах студентів і колег тощо,

то виконати їх можна тільки в єдиний спосіб, застосовуючи в освітньому процесі сучасні інформаційні технології з використанням обчислювальної техніки і мультимедійних засобів. Це – так зване «електронне навчання» (е-навчання, e-learning), яке передбачає здійснення всіх процесів навчання в електронній формі. Для навчання, крім персональних комп’ютерів, зараз також широко використовуються мобільні пристрої, такі, як електронні книжки, планшети, мобільні телефони тощо. На всі пристрої навчальний контент може бути завантажений безпосередньо з мережі чи флеш-карти. Усі ці технічні аспекти дозволяють реалізувати принцип «навчання де завгодно і коли завгодно».

Основним завданням викладача є представлення навчальних матеріалів (контенту) в зрозумілій формі, що легко та надовго запам’ятовується. Контент е-навчальних матеріалів відрізняється широкою різноманітністю: від простих текстів до складних мультимедійних документів і далі – до віртуальних лабораторних робіт і тренажерів. Численні дослідження доводять пряму залежність розуміння і запам’ятовування навчального матеріалу від складності навчального контенту.

На рис. 3.1 наведено відому з дидактики діаграму, яка демонструє рівень розуміння і запам’ятовування навчального матеріалу залежно від складності контенту. Діаграма наочно показує, що, чим вищого рівня розуміння і запам’ятовування навчального матеріалу ми намагаємося досягти, тим більший за складністю контент ми повинні використовувати.

Рис. 3.1

Численні опитування викладачів і студентів, а також об'єктивні результати досліджень дозволяють стверджувати, що проведення занять з використанням сучасних технологій навчання із застосуванням комп'ютерної техніки і мультимедійних засобів має істотні переваги перед традиційними методами.

До е-навчального слід віднести такий контент, який може бути створений, збережений і відтворений тільки електронними засобами. Наприклад, прості навчальні матеріали першого і другого рівнів (рис. 3.1) можуть існувати як в електронному, так і в паперовому вигляді.

Що стосується складних навчальних матеріалів третього-п'ятого рівнів, то вони створюються і відтворюються тільки спеціалізованими електронними засобами, і тому повною мірою можуть бути віднесені до е-навчальних матеріалів.

Для створення ефективного е-контенту третього-четвертого рівнів (рис. 1) достатньо володіння програмами з офісного пакету Word, Excel і PowerPoint. Характерною ознакою навчальних матеріалів такого рівня є їх мультимедійність та інтерактивність. Створення віртуальних лабораторних робіт і тренажерів потребує високого рівня володіння програмуванням, що не властиво більшості викладачів, і тому тут не розглядається.

До основних особливостей е-навчальних матеріалів, порівняно з традиційними, слід віднести:

мультимедійність – використання різноманітних інформаційних потоків (текст, графіка, звук, анімація, відео тощо) з метою суттєвого підвищення рівня розуміння і запам'ятовування навчального матеріалу;

інтерактивність – адекватна реакція на дії користувача (перехід до певних розділів навчального матеріалу, тобто вибір траєкторії навчання, відтворення мультимедіа, налаштування у відповідності до вимог користувача тощо);

автоматизована перевірка рівня засвоєння навчального матеріалу.

Крім того, для е-навчальних матеріалів важливе забезпечення можливості відтворення як у середовищі спеціалізованих систем електронного навчання (LMS/LCMS системи), так і на комп'ютерах користувачів з будь-якою операційною системою і пакетом офісних програм.

Е-навчальні матеріали у вигляді презентацій. В основі процесу навчання лежить представлення учням навчального матеріалу, тобто його презентація. Тому представлення е-контенту у вигляді презентацій є доцільним, природним і виправданим. Можливості сучасних програмних засобів, і перш за все програми PowerPoint, дозволяють створювати мультимедійні та інтерактивні навчальні матеріали високого рівня. За можливостями створення е-навчальних матеріалів, які удосконалюються і розширюються від версії до версії, з PowerPoint не може змагатися жодна з програм пакету MS Office, а також переважна більшість спеціалізованих авторських програм для створення навчального контенту. Важливим є те, що програма PowerPoint легка і зручна в опануванні і використанні, що дозволяє більшості викладачів самостійно створювати е-навчальні матеріали третього- четвертого рівнів з широкими

мультимедійними та інтерактивними можливостями. До того ж широкі можливості PowerPoint дозволяють використовувати одну і ту саму програму як для презентації навчальних матеріалів на лекціях, так і для створення електронних підручників і посібників високого рівня. Крім того, як презентації, так і електронні підручники, створені у середовищі PowerPoint, легко і без проблем інтегруються в LMS/LCMS-системи, у тому числі і у Moodle.

Процес створення презентації в Microsoft PowerPoint складається з таких *дій*:

– вибір загального оформлення із застосуванням різноманітних шаблонів оформлення;

– додавання нових слайдів та їх вмісту;

– вибір розмітки слайдів;

– зміна оформлення слайдів у разі необхідності, зміна колірної схеми;

– створення ефектів анімації під час демонстрації слайдів.

Процес створення мультимедійних презентацій та можливості програми Microsoft PowerPoint детально розглянуті в [1; 2].

Формати збереження презентацій у PowerPoint 2010

Тип файлу	Розширення	Використовується для збереження
Презентація	pptx	Звичайна презентація PowerPoint
Метафайл Windows	wmf	Слайда у формі малюнка
Малюнок у форматі GIF	gif	Слайда у формі малюнка для використання на web-сторінках
Малюнок у форматі JPEG	jpg	Слайда у формі малюнка для використання на web-сторінках
Структура RTF	rtf	Вмісту презентації у вигляді документу структури
Шаблон оформлення	pot	Презентації у вигляді шаблону
Демонстрація PowerPoint	ppsx	Презентації, яка автоматично відкривається в режимі показу слайдів
Web-сторінка	htm; html	Web-сторінка у формі папки з html файлом і всіма допоміжними файлами
Web-архів	mht; mhtml	Web-сторінка у формі одного файла

Вимоги до навчальної презентації:

1) усі слайди презентації мають бути витримані в одному стилі;

2) ретельно структурована інформація з акцентом на правові аспекти питання, проблеми, завдання тощо.

3) кожен слайд має відображати одну думку (тезу, факт, твердження), головну ідею треба викласти в першому рядку абзацу;

4) стислий виклад матеріалу, максимальна інформативність тексту (текст має складатися з коротких слів та простих речень; великий текст дуже важко читати та майже неможливо запам’ятати; слухачі можуть одноразово запам’ятати не більше трьох фактів, висновків, визначень);

5) рядок має містити 6–8 слів; всього на слайді має бути 6–8 рядків; загальна кількість слів не повинна перевищувати 50;

6) текст рекомендовано вирівнювати по ширині; не слід використовувати переноси в словах; не слід писати весь текст прописними літерами;

7) короткі та лаконічні заголовки мають привертати увагу та узагальнювати основні ідеї слайду; у заголовках мають бути і великі, і малі літери;

8) важливу інформацію (наприклад, висновки, визначення, правила тощо) треба розміщувати в лівому верхньому кутку слайда; другорядну інформацію бажано розміщувати внизу слайда;

9) розмір шрифту не повинен бути дрібним: найбільш «дрібний» для презентації – шрифт 22 пт;

10) неможна використовувати у презентації понад трьох шрифтів на слайді (шрифт Verdana визнаний кращим шрифтом для читання тексту з екрану, Tahoma, Bookman спеціально розроблені для створення презентацій, Times New Roman легко зчитується, тому його використовують для друку тексту, Arial краще виглядає у заголовках та колонтитулах);

11) зображення має органічно доповнювати текст, його потрібно розташувати або під текстом, який ілюструється, або ліворуч від нього; підпис до ілюстрації розмішується під нею, а не над нею;

12) слайди мають бути не надто яскравими (зайві прикраси лише створюють бар'єр на шляху ефективного передавання даних);

13) найкраще поєднання кольорів шрифту і фону: чорний на білому, білий на темно-синьому, жовтий на синьому;

14) відсутність граматичних, орфографічних, мовних, фактичних помилок, достовірність представленої інформації;

15) на титульному і завершальному слайдах використання анімаційних об'єктів не допускається.

3.2. Інтернет-технології в науково-педагогічній діяльності

Телеконференції USENET. Для організації глобального спілкування в мережі організуються телеконференції. Телеконференції призначені для ведення дискусії і обміну новинами.

Юзнет (англ. Usenet скор. від User Network) – комп'ютерна мережа, використовувана для спілкування та публікації файлів. Usenet складається з новинних груп, в які користувачі можуть надсилати повідомлення. Повідомлення зберігаються на серверах, які обмінюються ними один з одним. Usenet справив великий вплив на розвиток сучасної вебкультури, давши початок таким широко відомим поняттям, як ніки, смайли, підпис, модератори, троллінг, флуд, флейм, бан, FAQ і спам. Юзнет є частиною Інтернету, а не окремою від нього мережею. Фактично це набір дискусійних груп за інтересами, де можна обговорити будь-яку проблему.

Новини мережі Usenet (*телеконференції*) – це один з найважливіших сервісів Інтернет. Якщо електронна пошта передає повідомлення по принципу «від одного – одному», то новини мережі передають повідомлення «від одного – багатьом». Механізм передачі кожного повідомлення схожий на передачу пліток: кожен вузол мережі, який отримав якусь нову інформацію (тобто нове повідомлення), передає її на всі знайомі вузли, тобто всім тим вузлам, з якими обмінюється новинами. Таким чином, послане користувачем повідомлення розповсюджується, багатократно дублюючись, по мережі, досягаючи за доволі короткі строки всіх учасників телеконференції Usenet у всьому світі. При цьому в обговоренні теми, яка цікавить користувача, може брати участь безліч людей, незалежно від того, де вони знаходяться фізично. Кількість користувачів Usenet доволі велика – за оцінками UUNET technologies кількість нових повідомлень, які поступають у телеконференції щоденно, становить близько мільйона.

Сьогодні існують десятки тисяч різних груп новин. Дошка оголошень телеконференцій доступна через поштову програму (зокрема, Outlook Express), подібно електронній пошті. Не відходячи від комп'ютера, можна читати або поміщати статті в ту чи іншу конференцію, знайти корисну пораду або вступити в дискусію. Статті періодично знищуються, звільняючи місце для нових. Основна мова спілкування на міжнародних дошках оголошень – англійська. Порядок в публікаціях забезпечується самими учасниками.

У кожній конференції існують правила поведінки, які повинен знати кожен учасник і беззастережно дотримуватися. За дотриманням правил стежить користувач, наділений широкими правами – модератор.

Новачкам необхідно буде відвідати наступні телеконференції:

– *relcom.answers* – правила телеконференцій;

– *relcom.newusers* – інформація для нових користувачів.

Групи новин організовані та згруповані за заголовками за допомогою складових імен, наприклад, *rec.sport.footbalolл.college*. Тут «rec» вказує на розділи за темою «recreation», «sport» – на підгрупу розділу «recreation» і т.ін.

Соціальні мережеві сервіси. Web-технології другого покоління стали каталізатором революційних змін у засобах взаємодії людей з мережею. Internet, будучи досі переважно «мережею читачів», трансформується в «мережу письменників». Сучасну концепцію розвитку Інтернет прийнято називати Веб 2.0 (Web 2.0).

Принциповою відмінністю Веб 2.0 від традиційної мережі є можливість створювати зміст Інтернету будь-якому користувачеві. Завдяки інструментарію Web 2.0, використовуючи соціальні мережеві сервіси, кожен має можливість стати творцем, а не пасивним споживачем інформації в WWW.

Соціальний мережевий сервіс – це віртуальний майданчик, що об'єднує людей в мережеві спільноти за допомогою спеціального програмного забезпечення в мережі Інтернет.

Мережеве співтовариство – це група людей, що підтримують спілкування та здійснюють спільну діяльність за допомогою комп'ютерних мережевих

засобів. Завдяки мережевим зв'язкам формуються об'єднання користувачів з метою обміну знаннями. Спільноти такого типу не можуть бути спеціально спроектовані, організовані або створені у наказному порядку. З розвитком комп'ютерних технологій у спільнотах обміну знаннями з'являються нові форми для зберігання знань і нові програмні сервіси, що полегшують управління знаннями та використання цих знань новачками. Інтернет-технології Web 2.0, зокрема, соціальні сервіси, надають технічні можливості для вирішення виховних та соціально-педагогічних проблем молодої людини.

Інтернет, об'єднуючи людей за спільними інтересами, стимулює розвиток міжособистісних і професійних стосунків. Технологія Web 2.0 дозволяє створювати сайти співтовариств з можливістю власних налаштувань і особистою зоною для кожного учасника (викладення в мережі власних файлів, аудіо та відео фрагментів, зображень, щоденників тощо).

Ці можливості створюють у користувача відчуття власної унікальності, необхідності, дають змогу поділитися творчими доробками, отримати оцінку, критику, поради.

Соціальні сервіси відкривають великі можливості щодо ***застосування їх у науково-педагогічній діяльності***:

1. *Використання відкритих, безкоштовних і вільних електронних ресурсів.* У результаті поширення соціальних сервісів в мережевому доступі виявляється величезна кількість матеріалів, які можуть бути використані з навчальною метою. Мережеві співтовариства обміну знаннями можуть поділитися своїми колекціями цифрових об'єктів і програмними агентами з освітою.

2. *Самостійне створення мережевого навчального змісту.* Сервіси соціального забезпечення радикально спростили процес створення матеріалів та публікації їх в мережі. Кожен може не тільки отримати доступ до цифрових колекцій, а й взяти участь у формуванні власного мережевого контенту. Наразі новий контент створюється мільйонами людей. Вони приносять в мережу нові тексти, фотографії, малюнки, музичні файли.

3. *Освоєння інформаційних концепцій, знань і навичок.* Середовище інформаційних додатків відкриває принципово нові можливості для діяльності, до якої надзвичайно легко залучаються люди, що не володіють спеціальними знаннями в галузі інформатики. Нові форми діяльності, пов'язані як з пошуком в мережі інформації, так і з створенням та редагуванням власних цифрових об'єктів – текстів, фотографій, програм, музичних записів, відеофрагментів. Участь у нових формах діяльності дозволяє освоювати важливі інформаційні навички – повторне використання текстів і кодів, використання метатегів тощо.

4. *Спостереження за діяльністю учасників мережевої спільноти.* Мережа Інтернет відкриває нові можливості для участі студентів у фахових наукових спільнотах. Мережа спонукає до творчості, розширює не тільки розумові здібності, але й поле для спільної діяльності та співпраці з іншими людьми.

Види соціальних мережевих сервісів. Використання соціальних мереж допомагає викладачу оперативно знайти необхідну інформацію, узагальнити та структурувати навчальні матеріали, полегшує роботу в аудиторії та дозволяє

організувати науково-педагогічну роботу поза нею, надає можливість творчості і співпраці з однодумцями. Викладачі нового «цифрового» покоління збирають та відображають навчальні матеріали в мережі. Це можуть бути документи, презентації, фотографії, відеофрагменти, тести, опитувальники, вікі-документи, карти (Mindmaps), вебсторінки, навчальні середовища.

Розглянемо приклади деяких соціальних сервісів.

Спільні сховища закладок – засоби для зберігання посилань на вебсторінки, які користувач регулярно відвідує. Такий засіб надається і звичайним браузером, за допомогою якого користувач переглядає Інтернет-ресурси, проте нові соціальні засоби зберігання закладок мають *принципові відмінності*,

а саме:

– посилання можна додавати з будь-якого комп'ютера, підключеного до мережі Інтернет;

–посилання будуть доступні з будь-якого комп'ютера, підключеного до мережі Інтернет;

–кожна закладка повинна бути позначена одним або кількома тегами (мітками-категоріями).

Приклади спільних сховищ закладок: http://Del.icio.us .

Соціальні мережеві сервіси для зберігання мультимедійних ресурсів – засоби мережі Інтернет, які дозволяють безкоштовно зберігати, класифікувати, обмінюватися цифровими фотографіями, аудіо і відеозаписами, текстовими файлами, презентаціями, а також організовувати обговорення ресурсів.

Приклади соціальних мереж для зберігання мультимедійних ресурсів: http://flickr.com; http://www.panoramio.com; http://audacity.sourceforge.net; http://www.podomatic.com; http://www.slideshare.net; http://www.spresent.com.

Мережеві щоденники (блоги) – сервіс Інтернету, що дозволяє будь-якому користувачеві вести записи будь-яких текстів. За аналогією з особистими щоденниками блоги називають мережевими щоденниками. Блогер (той, що веде щоденник) може керувати доступом до своїх записів: робити їх відкритими всім бажаючим, визначеному колу користувачів або зовсім приватними. За авторським складом блоги можуть бути особистими, груповими (корпоративними, клубними) або загальними (відкритими).

Для блогів характерна можливість публікації відгуків. Ведення блогу припускає наявність програмного забезпечення, що дозволяє звичайному користувачеві додавати і змінювати записи, публікувати їх в Інтернеті.

Блоги сприяють розвитку комунікації, згуртуванню та утриманню соціальних зв'язків, саморозвитку, рефлексії, а також здійснюють психотерапевтичну функцію. У навчальному процесі їх можна використовувати як блог професійної спільноти, джерело навчальної інформації, попередньо опублікованої вчителем (блог-конспект), для організації дистанційного навчання дітей з особливими потребами, що не можуть постійно відвідувати школу, для підтримки різноманітних проектів, тощо.

Приклади мережевих щоденників приведені: http://www.blogger.com.

ВікіВікі (WikiWiki) – соціальний сервіс, що дозволяє будь-якому користувачеві редагувати текст сайту (писати, вносити зміни, видаляти, створювати посилання на нові статті). Різні варіанти програмного забезпечення Вікі дозволяють завантажувати на сайти зображення, файли, що містять текстову інформацію, відеофрагменти, звукові файли і т.п.

Приклади ВікіВікі: http://eduwiki.uran.net.ua; http://wikipedia.org

Соціальні Геосервіси – сервіси мережі Інтернет, які дозволяють знаходити, відзначати, коментувати, забезпечувати фотографіями різні об'єкти в будь-якому місці на зображенні Земної кулі з досить високою точністю, використовуючи реальні дані, отримані за допомогою навколоземних супутників.

Приклади соціальних геосервісів: http://maps.google.com; http://wikimapia.org; http://earth.google.com.

Соціальні сервіси, що дозволяють організовувати спільну роботу з різними типами документів – інтегровані сервіси Інтернет, орієнтовані на організацію спільної роботи з текстовими, табличними документами, планувальниками, іншими корпоративними завданнями.

Приклади соціальних сервісів для спільної роботи з документами: http://docs.google.com; http://scribd.com; http://slideshare.net; http://www.spresent.com.

Карти знань (англ. Mind map) – спосіб зображення процесу загального системного мислення за допомогою схем. Їх іноді називають «карти розуму», «карти пам'яті», «інтелект-карти», «Майнд-мепи».

Приклади карт знань: http://bubbl.us.

Соціальні пошукові системи – це системи, які дозволяють користувачам самим визначати: в якому напрямку вести пошук, які сайти переглядати перш за все, на які слова звертати першочергову увагу і яким чином представляти знайдені результати. Пошук можна адаптувати до певної тематики і до певної спільноти.

Приклади соціальних пошукових систем: http://www.eurekster.com; http://www.google.com/coop/cse.

Все частіше курсанти, студенти, слухачі надають перевагу не читанню книг, а вважають за краще мати справу з невеликими об'єктами в електронному форматі: читають блоги, дивляться відеозаписи на YouTube, розміщують фотографії на Flickr, обмінюються думками на форумах, створюють власні соціальні мережі типу MySpace або групи Google.

Ці реалії викладач зобов'язаний враховувати, плануючи свою у педагогічну діяльність.

Одним з таких соціальних сервісів, який допомагає у створенні середовища для організації навчальної діяльності, є група Google.

Створення групи в Google надає такі *можливості*:

– пошук корисної інформації;

– створення власних груп;

– приєднання до груп;

– обговорення різних тем;

– ведення обговорення в режимі on-line або електронною поштою;

– створення власної вебсторінки безпосередньо в групі;

– побудова бази знань;

– створення унікального оформлення;

– спільне використання файлів та інформації, що надходить від учасників групи;

– більш близьке знайомство з учасниками групи та ін.

Використання Google-груп надає можливості для *вдосконалення науково-педагогічної діяльності викладача*:

– оперативне викладення в групі електронних навчальний посібників, конспектів, завдань на практичні заняття;

– консультування, зокрема, слухачів заочної форми навчання, які не мають змоги регулярно відвідувати вищий навчальний заклад;

– організація обговорень за певною тематикою;

– координація навчальної та наукової діяльності;

– викладення в групі результатів навчальної діяльності курсантів, студентів, слухачів (творчих завдань, рефератів, результатів науково-дослідницьких робіт тощо) та організація їх обговорення.

Для створення групи необхідно зайти у Google, зареєструватися на gmail. Після реєстрації у головному меню Google знайти «Групи» та слідувати інструкції.

Питання для самоконтролю

1. Що таке «презентація»?
2. Які способи створення слайдів Ви знаєте?
3. Що таке «макет» слайду? Як його застосувати?
4. Як можна оформити дизайн слайду?
5. Як створити фон слайду власноруч?
6. Які Ви знаєте режими відображення слайдів?
7. Що означає слово «анімація»?
8. Як додати переходи між слайдами презентації?
9. Як додати анімацію до об’єктів слайду?
10. Як встановити параметри анімації елементів слайду?
11. Як встановити порядок відображення анімації різних об’єктів слайду?
12. Як автоматизувати показ слайдів?
13. Як встановити параметри зміни слайдів?
14. Як відбувається демонстрація презентації?
15. Як сформувати довільний показ створеної презентації?
16. Які способи керування презентацією Ви знаєте?
17. Що означає «Налаштувати демонстрацію» презентації? Як це зробити?
18. Як задати час демонстрації конкретного слайду презентації?
19. Яку роль відіграють графічні об’єкти на слайдах?
20. Які є способи введення графічних об’єктів у слайд?

21. Як згрупувати (розгрупувати) відповідні графічні об’єкти на слайді?
22. Як встановити звукове оформлення слайдів?
23. Як можна додати відео програми PowerPoint?
24. Як користуватися колекцією кліпів?
25. Які Ви знаєте формати збереження презентацій?
26. Яке розширення присвоює програма PowerPoint для імені файлу презентації?
27. Поняття телеконференції USENET.
28. Можливості соціальних мережевих сервісів.

Практичні завдання до розділу ІІІ

Практичне заняття № 3.1

Мета заняття: поглибити практичні навички здобувачів щодо використання системи презентацій PowerPoint для представлення результатів науково-педагогічної діяльності.

Завдання:

1. Створити за допомогою програми PowerPoint файл презентації з назвою **Ваше прізвище_П.з. 3.1**.
2. Встановити пароль на файл.
3. Ознайомитись з **Вимогами до презентації**:

1) усі слайди презентації мають бути витримані в одному стилі;
2) ретельно структурована інформація з акцентом на правові аспекти питання, проблеми, завдання тощо.
3) кожен слайд має відображати одну думку (тезу, факт, твердження), головну ідею треба викласти в першому рядку абзацу;
4) стислий виклад матеріалу, максимальна інформативність тексту (текст має складатися з коротких слів та простих речень; великий текст дуже важко читати та майже неможливо запам’ятати; слухачі можуть одноразово запам’ятати не більше трьох фактів, висновків, визначень);
5) рядок має містити 6 – 8 слів; всього на слайді має бути 6 – 8 рядків; загальна кількість слів не повинна перевищувати 50;
6) текст рекомендовано вирівнювати по ширині; не слід використовувати переноси в словах; не слід писати весь текст прописними літерами;
7) короткі та лаконічні заголовки мають привертати увагу та узагальнювати основні ідеї слайду; у заголовках мають бути і великі, і малі літери;
8) важливу інформацію (наприклад, висновки, визначення, правила тощо) треба розміщувати в лівому верхньому кутку слайда; другорядну інформацію бажано розміщувати внизу слайда;
9) розмір шрифту не повинен бути дрібним: найбільш «дрібний» для презентації – шрифт 22 пт;
10) неможна використовувати у презентації понад трьох шрифтів на слайді (шрифт Verdana визнаний кращим шрифтом для читання тексту з екрану, Tahoma, Bookman спеціально розроблені для створення презентацій, Times New

Roman легко зчитується, тому його використовують для друку тексту, Arial краще виглядає у заголовках та колонтитулах);

11) зображення має органічно доповнювати текст, його потрібно розташувати або під текстом, який ілюструється, або ліворуч від нього; підпис до ілюстрації розмішується під нею, а не над нею;

12) слайди мають бути не надто яскравими (зайві прикраси лише створюють бар'єр на шляху ефективного передавання даних);

13) найкраще поєднання кольорів шрифту і фону: чорний на білому, білий на темно-синьому, жовтий на синьому;

14) відсутність граматичних, орфографічних, мовних, фактичних помилок, достовірність представленої інформації;

15) на титульному і завершальному слайдах використання анімаційних об'єктів не допускається.

4. **ТВОРЧА РОБОТА**: створити презентацію з 5 слайдів на запропоновану викладачем тему, яка співпадає з Вашим порядковим номером за списком.

№ з/п	*Тема презентації*
1.	Конституція України
2.	Кримінальний кодекс України
3.	Міністерство внутрішніх справ
4.	Умисне вбивство
5.	Національна поліція України
6.	Домашнє насильство
7.	Національна академія внутрішніх справ
8.	Поліцейський
9.	Торгівля людьми
10.	Реєстри Міністерства юстиції України
11.	Навчально-науковий інститут № 1 НАВС
12.	Крадіжка
13.	Інтерпол
14.	Грабіж
15.	Навчально-науковий інститут № 2 НАВС
16.	Корупція
17.	Розбій
18.	Інформаційний портал НПУ
19.	Шахрайство
20.	Навчально-науковий інститут заочного та дистанційного навчання НАВС
21.	БД «Законодавство України» вебпорталу ВРУ
22.	Контрабанда
23.	Розшукові обліки МВС
24.	Інститут підготовки керівних кадрів та підвищення кваліфікації НАВС
25.	Наркоманія
26.	ДТП
27.	Кіберполіція
28.	Інтернет
29.	Штучний інтелект
30.	Кримінальний процесуальний кодекс України

Критерії оцінювання презентації:

1. Повнота розкриття теми.
2. Структурування інформації, розміщення і комплектування об’єктів, єдиний стиль слайдів.
3. Наявність і правильність оформлення обов’язкових слайдів (титульний, завершальний).
4. Відсутність граматичних, орфографічних, мовних, фактичних помилок, достовірність поданої інформації.
5. Обґрунтованість і раціональність використання засобів мультимедіа та анімаційних ефектів.
6. Грамотність використання шрифтів, кольорового оформлення.

Практичне заняття № 3.2

Час виконання: 2 години.

Мета заняття: поглибити практичні навички щодо використання мультимедійних технологій уявлення даних в науково-педагогічній та професійній діяльності.

Завдання: створити презентацію з дисципліни «Сучасні інформаційні технології в юридичній діяльності».

Порядок виконання:

Завдання № 1

Створити слайд № 1 "Інформаційні технології" за допомогою автомакету ***Титульний слайд****, згідно наведеного малюнка:*

Встановити ефекти слайду:

для заголовка (Заголовок слайда) – ефект **Виліт справа**, поява тексту **По буквах**;

для підзаголовка (Підзаголовок слайда) – ефект **Виліт знизу**, поява тексту **По буквах**.

Порядок виконання завдання № 1

Запустити програму PowerPoint.

На панелі **Основне** клацнути інструмент **Створити слайд** та вибрати макет **Титульний слайд.**

Ввести текст заголовка: *Інформаційні технології* (використайте **Вставлення**-**WordArt**)

Встановити для ***заголовку*** розмір шрифта – 60, колір – червоний.

Встановити для ***заголовку*** жовту тінь та налаштувати її, як на малюнку зразка (Використати кнопку **Текстові ефекти** з групи інструментів **Формат фігури** вкладки **Засоби креслення.** Вибрати колір тіні, зменшити її прозорість, збільшити розмір).

Ввести текст підзаголовку: створення мультимедійних презентацій.

Встановити для ***підзаголовку*** розмір шрифта – 40, колір – синій.

Встановити для ***підзаголовку*** синю тінь.

Встановити фон слайду – білий мармур за допомогою команди **Формат фону** з контексного меню слайда. В діалоговому вікні **Формат фону** в списку лівої частини вікна вибрати пункт **Заливка**, потім у правій частині вибрати **Зображення або текстура**. Серед зразків текстур, що розчиняється, вибрати текстуру білий мармур.

Клацнути по кнопці **Область анімації** на вкладці **Анімація.** У робочому вікні програми з’явиться додаткове підвікно **Область анімації** для роботи з анімаційними ефектами.

Виділяєте на слайді об’єкт, до якого хочете застосувати анімаційний ефект. В нашому випадку це заголовок слайда («Інформаційні технології»). На вкладці **Анімація** клацаємо інструмент **Додати анімацію.** Далі з групи ефектів **Вхід** вибираємо ефект **Виліт**. У вікні **Область анімації** з’явиться поле, що відповідає даному анімаційному ефектові і може бути використане для його налаштування. Клацаємо мишею по кнопці, що розташована в правій частині цього поля. У меню, що з’явиться, вибираємо пункт **Параметри ефектів.** Відкриється вікно **Виліт**, в якому в полі **Напрямок** слід встановити значення **Справа**, в полі **Анімація тексту** – значення **По буквам.**

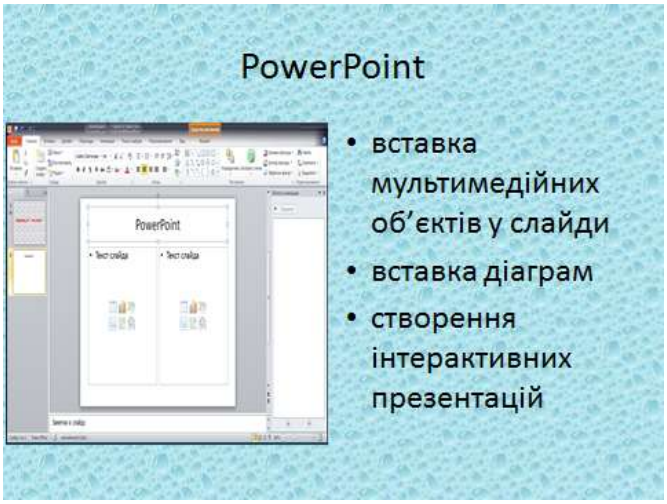
Аналогічно додаємо анімаційний ефект для підзаголовку.

Після додавання анімаційних ефектів клацнути на кнопці **Зберегти** у верхній лівій частині заголовка вікна програми.

Для додавання наступного слайду використовуємо на вкладці **Основне** інструмент **Створити слайд,** який дозволяє створювати слайди різних типів (вибираються з вікна **Тема Office**).

Завдання № 2

Створити слайд № 2 «PowerPoint» за допомогою автомакету ***Два об'єкти****, згідно наведеного малюнку:*



– Встановити для заголовка – ефект **Збільшення з поворотом,** поява тексту **По буквах.**

– Встановити для списку тем – ефект **Випадкові смуги,** поява тексту **По словам,** ефект повинен відбуватись повільно.

– Вставити скріншот з зображенням вікна програми PowerPoint.

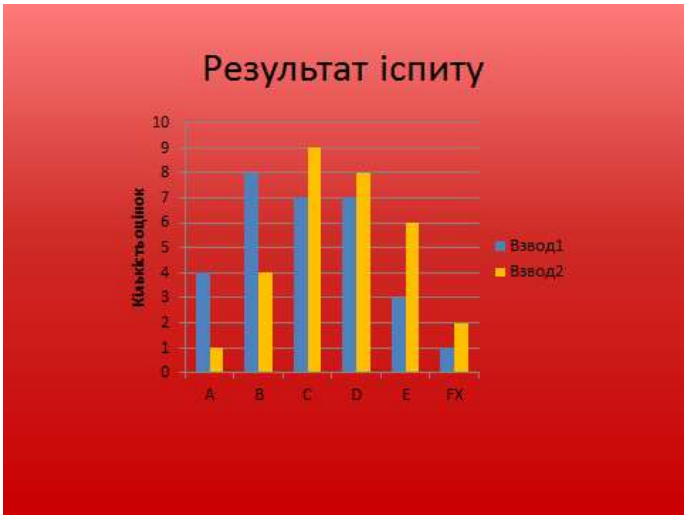
– Встановити для малюнка – ефект входа **Спіраль.**

Завдання № 3

Дві групи курсантів на екзамені отримали наступні оцінки з предмета:

Оцінка / Група	**A**	**B**	**C**	**D**	**E**	**FX**
1-й взвод	4	8	7	7	3	1
2-й взвод	1	4	9	8	6	2

За результатами іспиту створити наступний слайд № 3 (рис. нижче):



– Для фону слайду використати градієнтну заливку.

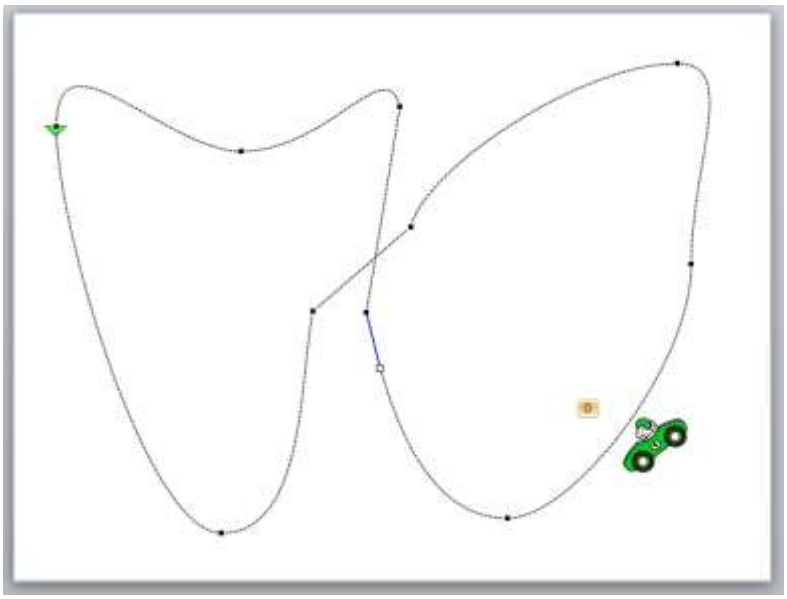
– Для діаграми встановити анімаційний ефект виникнення (**за категоріями**)

Завдання № 4

Створити слайд, що містить зображення автомобіля, який рухається по полотну слайда і описує траєкторію складної форми (що не є правильною симетричною фігурою).

Автомобіль повинен рухатись досить повільно, щоб можна було роздивитись напрямки його руху.

Приклад зображення автомобіля і можливої траєкторії руху показано на малюнку нижче.



Завдання № 5

Створити слайд № 5 «Повторити чи вийти?» згідно наведеного малюнку:

Для фона використати градієнтну заливку (**Полум'я**).

Заголовок зробити як об'єкт WordArt. Застосувати до нього ефект **Світіння.**

За кнопками повинні бути закріплені відповідні гіперпосилання, що дозволяють повернутися на початок презентації або завершити її перегляд.

Завдання № 6

Перейти на вкладку ***Переходи*** *та встановити для слайдів такі параметри:*

Слайд № 1 – **Вицвітання** (**Поступово**, на протязі 3 сек.), зміна слайду відбувається автоматично через 4 сек.

Слайд № 2 – **Поява** (знизу зліва, на протязі 1 сек.), зміна слайду відбувається автоматично через 3 сек.

Слайд № 3 – **Тріщина,** зміна слайду відбувається автоматично через 3 сек.

Слайд № 4 – **Галерея,** зміна слайду відбувається автоматично через 10 сек.

Слайд № 5 – **Вир,** зміна слайду відбувається автоматично через 59 хвилин 59 секунд.

Для того, щоб запобігти випадковим натисканням миші, перейдіть на вкладку **Показ слайдів** та за допомогою піктограми **Налаштувати показ слайдів** встановіть автоматичний режим показу слайдів.

Практичне заняття № 3.3

Мета заняття: Поглибити практичні навички щодо використання засобів Microsoft Excel графічного уявлення даних для візуалізації результатів наукових досліджень

Підготовка до виконання завдань:

1. Створити за допомогою програми Excel файл з назвою **Ваше прізвище_П.з. 3.3**.

2. Встановити **пароль** на файл.

3. Уважно ознайомитись з наступною **інструкцією**.

Формула завжди починається із символу «=».

Під ***формулою*** в електронній таблиці розуміють вираз, який складається з операндів і операцій.

У якості *операндів* використовуються: числа; текст (вводиться в подвійних лапках, наприклад «Київ»); логічні значення (наприклад, умови типу A23=A45 та ін.); посилання – адреси клітинок (при перерахуванні посилання розділяються крапкою з комою, наприклад: *A4; B5; B10; E20;* вбудовані функції Excel.

Операнди у формулах з’єднуються за допомогою символів *операцій:*

арифметичних операцій: «+» (додавання), «-« (віднімання), «/» (ділення), «*» (множення), «^» (возведення у ступінь);

операцій відносин: «>» (більше), «>=» (не менше), «<» (менше), «<=» (не більше), «=» (дорівнює), «<>» (не дорівнює).

У будь-яких версіях Excel для різних типів обчислень є велике число вбудованих функцій: математичних, статистичних, логічних, текстових, фінансових та ін. Функції вводяться звичайним набором із клавіатури або більш раціональним способом — за допомогою *Майстра функцій*, діалогове вікно якого викликається кнопкою **Вставити функцію** на лінійці **Формули**.

Завдання 1. Побудувати графік функції: $y = 5\sin(x)\cos(2x+1)$. Значення X вибрати з діапазону -2 до 2 кроком 0,05. Побудувати діаграму за результатами розрахунків.

Рішення:

1. Розрахувати необхідний діапазон значень для X та Y. Кількість стовпців дорівнює кількості невідомих, кількість рядків визначається як ширина діапазону варіювання змінної X поділена на крок прогресії плюс один:

(2-(-2))/0,05+1. В нашому випадку кількість стовпців дорівнює 2, кількість рядків 81.

2. В клітинку A1 заносимо назву змінної X, в клітинку B1 назву змінної У.

3. Початкове значення X дорівнює -2. Вводимо це значення в клітинку A2.

4. Для автоматизації побудови прогресії (початкові значення діапазону та крок відомі):

4.1. Виділяємо клітинку A2, зробивши клік лівою кнопкою маніпулятора (миша) у відповідному місці;

4.2. Курсор встановлюємо в правий нижній кут клітинки (курсор повинен прийняти вигляд хрестика);

4.3. Зафіксувавши ПРАВУ кнопку маніпулятора, тягнемо його вниз, виділяючи діапазон A2:A82;

4.4. У контекстному меню, що з'явиться, необхідно вибрати «**Прогресія**…»;

4.5. Встановлюємо значення типу та кроку прогресії (арифметична та 0,05, відповідно).

4.6. Значення X з наданого діапазону визначені.

5. Для розрахунку Y необхідно скористатися наданою функцією: $y = 5\sin(x)\cos(2x+1)$:

5.1. В клітинку B2 необхідно ввести надану формулу (з клавіатури або за допомогою *Майстра функцій*);

5.2. Формула вводиться у наступному вигляді: =5*SIN(A2)*COS(2*A2+1);

5.3. Курсор маніпулятора ставимо в нижній правий кут клітинки B2;

5.4. Фіксуємо ЛІВУ кнопку маніпулятора і виділяємо стовпчик B в необхідному діапазоні (B2:B82).

В результаті ми повинні отримати таблицю значень X та Y в наступному вигляді:

	A	**B**
1	x	y
2	-2	4,500988149
3	-1,95	4,509905102
4	-1,9	4,458125418
5	-1,85	4,345310659
6	-1,8	4,172395412
7	-1,75	3,941570296
. . .	. . .	. . .
76	1,7	-1,523855961
77	1,75	-1,037100521
78	1,8	-0,546097363
79	1,85	-0,059544575
80	1,9	0,414001479
81	1,95	0,866312388
82	2	1,289666477

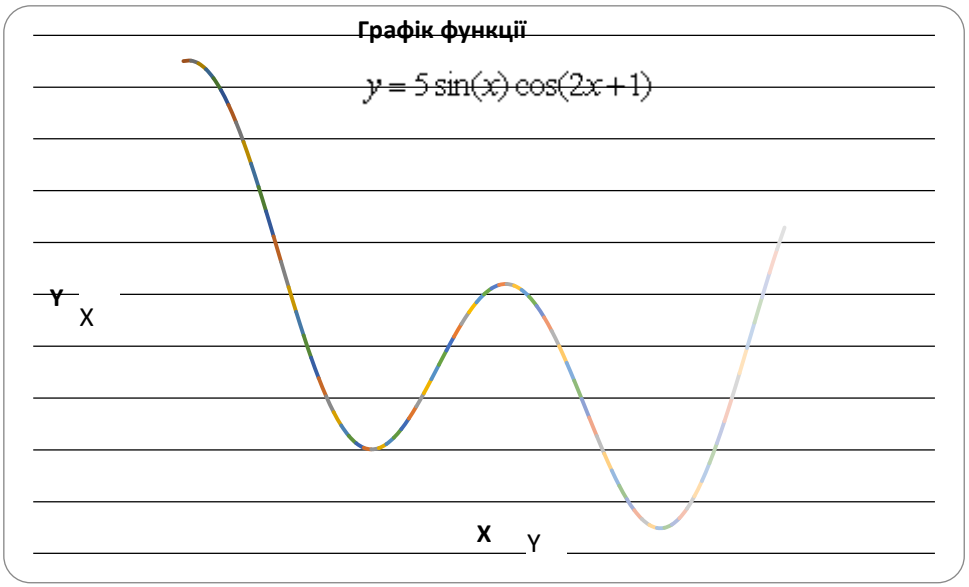
6. Побудова діаграми:

6.1. Зафіксувавши ліву кнопку маніпулятора, виділити діапазон значень X та Y, на основі якого буде будуватися діаграма;

6.2. Вибрати **Вставка, Діаграма**;

6.3. Тип діаграми: **Точкова з гладкими кривими**;

6.4. В результаті ми повинні отримати графік заданої функції у наступному вигляді:



Завдання 2. Побудувати на окремих аркушах графіки функцій згідно виразів, наведених нижче.

Під час побудови **виділяти тільки** діапазони значень змінних X та У.

2.1. Побудувати графік функції (Декартов аркуш): $x = \frac{9\cos(\varphi)\sin(\varphi)}{\cos^3(\varphi)+\sin^3(\varphi)}\cos(\varphi),\ y = \frac{9\cos(\varphi)\sin(\varphi)}{\cos^3(\varphi)+\sin^3(\varphi)}\sin(\varphi)$.

φ оберіть з діапазону від -0,15 до 2 з кроком 0,05.

2.2. Побудувати Верьсьєру: $x = t,\ y = \frac{27}{t^2+9}$.

Прийняти t від -5 до 5 кроком 0,3.

2.3. Побудувати Лемніскату Бернуллі: $x = 8\cos(2\varphi)\cos(\varphi),\ y = 8\cos(2\varphi)\sin(\varphi)$.

φ оберіть із діапазону від -3 до 0 із кроком 0,1.

2.4. Побудувати Равлика Паскаля:

$x = (10\cos(\varphi)+2)\cos(\varphi),\ y = (10\cos(\varphi)+2)\sin(\varphi)$.

φ оберіть від -2 до 4,3 із кроком 0,1.

2.5. Побудувати Астроіду: $x = 3\cos^3(t),\ y = 3\sin^3(t)$.

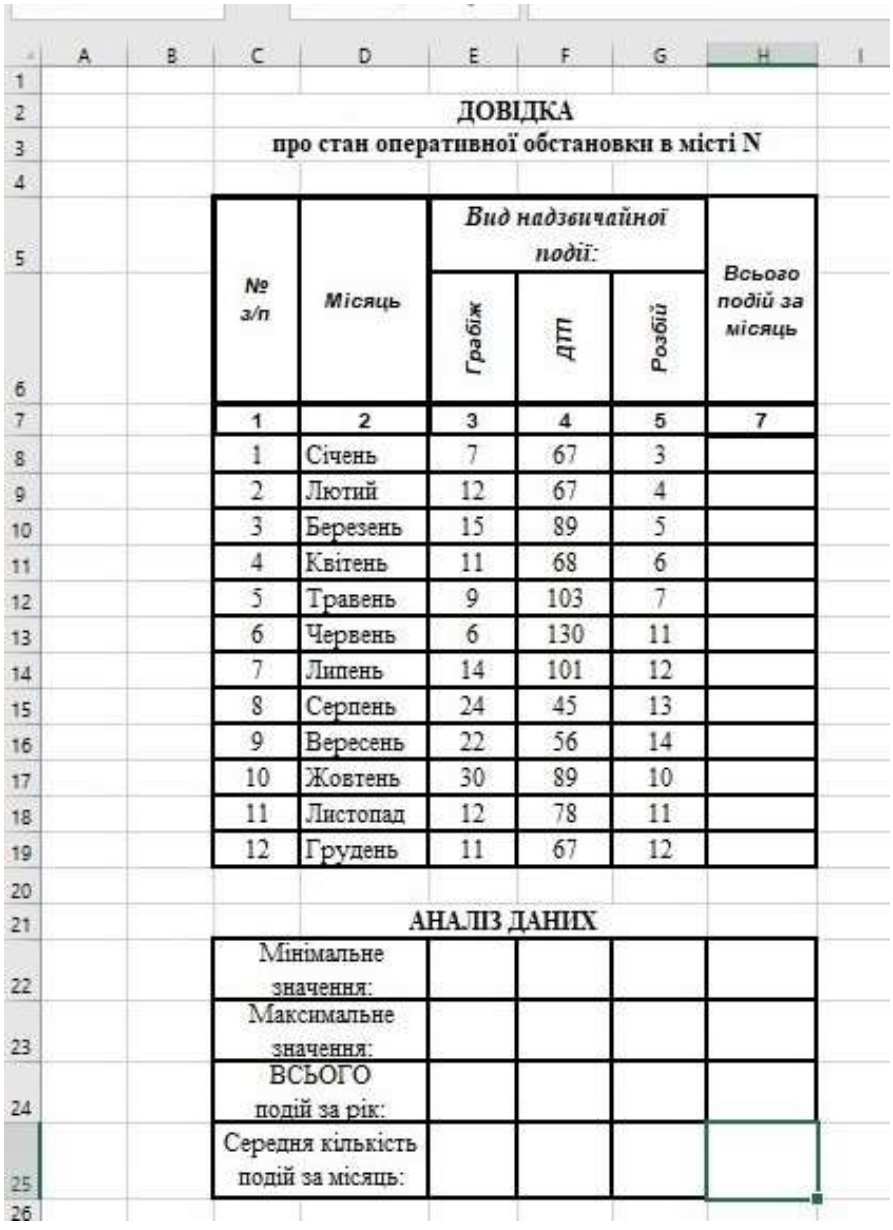
Оберіть t від -3 до 3 із кроком 0,1.

Практичне заняття № 3.4

Мета заняття: поглибити практичні навички здобувачів щодо використання засобів графічного уявлення даних Microsoft Excel для візуалізації результатів наукових досліджень.

Завдання:

1. Створити за допомогою програми Excel файл з назвою **Ваше прізвище_П.з. 3.4**.
2. Встановити **пароль** на файл.
3. Створіть таблицю, як показано на малюнку нижче, та заповнити її з використанням належних формул.
4. Побудувати лінійну діаграму для грабіжів, ДТП, розбоїв. Для ДТП побудувати лінію тренду «Лінійну».



ДОВІДКА
про стан оперативної обстановки в місті N

№ з/п	Місяць	Вид надзвичайної події:			Всього подій за місяць
		Грабіж	ДТП	Розбій	
1	2	3	4	5	7
1	Січень	7	67	3	
2	Лютий	12	67	4	
3	Березень	15	89	5	
4	Квітень	11	68	6	
5	Травень	9	103	7	
6	Червень	6	130	11	
7	Липень	14	101	12	
8	Серпень	24	45	13	
9	Вересень	22	56	14	
10	Жовтень	30	89	10	
11	Листопад	12	78	11	
12	Грудень	11	67	12	

АНАЛІЗ ДАНИХ

Мінімальне значення:				
Максимальне значення:				
ВСЬОГО подій за рік:				
Середня кількість подій за місяць:				

Список використаних і рекомендованих джерел

1. Кудінов В. А., Пакриш О. Є., Смаглюк В. М., Хахановський В. Г. Інформаційні технології в правозастосовній діяльності : підручник / за заг. ред. В. А. Кудінова. Київ : Нац. акад. внутр. справ, 2018. 176 с.

2. Інформатика в юридичній діяльності (частина 2) : підручник / [В. А. Кудінов, І. М. Мельников, О. Є. Пакриш та ін.] / за заг. ред. В. А. Кудінова. Київ, 2017. 332 с.

3. Кудінов В. А., Пакриш О. Є. Інформаційні технології в психології : навч. посіб. Київ, 2017. 88 с.

4. Інформаційні технології в науково-педагогічній діяльності : навч. посіб. / [В. А. Кудінов, В. Г. Хахановський, О. Є. Пакриш та ін.] / за заг. ред. В. А. Кудінова. Київ, 2017. 80 с.

5. Носенко Т. І. Інформаційні технології навчання : навч. посіб. Київ, 2011. 184 с.

6. Нелюбов В. О., Куруца О. С. Основи інформатики. Microsoft PowerPoint 2016 : навч. посіб. Ужгород : ДВНЗ «УжНУ», 2018. 122 с.

РОЗДІЛ IV
АВТОМАТИЗОВАНІ СИСТЕМИ ДОКУМЕНТООБІГУ. ІНФОРМАЦІЙНІ БАЗИ ТА БАНКИ ДАНИХ

4.1. Автоматизовані системи документообігу

Законом України «Про електронні документи та електронний документообіг» визначено, що *електронний документ* – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [2]. Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для сприймання його змісту людиною.

Електронний документообіг (обіг електронних документів) – одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів [2].

Електронний документообіг охоплює життєвий цикл електронних документів в організації, починаючи від їх отримання (введення, електронна пошта і т.ін.), проходження в підрозділах зі зміною стану (доведений до відома, узгоджений, підписаний, в роботі, закритий і т.ін.) і закінчуючи списанням в архів. Часто електронний документообіг позначається терміном workflow, який характеризує рух документів як потік робіт, що виконуються в межах того чи іншого управлінського процесу.

Функції електронного документообігу реалізують автоматизовані системи документообігу, тобто програмне забезпечення, головним завданням якого є організація і підтримка життєвого циклу електронних документів.

Основні принципи електронного документообігу:

- Однократна реєстрація документа, що дозволяє однозначно ідентифікувати документ в будь-якій інсталяції даної системи.
- Можливість паралельного виконання операцій, що дозволяє скоротити час руху документів і підвищення оперативності їх виконання.
- Безперервність руху документа, що дозволяє ідентифікувати відповідального за виконання документа (завдання) в кожен момент часу життя документа (процесу).
- Єдина (або погоджено розподілена) база документів, що дозволяє унеможливити дублювання документів.
- Ефективно організована система пошуку документа, що дозволяє знаходити документ, володіючи мінімальною інформацією про нього.
- Розвинена система звітності по різних статусах і атрибутах документів, що дозволяє контролювати рух документів по процесах документообігу і приймати управлінські рішення, ґрунтуючись на даних із звітів.

Найбільш поширеними в Україні є такі автоматизовані системи документообігу:

- Система електронного документообігу **e-Docs** (www.elgnc.com.ua).
- Система електронного документообігу та автоматизації бізнес-процесів Megapolis.DocNet (www.inbase.com.ua).
- Система електронного документообігу **MasterDoc** (www.bkc.com.ua).
- Система електронного документообігу **ДІЛО** (www.eos.com.ua).
- Система електронного документообігу **FossDoc** (www.fossdoc.com.ua).
- Система електронного документообігу **АСКОД** (www.infoplus.ua).
- Система електронного документообігу **SX-Government** (www.sx-ua.com).
- Система електронного документообігу **Optima-WorkFlow-Стандарт** (www.iisd.com.ua).

Розглянемо *можливості систем електронного документообігу* на прикладі FossDoc [1].

Система електронного документообігу **FossDoc –** це рішення на платформі FossLook, призначене для створення електронного архіву документів, організації корпоративного документообігу (workflow) і автоматизації управлінських процесів на підприємствах, в установах і організаціях будь-якого роду діяльності. Програма дозволяє вирішити велику кількість завдань, реалізація яких покладена на відповідні модулі. Система може бути легко перелаштована з урахуванням специфіки роботи кожної конкретної установи.

Програмне забезпечення побудовано на основі класичної клієнт-серверної архітектури. В його склад входять (рис. 4.1):

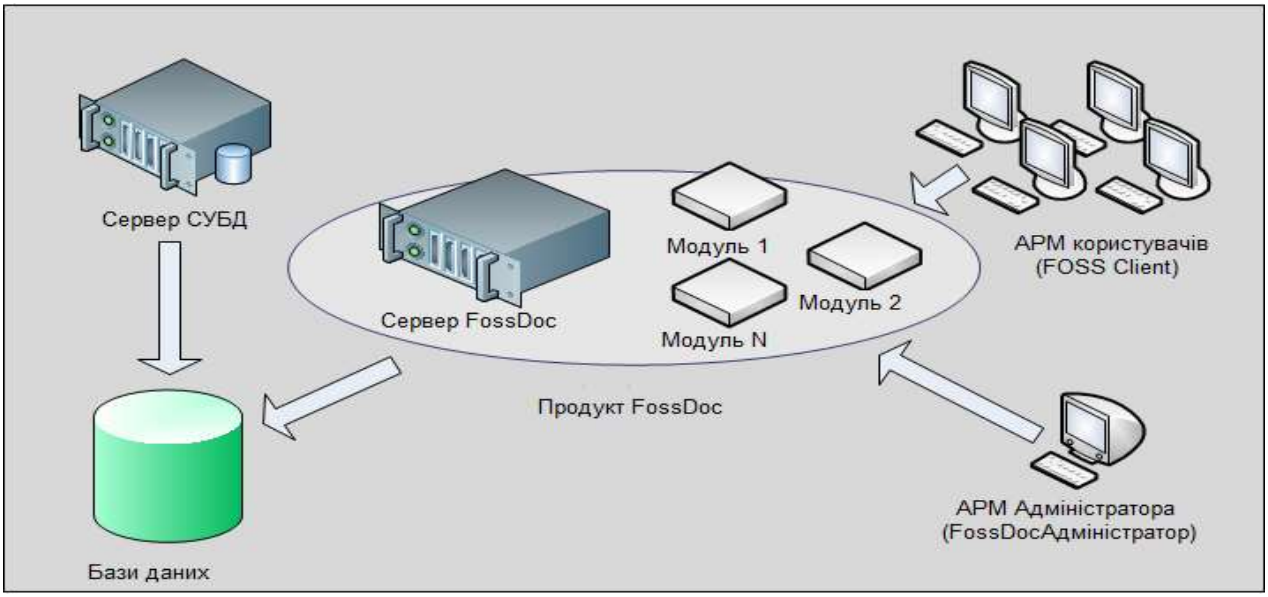


Рис. 4.1. Побудова FossDoc

– **Сервер FossDoc** – сервер додатків, який реалізує логіку і здійснює взаємодію клієнтських програм з сервером системи управління базами даних (далі – СУБД). Модулі, що визначають функції системи, підключаються до сервера додатків. Таким чином, продукти розрізняються серверними частинами, які містять різні набори модулів.

– **Web-сервер –** дозволяє працювати з сервером додатків за допомогою звичайного веббраузера. Реалізований у вигляді зовнішнього модуля, що підключається до сервера додатків.

– **База даних** – управляється за допомогою сервера СУБД (My SQL, Microsoft SQL Server або Oracle). Зберігає документи, довідники, інформацію про користувачів, налаштуваннях і т.ін.

– **FossDoc Client** – клієнтський windows-додаток, АРМ користувача. За допомогою цієї програми звичайний користувач підключається до сервера додатків (по локальній мережі або Інтернету) і вирішує свої службові завдання, як співробітник підприємства (організації). Одночасно АРМ користувача є поштовим клієнтом і може приймати-відправляти листи за допомогою зовнішніх поштових серверів.

– **FossDoc Web Client** – вебінтерфейс (вебклієнт), який реалізує ті ж функції робочого місця користувача, що і windows-програма FossDoc Client, за допомогою звичайного веббраузера. Роботу вебклієнта забезпечує вебсервер системи.

– **FossDoc Адміністратор** – клієнтська програма, майстер адміністрування (АРМ адміністратора). За допомогою даного програмного забезпечення проводиться адміністрування сервера додатків (введення користувачів, розподіл прав доступу, підключення додаткових функцій, проектування маршрутів, створення нових типів документів і т.ін.).

Система автоматизує всі аспекти сучасного діловодства: створення реєстраційно-контрольних карток документа; відправку доручень (аналог «бігунка» в звичайному документообігу); облік паперових оригіналів за допомогою спеціальних журналів; здійснення контролю над виконанням документів; підготовку резолюцій; роботу з електронно-цифровим підписом, генерацію звітів (рис. 4.2).

Все різноманіття документів, з якими працюють користувачі, розділяється на окремі категорії – типи документів. В системі існують зумовлені типи документів (поширені у вітчизняному діловодстві): вхідні та вихідні листи, звернення громадян, службові записки, накази і т.ін. Документи можуть посилатися на інші документи або бути дочірніми по відношенню до головних. Поля документів можуть заповнюватися значеннями з довідників (рис. 4.3).

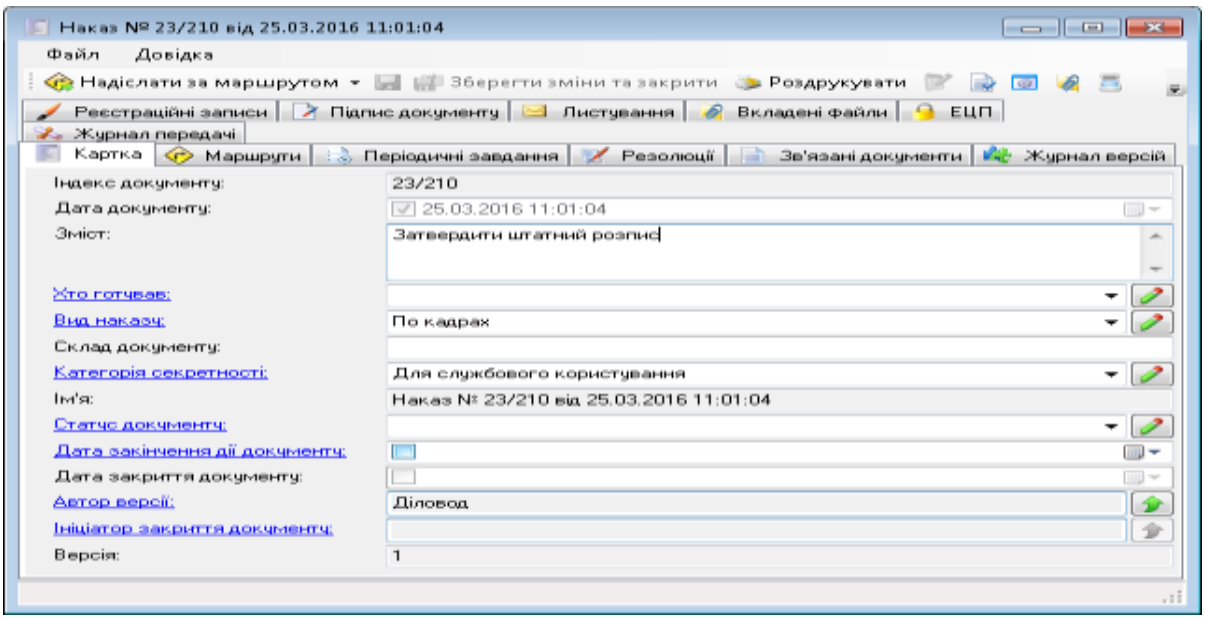


Рис. 4.2. Автоматизація діловодства

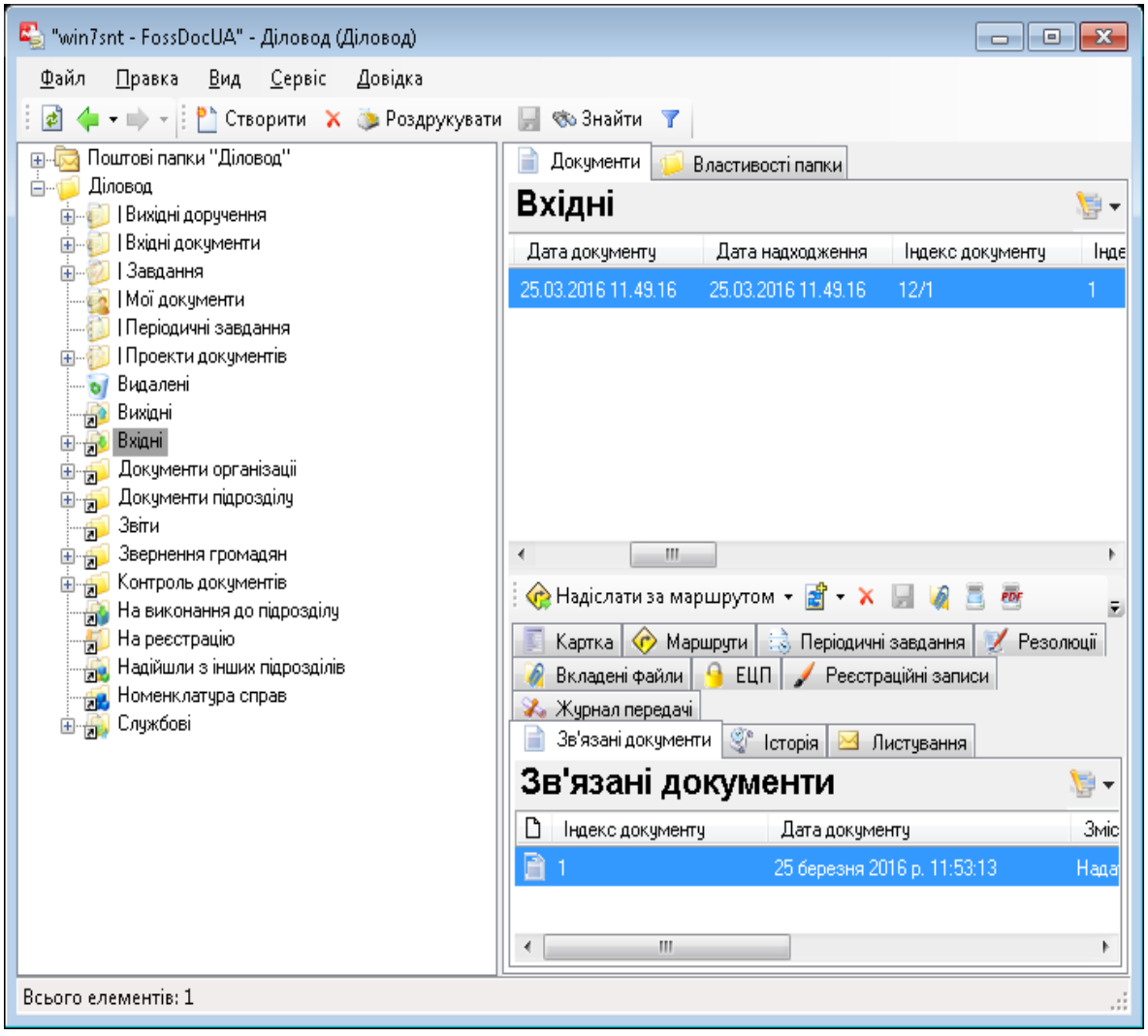


Рис. 4.3. Підтримка різних типів документів

Також існує можливість налаштувати програму за допомогою функціональності бібліотек документів: додати або видалити поля і/або функції документів, налаштувати довідники. Можна спроектувати власні типи документів, а також шаблони друкарських форм, які будуть відповідати тільки певному діловодству. Система дозволяє створювати нові документи на базі існуючих, використовуючи механізм успадкування (рис. 4.4).

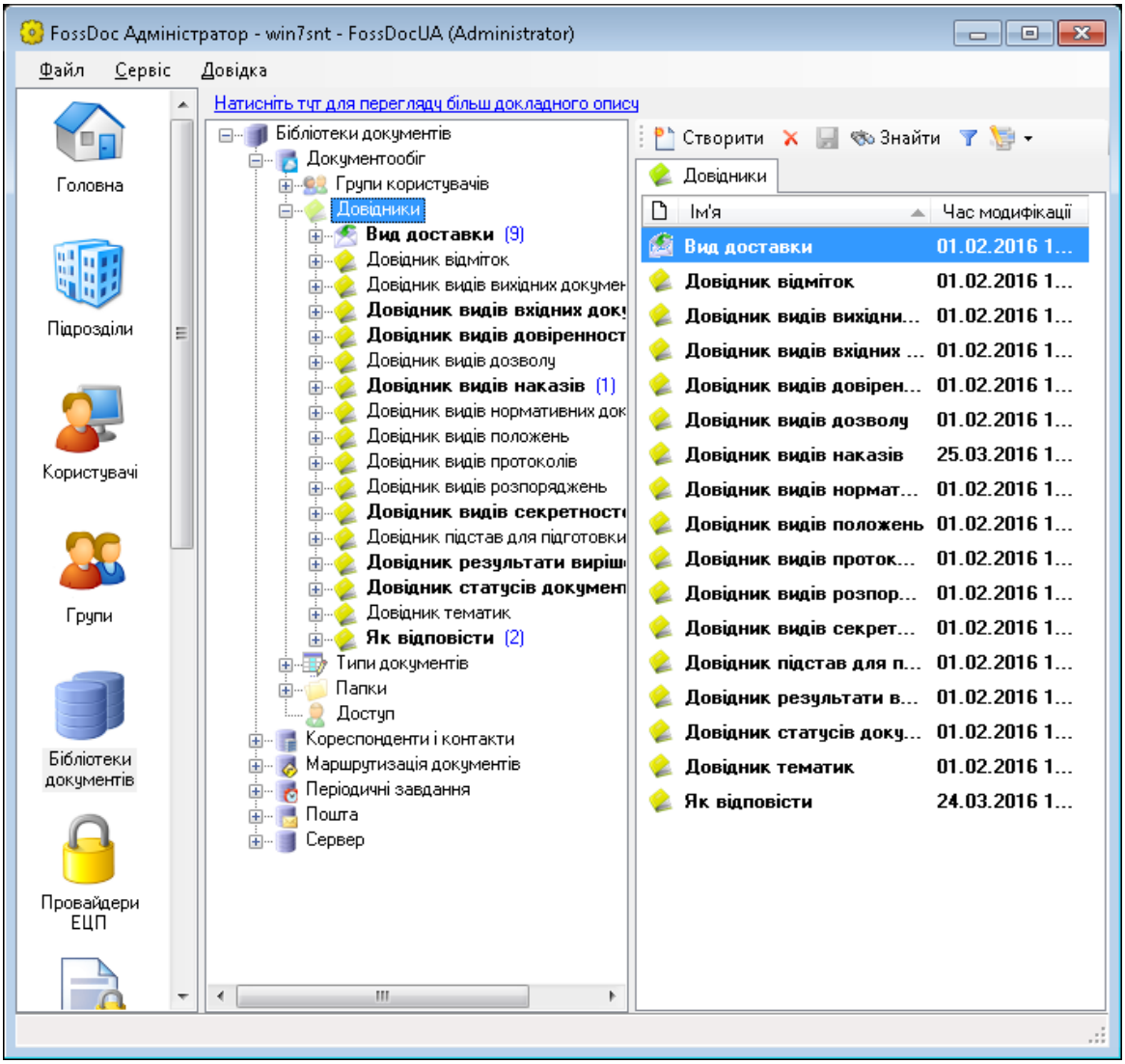


Рис. 4.4. Проєктування документів

Система дозволяє гнучко налаштувати маршрути руху документів між підрозділами установи, вказати їх порядок виконання, узгодження, підпису, реєстрації і т.ін. Можна налаштувати реєстрацію в декількох канцеляріях. Підтримується ефективний механізм створення документа на основі його проекту з фіксацією кожної стадії узгодження в окремій версії проекту.

За допомогою довідника підрозділів проектується віртуальна структура організації будь-якої складності. Рольова модель поведінки користувачів дозволяє співробітникам швидко освоїти функції системи і ефективно замінювати одного користувача іншим. Надаються потужні засоби розподілу доступу до загальних ресурсів і колективної роботи над документами (рис. 4.5).

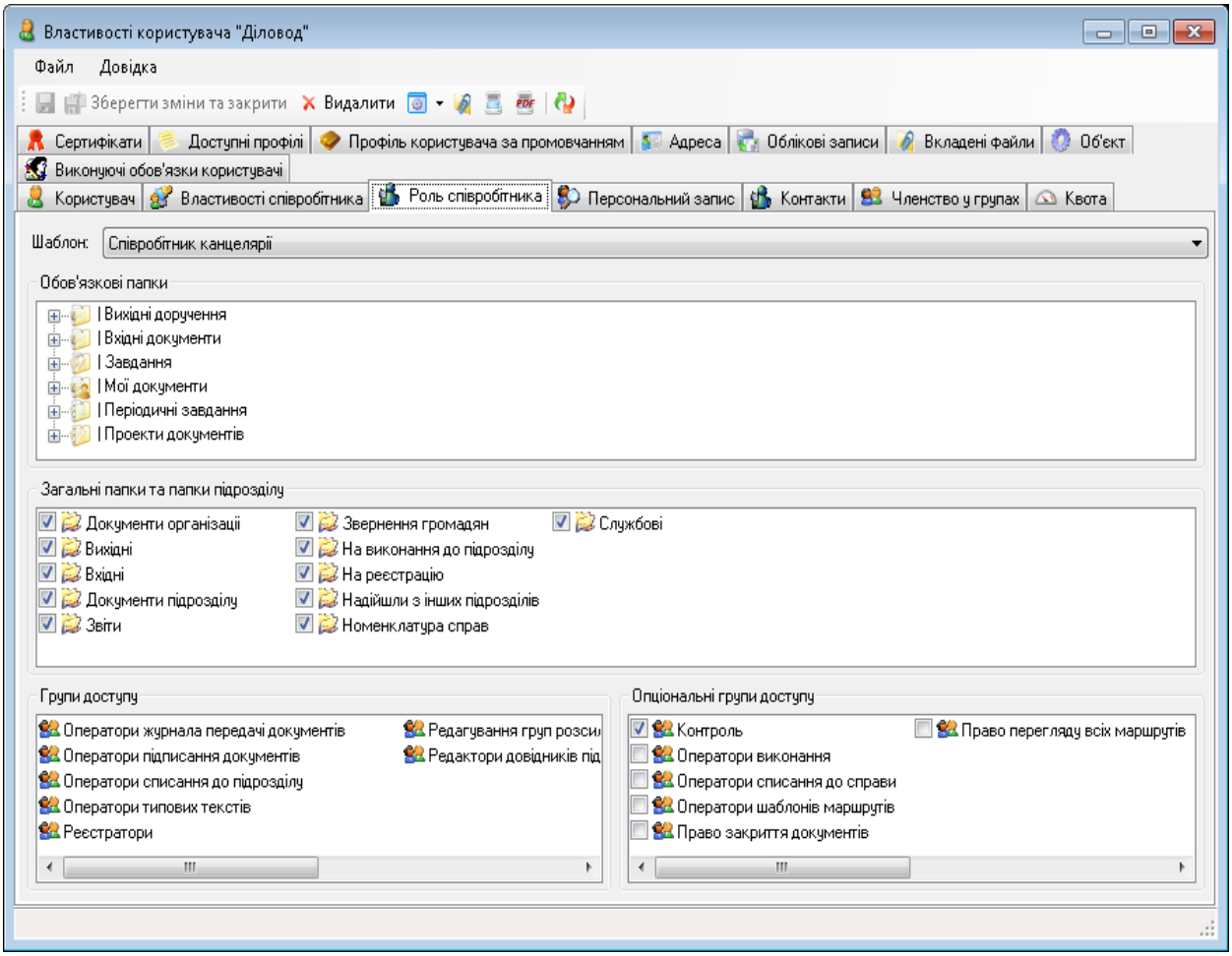


Рис. 4.5. Підтримка колективної роботи користувачів

Поштовий сервер системи призначений для створення “внутрішніх” поштових скриньок користувачів (на домені установи) і роботи з ними – прийому/відправки повідомлень. Сервер також ініціює прийом повідомлень з інших поштових серверів (ukr.net, gmail.com і т.п.), а також відправку ними повідомлень, якщо у користувачів, зареєстрованих на сервері, є зовнішні поштові скриньки.

В системі підтримується робота з електронним цифровим підписом. Такий підпис гарантує цілісність і автентичність відбитку даного документа. Ніхто, крім автора документа, не зможе внести зміни в нього так, щоб про це не стало відомо під час перевірки електронного цифрового підпису.

4.2. Інформаційні бази та банки даних

При побудові інформаційних масивів використовують *файлову організацію* або *організацію у вигляді бази даних*.

Файлова організація передбачає спеціалізацію та збереження інформації, орієнтованої, як правило, на одну прикладну задачу, та забезпечується

прикладним програмістом. Така організація дозволяє досягнути високої швидкості обробки інформації, але характеризується рядом *недоліків*.

Характерна риса файлового підходу – вузька спеціалізація як обробних програм, так і файлів даних, що служить причиною великої надлишковості, тому що ті самі елементи даних зберігаються в різних системах. Оскільки керування здійснюється різними особами (групами осіб), відсутня можливість виявити порушення суперечливості збереженої інформації. Розроблені файли для спеціалізованих прикладних програм не можна використовувати для задоволення запитів користувачів, які перекривають дві і більше області. Крім того, файлова організація даних внаслідок відмінностей структури записів і форматів передання даних не забезпечує виконання багатьох інформаційних запитів навіть у тих випадках, коли всі необхідні елементи даних містяться в наявних файлах. Тому виникає необхідність відокремити дані від їхнього опису, визначити таку організацію збереження даних з обліком існуючих зв'язків між ними, яка б дозволила використовувати ці дані одночасно для багатьох застосувань.

Вказані причини обумовили появу баз даних.

База даних – це іменована сукупність даних, що відображає стан об'єктів та їх взаємозв'язків у визначеній предметній області (ст. 1 Закону України «Про Національну програму інформатизації») [3]. Або: *база даних* – це сукупність даних, матеріалів або творів у формі, яку читає машина (ст. 4 Закону України «Про авторське право і суміжні права» від 23.12.1993 р.) [4]. *База даних* – це організована структура, яка призначена для зберігання інформації.

Дані у базі взаємопов'язані. Це полегшує доступ до інших даних цієї групи, коли вже відкриті якісь дані.

Система управління базами даних – це комплекс програмних засобів, які забезпечують створення структури бази даних, ведення бази даних, взаємодію користувача з базою даних.

СУБД – це комплекс програмних засобів, призначених для створення структури нової бази даних, наповнення її вмістом, редагування вмісту і візуалізації інформації. Під візуалізацією інформації розуміється добір відображуваних даних відповідно до заданого критерію, їхнє впорядкування, оформлення і подальша видача на пристрої виводу або канали зв'язку.

Банк даних – це сукупність бази даних та системи управління базами даних. *Банк даних* – це заснована на технології БД система програмних, мовних, організаційних і технічних засобів, призначених для централізованого нагромадження і колективного використання даних.

Вимоги до баз даних: 1) актуальність; 2) повнота; 3) вірогідність.

Основні властивості баз даних:

1. Для даних допускається така мінімальна надлишковість, що сприяє їх оптимальному використанню в одному чи кількох застосуваннях.

2. Незалежність даних від програм.

3. Для пошуку та модифікації даних використовуються спільні механізми.

4. Як правило, у складі БД існують засоби для підтримки її цілісності та захисту від несанкціонованого доступу. Є також механізми перевірки змісту даних.

Прокоментуємо додатково вищенаведені властивості порівнюючи в основному з близьким попередником БД – файловими системами (далі – ФС).

На відміну від ФС БД зорієнтована для підтримки даних для кількох застосувань. Взаємопов'язаність даних полягає в тому, що доступ до певної групи даних якогось застосування загалом полегшує доступ до інших груп даних цього ж застосування. В умовах орієнтації БД на велику кількість застосувань виникає необхідність у підтримці значного числа різноманітних зв'язків між даними.

Вимога *мінімізації надлишковості* полягає у мінімальній кількості копій для одних і тих же даних з урахуванням орієнтації на кілька застосувань. Ці надлишкові копії використовуються для підтримки зв'язків між даними. Як приклад, розглянемо відомості, що зберігаються у відділі кадрів деякого підприємства про своїх співробітників. Користувачами цієї інформації виступають адміністрація, профспілкова організація та бухгалтерія підприємства. Адміністрацію цікавлять дані про кваліфікацію, професійний рівень і досвід роботи, профспілки використовують відомості соціально-побутового характеру, а бухгалтерія оброблює ті дані, що потрібні для нарахувань заробітної плати та підрахунку податків, інших нарахувань та відрахувань. Хоча інформація і різнорідна, але все ж має значну спільну частину. Всім користувачам потрібні службовий номер, прізвище, ім'я, по-батькові співробітника, його рік народження, дані про умови праці. Інформація про сімейний стан та склад сім'ї використовується бухгалтерією і профспілками. Якщо для зберігання даних застосувати технологію ФС, то можливі два крайні варіанти:

а) незалежні один від одного файли, відсортовані згідно з потребами того чи іншого користувача, передбачають значну надлишковість даних;

б) всі дані знаходяться у одному файлі, відсортованому так, як потрібно одному з користувачів (наприклад, адміністрації) – надлишковість при цьому практично відсутня, але зручно працювати тільки одному з користувачів.

Концепція БД займає проміжне становище між вищеописаними крайніми позиціями. Зайва надлишковість має кілька *недоліків*:

По-перше, зберігання кількох копій веде до додаткових витрат пам'яті.

По-друге, доводиться виконувати численні операції оновлення для кількох надлишкових копій.

Крім того, оскільки різні копії даних можуть відповідати різним стадіям оновлення, то інформація, що зберігається в системі на певний час може стати суперечливою.

Про *незалежність даних* часто говорять, як про одну з основних властивостей БД. Під цим поняттям розуміється можливість зміни структури даних без зміни програм, що її використовують, а також рівень

самоінтерпретованості даних. Міра незалежності даних тісно пов'язана з ступенем необхідної деталізації відомостей про організацію їх зберігання.

Під *цілісністю* БД розуміють несуперечливість між собою даних, що в ній зберігаються. Наприклад, для кадрових відомостей рік народження співробітника не може бути більшим року призначення на посаду або поточного року. Щоб запобігти виникненню таких ситуацій при модифікації і поповненнях БД, співвідношення між даними контролюються спеціальними засобами підтримки цілісності БД. Специфікація подібних умов, що накладаються на дані і відслідковуються при будь-яких їх оновленнях, покладаються на спеціальну службу адміністратора бази даних (далі – АБД), а системи управління базами даних надають інструментальні засоби, які забезпечують службі АБД можливість виконання її функцій.

Оскільки однією з основних властивостей БД є орієнтація на широке коло застосувань, то природно передбачити засоби захисту від неавторизованого доступу (навмисного чи ненавмисного) користувачів до даних. З цією метою в БД встановлюється система паролів та ідентифікацій користувачів, а також розподіл даних і користувачів на групи з різними взаємними правами.

Інформаційна система – це система, яка організовує накопичення і оперування інформацією у певній області. Як відомо, законодавче визначення: «*Інформаційна (автоматизована) система* – це організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів». Багато видів сучасних інформаційних систем побудовані на технологіях баз даних.

***Класифікація інформаційних систем*:**

– за призначенням (документальні, фактографічні та змішані);

– за мовами (замкнуті системи, системи з базовою мовою, змішані);

– за локалізацією (локальні та розподілені);

– за схемою додаткової обробки даних (з постобробкою, з попередньою обробкою);

– за структурами даних (ієрархічні, мережного типу, реляційні).

Розглянемо по черзі і детальніше кожний з критеріїв.

1. ***За призначенням*** (документальні, фактографічні та змішані).

Документальні системи зорієнтовані на обробку та зберігання документа (порівняно великої за розміром послідовності символів), внутрішню структуру якого система (майже) повністю ігнорує, тобто він неподільний (атомарний) з точки зору системи. Споживачем результатів пошуку виступає, як правило, кінцевий користувач.

Документальні (або дескрипторні) автоматизовані інформаційні системи (далі – ДАІС) історично були першими. Спочатку їх мовою була нічим не обмежена природна мова. Перші ДАІС були призначені для пошуку книг та документів у бібліотеках і великих сховищах, тому їх і назвали документографічними.

Основним елементом інформаційного простору ДАІС була анотація або реферат книги, документа, явища чи об'єкта. Реферат повинен відображувати ті

риси, які цікавлять користувача (як правило – людини). В ньому виділяються слова чи словосполучення, які в сукупності майже однозначно (в ідеалі точно) відповідають повному опису об'єкта. Крім того, таких слів повинно бути відносно небагато. Їх називають ключовими словами або дескрипторами. Запит для ДАІС можна сформулювати у вигляді переліку дескрипторів, який на думку користувача характеризує потрібний реферат, а значить, і відповідний об'єкт. Алгоритм формування відповіді послідовно порівнює запит з кожним рефератом і вибирає такі, що пройшли порівняння. В таких системах запит називають пошуковим розпорядженням, а реферат – пошуковим образом.

Фактографічні системи оперують фактами (даними) різних типів, що зв'язані в системі в більш чи менш складні структури. Дані, що є результатом пошуку, можуть стати складовою частиною звітів або використовуються різноманітними обчислювальними процесами.

Змішані системи включають в себе в тих чи інших пропорціях риси обох вищеназваних варіантів. Переважну більшість сучасних систем слід віднести до категорії змішаних.

Звичайно, наведені описові характеристики не дають можливості чітко визначитись у випадку класифікації кожної конкретної інформаційної системи, але дозволяють зробити перші грубі припущення. Для більш точних класифікаційних оцінок необхідно враховувати додаткові властивості, що відносяться до пошукового процесу, а також до особливостей мов запитів, реалізованих в тій чи іншій системі.

2. ***За мовами*** (замкнуті системи, системи з базовою мовою та змішані).

Замкнуті системи самостійно забезпечують користувача всіма необхідними засобами як для локалізації даних, так і для їх постпошукової чи передпошукової обробки. Недоліком таких систем є те, що в них відсутні (або малоефективні) засоби для розробки надбудов – проблемно-орієнтованих комплексів.

Системи з базовою мовою передбачають взаємодію користувача з системами управління базами даних з середовища якоїсь іншої мови програмування, де і виконуються більшість постпошукових перетворень даних. Такий підхід зручний для розробки різного роду систем як надбудов над СУБД, бо дає можливість створювати високоефективні програми постпошукової обробки даних.

Змішані системи передбачають наявність обох можливостей двох попередніх підходів і є найбільш поширеними на сьогодні.

3. ***За локалізацією*** (локальні та розподілені).

Локальність передбачає розташування всього програмного забезпечення і даних на одному ізольованому комп'ютері, а розподіленість означає розташування системи на мережі комп'ютерів з певною стратегією рознесення даних.

4. ***За схемою додаткової обробки*** (з постобробкою, з попередньою обробкою).

Головним призначенням будь-якої системи баз даних є підтримка функцій локалізації даних, що зберігаються, але дуже важливою властивістю, що може значно підняти інтерфейсний рівень системи, є наявність *постобробки даних* після їх локалізації в базі даних чи *попередньої обробки*.

5. ***За структурами даних*** (ієрархічні, мережного типу, реляційні).

В основі організації бази даних є модель логічного рівня, яка підтримується засобами конкретної СУБД і визначає правила, згідно з якими структуруються дані. Це зовнішній рівень моделювання. За допомогою зазначеної моделі подається велика кількість даних і описуються взаємозв'язки між ними. Структури даних, що підтримуються в системі бази даних, – це важливий фактор, що впливає, як на виразову потужність, так і на ефективність функціонування.

Ієрархічна модель даних будується на основі принципу підпорядкованості елементів даних і є деревоподібною структурою, що складається з вузлів (сегментів) і дуг (гілок). Дерево в ієрархічній структурі впорядковане за чинними правилами розміщення його сегментів і гілок:

– на верхньому рівні перебуває один сегмент – кореневий (вихідний);

– сегмент другого рівня – породжений – залежить від першого, вихідного;

– доступ до кожного породженого (крім кореневого) відбувається через його вихідний сегмент;

– кожен сегмент може мати по кілька примірників конкретних значень елементів даних, а кожен елемент породженого сегмента пов'язаний з примірником вихідного і створює один логічний запис;

– примірник породженого сегмента не може існувати самостійно, тобто без кореневого сегмента;

– при вилученні примірника кореневого сегмента також вилучаються всі підпорядковані і взаємопов'язані з ним примірники породжених сегментів.

Мережева модель даних являє собою орієнтований граф з пойменованими вершинами та дугами. Вершини графа – записи, що є пойменованою сукупністю логічних взаємопов'язаних елементів даних або агрегатів даних. Під агрегатом даних розуміють пойменовану сукупність елементів даних, які є всередині запису.

Для кожного типу записів може бути кілька примірників конкретних значень його інформаційних елементів. Два записи, взаємопов'язані дугою, створюють набір даних. Запис, з якого виходить дуга, називається власником набору, а запис, до якого вона спрямована, – членом набору.

В останні десятиріччя найбільшого розповсюдження зазнали СУБД *реляційного типу*, для яких характерна найпростіша структура даних (плоский файл). Концепція реляційних баз даних була розроблена Є. Ф. Коддом у 1970 р. на основі математичної теорії відношень (відношення – relation).

Реляційна модель даних являє собою набір двовимірних плоских таблиць, що складаються з рядків і стовпців. Первинний документ або лінійний масив являє собою плоску двовимірну таблицю. Така таблиця називається відношенням, кожен стовпець – атрибутом, сукупність значень одного типу (стовпця) – доменом, а рядка – кортежем. Стовпці таблиці є традиційними елементами даних, а рядки – записами. Таблиці (відношення) мають імена.

Імена присвоюються також і стовпцям таблиці. Кожний кортеж (запис) відношення має *ключ*. Ключі бувають прості та складні. *Простий ключ* – це

ключ, який складається з одного атомарного атрибута, значення якого унікальне (не повторюється).

Складний ключ складається з двох і більше атрибутів. Для зв'язків відношень одного з одним у базі даних є *зовнішні ключі*. Атрибут або комбінація атрибута відношення є зовнішнім ключем, якщо він не є основним (первинним) ключем цього відношення, але є первинним ключем для іншого відношення.

Внутрішній рівень пов'язаний з фізичним розміщенням даних у пам'яті обчислювальної техніки. На цьому рівні формується фізична модель бази даних, яка містить структури зберігання даних у пам'яті і включає опис форматів записів, їхнє логічне чи фізичне впорядкування, розміщення за типами пристроїв, а також характеристики і шляхи доступу до даних. Запит оформляється за певною формою та охоплює назву даних, період часу, за який потрібні дані, а також структуру та зміст відео- або документограм.

Від параметрів фізичної моделі залежать такі характеристики бази даних: обсяг пам'яті та час реакції системи. Фізичні параметри бази даних можна змінювати в процесі її експлуатації (не змінюючи при цьому опису інших рівнів) з метою підвищення ефективності функціонування системи.

Користувачі інформаційної системи (бази даних) – це особи, які працюють з інформаційною системою і використовують відомості, що містяться у базах даних. Їх умовно можна розділити на такі групи:

– *внутрішні* (розробляють інформаційну систему і підтримують її функціонування);

– *кінцеві* (спеціалісти, які, як правило, не мають хорошої підготовки в області програмування, але які користуються БД у своїй повсякденній роботі; для цих користувачів і розробляються БД).

У свою чергу внутрішні користувачі поділяються на:

– *адміністратора бази даних* (на стадії проектування – це ідеолог і головний конструктор системи; на стадії експлуатації – це відповідальна особа за функціонування інформаційної системи, керує режимом використання даних, відповідає за збереження даних, розробляє заходи щодо захисту даних від руйнування, забезпечення їх достовірності і ефективного використання);

– *системних програмістів* (забезпечують контроль за функціонуванням банку даних, розробляють програми, що розширюють можливості СУБД);

– *прикладних програмістів* (розробляють програми обробки даних, що містяться в БД, відповідно до потреб кінцевих користувачів). При експлуатації простих БД функції трьох категорій внутрішніх фахівців реалізуються однією людиною.

Створена велика кількість СУБД (dBase, FoxBase, Paradox, FoxPro, Microsoft Access, Oracle тощо). Вони мають близькі можливості, здатні працювати з багатьма форматами представлення даних, здійснювати експорт і імпорт даних завдяки наявності значного числа конвертерів. Загальноприйнятими також є технології, що дозволяють використовувати можливості інших додатків, наприклад, текстових редакторів, пакетів побудови графіків і т.ін., мають

вбудовані версії мов високого рівня і засоби візуального програмування інтерфейсів для різних об'єктів, що створюються.

Усе це дає можливість розглянути одну систему (наприклад, Microsoft Access) та узагальнити її поняття, прийоми і методи на весь клас СУБД.

Microsoft Access – це функціонально повна реляційна СУБД. У ній передбачені усі необхідні засоби для визначення й обробки даних, а також для керування ними при роботі з великими обсягами інформації.

Функції:

– визначення (завдання структури й опис) даних;

– обробка даних;

– управління даними.

Об'єкти бази даних:

– таблиці – основний об'єкт будь-якої бази даних;

– запити – для вибирання даних з таблиць і надання їх користувачу у зручному вигляді. Виконують добір даних, сортування і фільтрацію. За допомогою запитів можна виконувати перетворення даних за заданим алгоритмом, створювати нові таблиці і т. ін.;

– форми – засіб для введення даних;

– звіти – схожі на форми, але призначені для виводу на друк;

– сторінки – об'єкт, що виконаний у коді HTML, розміщений на Web-сторінці і переданий клієнту разом з нею. Здійснюють інтерфейс між клієнтом, сервером і базою даних, розміщеною на сервері;

– макроси та модулі – для автоматизації повторюваних операцій та створення нових функцій шляхом програмування.

Таблиці. Таблиця бази даних схожа на електронну таблицю, в якій дані зберігаються в рядках і стовпцях. В результаті зазвичай досить легко імпортувати електронну таблицю до таблиці бази даних. Головна відмінність між збереженням даних в електронній таблиці та базі даних – це спосіб упорядкування даних.

Щоб забезпечити максимальну гнучкість бази даних, дані необхідно впорядкувати в таблицях, щоб позбутися зайвих елементів.

Наприклад, якщо потрібно зберігати дані про працівників, відомості про кожного працівника необхідно один раз ввести в таблиці, яка настроєна лише для розміщення даних про працівників. Цей процес називається оптимізацією.

Кожний рядок у таблиці називається записом. Записи – це місце розташування окремих елементів даних. Кожний запис складається з одного або кількох полів. Поля відповідають стовпцям у таблиці. Наприклад, можна створити таблицю «Працівники», де кожний запис (рядок) зберігає відомості про окремого працівника, а кожне поле (стовпець) містить власний тип даних, наприклад ім'я, прізвище, адресу тощо. Поля мають містити певний тип даних: текст, дату або час, число або інший тип.

Ще один спосіб опису записів і полів: уявіть старий картковий каталог у бібліотеці. Кожна картка у ящику відповідає запису бази даних. Кожний елемент даних на окремій картці (автор, назва тощо) відповідає полю БД.

Форми. Форми іноді називаються «екранами вводу даних». Це інтерфейси, які використовуються під час роботи з даними, тому вони часто містять кнопки для виконання різних команд. Можна створити БД без використання форм, просто редагуючи дані в таблицях даних. Проте більшість користувачів баз даних використовують форми для перегляду, введення та редагування даних у таблицях.

Форми пропонують простий у використанні формат роботи з даним. Крім того, до них можна також додавати функціональні елементи, наприклад, кнопки. Ці кнопки можна настроїти для визначення даних, що відображатимуться у формі, відкриття інших форм або звітів та для виконання низки інших завдань. Наприклад, є форма «Форма клієнта», у якій виконується робота з даними клієнта. Форма клієнта може містити кнопку, яка відкриває форму замовлення, де можна ввести нове замовлення цього клієнта.

Форми також дають змогу керувати способом взаємодії інших користувачів із даними бази даних. Наприклад, можна створити форму, яка відображає лише певні поля та дозволяє виконувати лише певні операції. Це допомагає захистити дані та забезпечує належне введення даних.

Звіти. Звіти використовуються для зведення та представлення даних у таблицях. Звіт зазвичай відповідає на певне питання, наприклад: «Яку суму було отримано від кожного клієнта цього року?» або «У яких містах розташовані наші клієнти?». Кожний звіт можна відформатувати таким чином, щоб він представляв дані найбільш зрозумілим способом.

Звіт можна запустити будь-коли і він завжди відображатиме поточні дані в базі даних. Звіти зазвичай мають формат для друку, але їх також можна переглядати на екрані, експортувати до іншої програми або надсилати електронною поштою.

Запити. Запити – це справжні робочі коники бази даних, які можуть виконувати багато різних функцій.

Їх найпоширеніша функція – отримання певних даних із таблиць. Дані, які потрібно переглянути, як правило, розташовані в кількох таблицях, і запити дають змогу переглянути їх в одній таблиці даних. Також, оскільки зазвичай не потрібно бачити всі записи одночасно, запити дозволяють додавати критерії для «фільтрування» даних, щоб переглядати лише потрібні записи. Запити часто виконують роль джерела записів для форм і звітів.

Певні запити є «оновлюваними», тобто дані в базових таблицях можна редагувати за допомогою таблиці даних запиту. Якщо дії виконуються з оновлюваним запитом, слід пам’ятати, що зміни, насправді, виконуються в таблицях, а не лише в таблиці даних запиту.

Запити поділяються на дві основні групи: запити на вибірку і запити на дію. Запит на вибірку просто отримує дані й робить їх доступними для використання. Результати запиту можна переглянути на екрані, роздрукувати або скопіювати до буфера обміну. Або можна використати результат запиту як джерело записів для форми чи звіту.

Запит на змінення, згідно з назвою, виконує з даними певне завдання. Запити на змінення можна використовувати для створення нових таблиць, додавання даних до наявних таблиць, оновлення або видалення даних.

Макроси. Макроси в програмі Microsoft Access можна вважати спрощеною мовою програмування, яку можна використовувати для додавання функціональності до бази даних. Наприклад, можна вкласти макрос до кнопки форми, щоб запускати макрос у разі натискання цієї кнопки. Макроси містять дії, які виконують завдання, наприклад, відкривають звіт, виконують запит або закривають базу даних. Більшість операцій із базою даних, які виконуються вручну, можна зробити автоматичними за допомогою макросів, тому вони можуть бути корисним засобом економії часу.

Модулі. Модулі, як і макроси, – це об'єкти, які можна використовувати для додавання функціональності до бази даних. Проте, якщо макроси Microsoft Access створюються за допомогою вибору зі списку дій макросу, модулі пишуться мовою програмування Visual Basic для застосунків (VBA). Модуль – це збірка декларацій, інструкцій і процедур, які зберігаються разом. Модуль може бути модулем класу або стандартним модулем. Модулі класу додаються до форм або звітів і зазвичай містять процедури, характерні для форми чи звіту, до яких вони додаються. Стандартні модулі містять загальні процедури, не пов'язані з жодним іншим об'єктом. Стандартні модулі відображаються в області переходів у розділі **Модулі**, проте модулі класу там не відображаються.

СУБД Microsoft Access працює з *даними таких типів* (типи полів таблиць):

– текстовий (255 символів у комірці);

– поле Мемо (для розміщення великих фрагментів тексту – до 65535 символів);

– числовий (збереження дійсних чисел);

– дата/час (календарні дати і поточний час);

– рахівник (лічильник);

– логічний (тільки два значення - "так" чи "ні");

– грошовий (тип даних для зберігання грошових сум);

– поле об'єкта OLE (об'єкти, що створені іншими додатками);

– гіперпосилання (спеціальне поле для збереження URL Web-об'єктів Internet);

– майстер підстановок – об'єкт налагодження, а не тип даних.

Властивості полів БД:

– ім'я поля – визначає, яким чином слід звертатись до даних цього поля при автоматичних операціях з базою даних (за замовченням імена полів використовуються в якості назв стовпців таблиць);

– тип поля – визначає тип даних, які можуть міститись у даному полі;

– розмір поля – визначає максимальну довжину (у символах) даних, які можуть міститись у даному полі;

– формат поля – визначає спосіб форматування даних у комірках, які належать полю;

– маска введення – визначає форму, в якій вводяться дані у поле (засіб автоматизації введення даних);

– підпис – визначає заголовок стовпця таблиці для даного поля (якщо підпис не вказаний, то у якості заголовка стовпця використовується властивість «Ім’я поля»);

– значення за замовчуванням – те значення, яке вводиться у комірки поля автоматично (засіб автоматизації введення даних);

– умова на значення – обмеження, що використовується для перевірки правильності введення даних (для даних числового типу, грошового типу та типу дата-час);

– повідомлення про помилку – текстове повідомлення, яке видається автоматично при спробі введення в поле помилкових даних (коли задана властивість «Умова на значення»);

– обов’язкове поле – визначає обов’язковість заповнення даного поля при наповненні бази;

– порожні рядки – дозволяє введення порожніх рядків;

– індексоване поле – при наявності цієї властивості всі операції, пов’язані з пошуком або сортуванням записів за значенням, яке зберігається у цьому полі, суттєво прискорюються.

Робота з програмою СУБД Microsoft Access

Починати роботу необхідно з *проектування* бази даних:

1. Визначити структуру бази даних, джерело даних, задачі бази даних.
2. Скласти перелік даних, розділити їх на групи, які стануть таблицями.
3. Визначити поля для кожної таблиці.
4. Визначити ключові поля.
5. Вибрати оформлення для форм і звітів.
6. Визначити умови вибору для запитів.

Після запуску програми Microsoft Access або після закриття БД без завершення роботи програми відображається вікно Microsoft Office:

У ньому можна розпочати створення нової бази даних, відкрити наявну базу даних, переглянути вміст вебсайту Office.com – тобто, скористатись усіма можливими діями програми Microsoft Access із файлом бази даних.

На вкладці **Створити** передбачено кілька способів створення нової БД:

– **Пуста база даних.** За бажанням можна почати роботу з нуля. Цей спосіб варто вибрати, якщо потрібна дуже особлива структура або наявні дані, які потрібно включити чи розмістити.

– **Інстальований у складі програми Microsoft Access шаблон.** Якщо для створення нового проекту потрібна основа, доцільно використати шаблон. У програмі Microsoft Access за замовчанням інстальовано кілька шаблонів.

– **Шаблон із вебсайту Office.com.** Окрім шаблонів, які постачаються у складі програми Microsoft Access, можна скористатися шаблонами з вебсайту Office.com. Для цього не потрібно навіть відкривати браузер – шаблони доступні на вкладці **Створити**.

Під час роботи в БД можна додавати поля, таблиці або частини додатку.

Це нова функція, яка дає змогу використовувати кілька пов’язаних об’єктів бази даних як один об’єкт. Наприклад, можна об’єднати таблицю та форму на основі таблиці.

Створення бази даних без використання шаблону

Якщо не потрібно використовувати шаблон, можна створити базу даних за допомогою власних таблиць, форм, звітів та інших об'єктів бази даних. Зазвичай потрібно виконати одну або обидві наведені нижче дії:

– Введення, вставлення або імпортування даних до таблиці, створюваної під час створення нової БД, і повторне виконання процесу з новими таблицями, які створюються за допомогою команди **Таблиця** на вкладці **Створення**.

– Імпортування даних з інших джерел і створення нових таблиць під час виконання цього процесу.

1. На вкладці **Файл** виберіть пункт **Створити** та натисніть кнопку **Нова база даних**.
2. У правій області в розділі **Пуста база даних** введіть ім'я файлу в поле **Ім'я файлу**. Щоб змінити вказане за замовчанням розміщення файлу, виберіть поруч із полем **Ім'я файлу** елемент **Пошук розміщення для бази даних** . Далі перейдіть до нового розміщення та натисніть кнопку **ОК**.
3. Натисніть кнопку **Створити**.

Програма Microsoft Access створює базу даних із пустою таблицею з іменем «Таблиця1», а потім відкриває цю таблицю у вікні табличного подання даних. Курсор розташовано в першій пустій клітинці у стовпці. Щоб додати дані, введіть або вставте дані з іншого джерела.

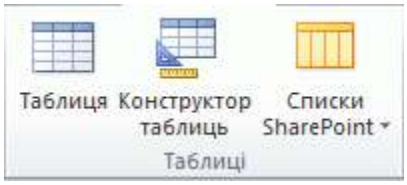
Введення даних у вікні таблиці даних подібне до роботи з аркушем Microsoft Excel. Структура таблиці створюється під час введення даних. Щоразу, коли користувач додає до даних новий стовпець, у таблиці визначається нове поле. Тип даних кожного поля автоматично визначається на основі введених даних.

Якщо наразі не потрібно вводити дані в таблицю «Таблиця1», натисніть кнопку **Закрити** . Якщо до таблиці внесено будь-які зміни, буде запропоновано зберегти їх. Щоб зберегти зміни, натисніть кнопку **Так**; щоб скасувати зміни, натисніть кнопку **Ні**; щоб залишити таблицю відкритою, натисніть кнопку **Скасувати**.

УВАГА! Якщо закрити таблицю без збереження, її буде видалено, навіть якщо вона містить дані.

Створення таблиць

За допомогою елементів у групі **Таблиці** на вкладці **Створити** можна додати нові таблиці до наявної бази даних.



Створення таблиці у режимі Таблиця.

У цьому режимі можна відразу вводити дані й автоматично створювати структуру таблиці. Імена полів позначаються цифрами («Поле1», «Поле2»

тощо) і програма Microsoft Access автоматично встановлює кожний тип даних поля на основі введених даних.

1. На вкладці **Створити** у групі **Таблиці** натисніть елемент **Таблиця**  .

У програмі Microsoft Access створюється таблиця з вибраною першою пустою клітинкою у стовпці **Клацніть, щоб додати**.

2. На вкладці **Поля** у групі **Додавання й видалення** виберіть потрібний тип поля. Якщо потрібний тип поля не відображається, натисніть кнопку **Інші поля**  .

Відобразиться список найуживаніших типів полів. Виберіть потрібний тип поля і програма Microsoft Access додасть нове поле до даних у місці вставлення. Ви можете перемістити поле, перетягнувши його. Під час перетягування поля в табличному вікні відображається вертикальна смуга вставлення, яка вказує, куди буде вставлено поле.

3. Щоб додати дані введіть дані в першій пустій клітинці або вставте дані з іншого джерела.

Якщо дані наразі збережено в іншій програмі, наприклад Microsoft Excel, їх можна скопіювати та вставити в таблицю Microsoft Access. Загалом цей метод найкраще використовувати в тому разі, якщо дані вже поділено на стовпці, як в аркуші Microsoft Excel. Якщо дані містяться в текстовому редакторі, перед копіюванням їх краще розділити на стовпці символами табуляції або перетворити їх у цьому редакторі на таблицю. Якщо дані потрібно редагувати або виконати з ними певні дії (наприклад, розділити повні імена на імена та прізвища), то це можна зробити перед копіюванням, особливо за відсутності досвіду роботи із програмою Microsoft Access.

Під час вставлення даних у пусту таблицю Microsoft Access установлює для кожного поля тип даних, який відповідає характеру розташованих у ньому відомостей. Наприклад, якщо вставлені поля містять виключно дати, програма Microsoft Access застосує до таких полів тип даних «Дата й час». Якщо вставлені дані містять лише слова «так» і «ні», Microsoft Access застосує до поля тип даних «Так/Ні».

У програмі Microsoft Access поля іменуються залежно від вмісту першого рядка вставлених даних. Якщо перший рядок вставлених даних містить дані того самого типу, що й наступні рядки, програма Microsoft Access вважає, що перший рядок – це частина даних, і призначає полям загальні імена (F1, F2 тощо). Якщо перший рядок вставлених даних не схожий на інші рядки, програма Microsoft Access вважає, що перший рядок містить імена полів. Тоді програма відповідним чином іменує поля й не включає перший рядок до даних.

Якщо Microsoft Access призначає полям загальні імена, то для уникнення плутанини поля слід якомога швидше перейменувати. Дотримуйтеся такої послідовності дій:

– Натисніть клавіші Ctrl+S, щоб зберегти таблицю.

– У вікні таблиці даних двічі клацніть кожен заголовок стовпця та введіть для нього описове ім’я поля.

– Збережіть таблицю знову.

ПРИМІТКА. Поля можна також перейменувати, перейшовши до подання конструктора й відредагувавши в ньому імена полів. Щоб перейти до режиму конструктора, помітьте правою кнопкою миші таблицю в області переходів і виберіть пункт **Конструктор**. Щоб повернутися до режиму таблиці, двічі клацніть таблицю в області переходів.

4. Щоб перейменувати стовпець (поле), двічі клацніть заголовок стовпця та введіть нове ім’я.

Слід надавати кожному полю зрозуміле ім’я, щоб під час відображення поля в області **Список полів** можна було визначити його вміст.

5. Для переміщення стовпця помітьте його заголовок, щоб вибрати стовпець, і перетягніть стовпець до потрібного розташування.

Можна також вибрати кілька пов’язаних стовпців і перетягнути їх усіх до нового розташування. Щоб вибрати кілька пов’язаних стовпців, помітьте заголовок першого стовпця, й утримуючи клавішу SHIFT, помітьте заголовок останнього стовпця.

Створення таблиці у режимі конструктора.

У режимі конструктора спочатку слід створити структуру таблиці. Потім слід перейти до вікна таблиці даних для введення даних або використати інші способи введення даних, наприклад, вставлення або імпортування.

1. На вкладці **Створити** у групі **Таблиці** натисніть елемент **Конструктор таблиць**  .

Для кожного поля таблиці введіть ім’я у стовпці **Ім’я поля** та виберіть тип даних зі списку **Тип даних**.

2. За потреби можна ввести опис кожного поля у стовпці **Опис**. Опис відображається в рядку стану, якщо курсор розташовано в цьому полі в вікні таблиці. Опис також використовується як текст рядка стану для всіх елементів керування форми або звіту, створюваних за допомогою перетягування поля з області **Список полів**, а також для всіх елементів керування, створюваних для поля під час використання майстра форм або майстра звітів.

3. Після додавання всіх полів збережіть таблицю:

На вкладці **Файл** виберіть команду **Зберегти**.

4. Ви можете почати вводити дані в таблицю в будь-який час, перейшовши до вікна таблиці даних у першу пусту клітинку. Можна також вставити дані з іншого джерела.

Налаштування властивостей поля в режимі конструктора.

Незалежно від способу створення таблиці рекомендовано перевіряти й налаштовувати властивості полів. Хоча деякі властивості доступні у вікні таблиці даних, інші властивості можна налаштувати лише в режимі конструктора. Щоб перейти в режим конструктора, помітьте таблицю правою кнопкою миші в області переходів і виберіть пункт **Конструктор**. Щоб переглянути властивості поля, виберіть поле у бланку. Властивості відображаються під бланком, у розділі **Властивості поля**.

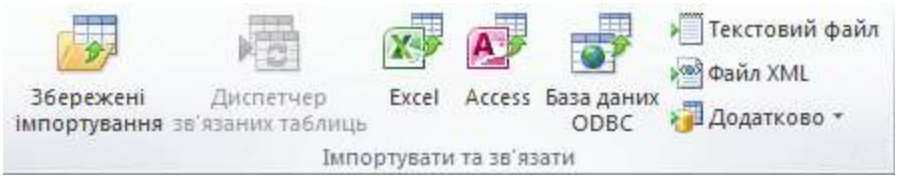
Щоб переглянути опис властивості кожного поля, виберіть властивість і прочитайте опис у полі поруч зі списком властивостей у розділі **Властивості поля**. Щоб отримати додаткові відомості, натисніть кнопку «Довідка».

Імпортування, додавання та зв'язування з даними з іншого джерела.

Вам може знадобитись імпортувати до нової таблиці дані, які зберігаються в іншій програмі, або додати їх до наявної таблиці Microsoft Access.

Можливо Вам потрібно встановити зв'язок і працювати в програмі Microsoft Access із даними Ваших партнерів, які зберігають свої дані в інших програмах. В обох випадках програма Microsoft Access полегшує роботу з даними з інших джерел. Дані можна імпортувати з аркуша Microsoft Excel, з таблиці в іншій базі даних Microsoft Access, зі списку SharePoint Foundation і з багатьох інших джерел. Залежно від джерела процеси дещо різняться, але подана нижче процедура достатня, щоб розпочати роботу.

1. У програмі Microsoft Access на вкладці **Зовнішні дані** у групі **Імпорт і зв'язування** виберіть команду для типу файлу, який імпортується.



Наприклад, в разі імпортування даних з аркуша Microsoft Excel виберіть елемент **Excel**. Якщо тип потрібної програми не відображається, виберіть елемент **Додатково**.

ПРИМІТКА. Якщо у групі **Імпорт** не відображається правильний тип формату, для імпортування даних у програмі Microsoft Access може бути потрібно запустити програму, у якій створено ці дані, і зберегти їх у стандартному форматі файлу (наприклад, у форматі текстовий файл із роздільниками).

2. У діалоговому вікні **Отримати зовнішні дані** натисніть кнопку **Огляд**, щоб знайти джерело даних, або в полі **Ім'я файлу** введіть шлях до нього.

3. Виберіть потрібний параметр (усі програми дають змогу імпортувати, а деякі – додавати та зв'язувати) у розділі **Укажіть спосіб і розташування для збереження даних у поточній базі даних**. Ви можете створити нову таблицю, яка використовує імпортовані дані, або (для деяких програм) додати дані до наявної таблиці чи створити зв'язану таблицю, яка підтримує зв'язок із даними у вихідній програмі.

4. Якщо запущено майстер, дотримуйтесь інструкцій на кількох наступних сторінках майстра. На останній сторінці майстра натисніть кнопку **Готово**.

У разі імпортування об'єктів або зв'язування таблиць із бази даних Microsoft Access відображається діалогове вікно **Імпортувати об'єкти** або **Зв'язок із таблицями**. Виберіть потрібні елементи та натисніть кнопку **ОК**.

Процес залежить від виконуваної дії – імпортування, додавання або зв’язування з даними.

5. Програма Microsoft Access пропонує зберегти відомості про виконану операцію імпортування. Якщо Ви плануєте виконати таку саму операцію імпортування в майбутньому, установіть прапорець **Зберегти етапи імпортування** та введіть відомості.

Згодом можна буде легко повторити операцію, натиснувши на вкладці **Зовнішні дані** у групі **Імпорт і зв’язування** кнопку **Збережені імпортовані елементи**. Якщо відомості про операцію зберігати не потрібно, натисніть кнопку **Закрити**.

У разі імпортування таблиці у програмі Microsoft Access дані імпортуються до нової таблиці, яка потім відображається в області переходів у розділі **Таблиці**. У разі додавання даних до наявної таблиці дані додаються до цієї таблиці. У разі зв’язування з даними, у програмі Microsoft Access в області переходів у групі **Таблиці** створюється зв’язана таблиця.

Додавання частини додатку.

Частину додатку можна використовувати для додавання функцій до наявної бази даних. Частина додатку може бути проста, як окрема таблиця, або може містити кілька зв’язаних об’єктів, наприклад, таблицю та зв’язану форму.

Наприклад, частина додатку «Нотатки» – це таблиця з полем ідентифікатора «Лічильник», полем дати та полем «Memo». Ви можете додавати її до будь-якої бази даних і використовувати без змін або з мінімальними налаштуваннями.

1. Відкрийте базу даних, до якої потрібно додати частину додатку.
2. Відкрийте вкладку **Створити**.
3. У групі **Шаблони** натисніть кнопку **Частини додатку**. Відкриється список доступних частин.
4. Виберіть частину додатку, яку потрібно додати.

Відкриття наявної бази даних Microsoft Access:

1. На вкладці **Файл** виберіть команду **Відкрити**.
2. У діалоговому вікні **Відкрити** перейдіть до БД, яку потрібно відкрити.
3. Виконайте одну з таких дій:

– Двічі натисніть на ярлик бази даних, щоб відкрити її в режимі за замовчанням, указаному в діалоговому вікні **Параметри Access**, або в режимі, призначеному адміністративною політикою.

– Натисніть кнопку **Відкрити** для відкриття бази даних для спільного доступу в багатокористувацькому середовищі, щоб користувачі мали змогу читати базу даних і вносити до неї дані.

– Щоб відкрити базу даних лише для читання, натисніть на стрілку поруч із кнопкою **Відкрити** та виберіть команду **Відкрити для читання**. Ви зможете переглядати її, але внесення змін буде заборонено. Інші користувачі зможуть читати базу даних і вносити до неї дані.

– Щоб відкрити БД для монопольного доступу, натисніть на стрілку поруч із кнопкою **Відкрити** та виберіть пункт **Монопольний доступ**. Якщо БД

відкрито для монопольного доступу, інші користувачі, які здійснять спробу відкрити БД, отримають повідомлення «Файл уже використовується».

– Щоб відкрити базу даних лише для читання, натисніть на стрілку поруч із кнопкою **Відкрити** та натисніть кнопку **Монопольно для читання**. Інші користувачі зможуть відкрити базу даних, але матимуть доступ лише для читання.

ПРИМІТКА. Файл даних можна відкрити безпосередньо в зовнішньому форматі, наприклад, dBASE, Microsoft Exchange або Microsoft Excel. Безпосередньо можна також відкривати будь-яке Джерело даних ODBC, наприклад, Microsoft SQL Server. Програма Microsoft Access автоматично створить нову базу даних у тій самій папці, де міститься файл даних, і додасть посилання на кожну таблицю в зовнішній базі даних.

Щоб відкрити базу даних, у якій Ви нещодавно працювали, на вкладці **Файл** виберіть пункт **Останні** та вкажіть ім'я файлу бази даних. Базу даних буде відкрито з тими самими налаштуваннями параметрів, що й останнього разу. Якщо список нещодавно використаних файлів не відображається, виберіть на вкладці **Файл** пункт **Параметри**. У діалоговому вікні **Параметри Access** виберіть категорію **Параметри клієнта**. У розділі **Відображення** вкажіть, скільки документів слід відображати у списку останніх документів (щонайбільше – 50).

Ви також можете відобразити бази даних, з якими Ви нещодавно працювали, на панелі переходів вікна Backstage: вкладка **Файл**, потрібна недавня база даних. У нижній частині вкладки **Останні** встановіть прапорець **Швидкий доступ до такої кількості останніх баз даних**, а потім укажіть кількість баз даних для відображення.

Якщо відкрити БД за допомогою команди **Відкрити** на вкладці **Файл**, можна переглянути список ярликів БД, які Ви відкривали раніше. Для цього виберіть у діалоговому вікні **Відкрити** елемент **Мої останні документи**.

Питання для самоконтролю

1. Поняття електронного документу та електронного документообігу.
2. Основні принципи електронного документообігу.
3. Найбільш поширені в Україні автоматизовані системи документообігу.
4. Можливості системи електронного документообігу FossDoc.
5. Поняття бази та банку даних, системи управління базами даних.
6. Основні властивості баз даних та вимоги до них.
7. Поняття інформаційної системи та їх класифікація.
8. Характеристика користувачів інформаційної системи (бази даних).
9. Загальна характеристика СУБД Microsoft Access.
10. Поняття таблиці та форми СУБД Microsoft Access.
11. Поняття звіту та запиту СУБД Microsoft Access.
12. Поняття макросів та модулів СУБД Microsoft Access.
13. Типи даних СУБД Microsoft Access.
14. Властивості полів СУБД Microsoft Access.
15. Етапи проектування баз даних в СУБД Microsoft Access.

16. Способи створення нової бази даних в СУБД Microsoft Access.
17. Особливості роботи з базами даних в СУБД Microsoft Access.

Практичні завдання до розділу IV

Практичне заняття № 4.1

Мета заняття: отримання здобувачами магістратури знань, умінь і навичок комплексного використання можливостей основних інформаційно-пошукових систем і баз даних державних органів України.

Завдання:

– Створити за допомогою програми Word файл з назвою **Ваше прізвище_П.з. 4.1**.

– Встановити **пароль** на файл.

– *Використовуючи інформацію з відкритих реєстрів та баз даних державних органів України знайти за допомогою мережі Інтернет наступну інформацію (зробити скріншоти відповідей):*

1. Знайти: ЄДРПОУ, адресу електронної пошти, номер факсу (телефаксу), поштову адресу, юридичну адресу ГУ Національної поліції в місті Києві.
2. Використавши базу даних поштових індексів та відділень поштового зв'язку України знайти поштові індекси всіх навчально-наукових інститутів, що входять до складу НАВС (допомога: адреси інститутів на сайті НАВС в розділі структурні підрозділи академії).
3. Використавши Єдиний державний реєстр судових рішень, знайти номери та форми судових рішень, що стосуються судової справи за номером 357/4959/21. В чому полягає сутність даної справи ?
4. Використавши інформацію щодо структур власності банків України, розміщену на сайті Національного банку, знайти перелік фізичних осіб, які станом на початок поточного року є акціонерами Укргазбанку.
5. Використавши інформацію з єдиного реєстру адвокатів України, знайти перелік адвокатів міста Київ, що мають прізвище «Коваленко» та отримали Свідоцтво на право займатись адвокатською діяльністю до 01.01.2008.
6. Використавши публічну кадастрову карту України, знайти місцерозташування ділянки з кадастровим № 3221282800:06:015:0046 та визначити тип грунтів на ній.
7. Набравши на телефоні комбінацію *#06#, визначте IMEI свого мобільного телефону та перевірте його в базі даних «Розшук» МВС України (Діяльність → Розшук → Мобільні телефони – Номер (IMEI)).
8. У розшукових обліках на сайті МВС (Діяльність → Розшук) знайти відомості про зниклих громадян: Гаврилюк Родіон, Оксамитна Оксана, Бородіна Наталія.
9. У розшукових обліках на сайті МВС України (Діяльність → Розшук) знайти відомості про осіб, які переховуються від органів влади, на прізвища: Ганжа Георгій, Данілова Олена, Албовк Жігмонд.
10. Під час бойових дій був знайдений труп вбитого російського військовослужбовця, за національністю можливо кримського чи російського

(казанського) татарина. При ньому був знайдений пошкоджений військовий білет, виданий (російською) на прізвище «мамедов», ім'я «самир», по-батькові – пошкоджено. Перевірити по сервісах МВС України (https://poternet.site/) наявність даних на зазначену особу.

За результатами пошуку підготуйте доповідну записку на ім'я викладача. Результати пошуку оформлюєте у вигляді таблиці у додатку до доповідної.

У якості власного підпису під доповідною використовуєте QR код, що містить Ваше ім'я та прізвище в англійській транслітерації.

Практичне заняття № 4.2

Мета заняття: отримання здобувачами магістратури знань, умінь і навичок щодо творчого проектування баз даних на запропоновану викладачем тему.

Завдання:

– Створити в папці за допомогою програми Word файл з назвою **Ваше прізвище_П.з. 4.2**.

– Встановити **пароль** на файл.

– Створити проект структури бази даних за наведеною нижче формою на тему, номер якої співпадає з Вашим порядковим номером у журналі.

№ з/п	*Назва інформаційного реквізиту*	*Тип даних*	*Максимальна довжина в символах*	*Ключове поле, словник*
1.				
2.				
3.				
…				
25.				

ТЕМИ БАЗ ДАНИХ:

1. «Облік осіб, що вживають наркотики»
2. «Облік слухачів магістратури ННІ № 1 НАВС»
3. «Облік дорожньо-транспортних пригод»
4. «Облік зареєстрованого автомототранспорту»
5. «Облік осіб, що мають судимість»
6. «Облік осіб, що переховуються від органів влади»
7. «Облік невідомих психічно-хворих осіб»
8. «Облік транспортних засобів, що розшукуються»
9. «Облік зареєстрованої зброї»
10. «Облік персоналу НАВС»
11. «Облік осіб, що зловживають алкоголем»
12. «Облік неопізнаних трупів»
13. «Облік зниклих громадян»
14. « Облік корупціонерів»
15. «Облік кримінальної зброї»
16. «Облік викрадених чи втрачених документів»
17. «Облік зброї, що розшукується»

18. «Облік сімейних бешкетників»
19. «Облік викрадених мобільних телефонів»
20. «Облік вбивць»
21. «Облік кишенькових злодіїв»
22. «Облік курсантів ННІ № 1 НАВС»
23. «Облік викрадених культурних цінностей»
24. «Облік власників мобільних телефонів»
25. «Облік викрадених чи втрачених речей»
26. «Облік власників автомототранспорту»
27. «Облік злочинів»
28. «Облік адміністративних правопорушень»
29. «Облік слідів рук, виявлених з місць вчинення злочину»
30. «Облік наказів в бібліотеці»

Практичне заняття № 4.3

Мета заняття: отримання здобувачами магістратури знань, умінь і навичок щодо створення та використання баз даних (таблиць) на прикладі MS Access.

Завдання:

1. Відкрити програму MS Access. Натиснути кнопку «Порожня база даних». Задати ім'я файлу **Ваше прізвище_Реєстр АМТ**. Вибрати папку d:\Тема 4. Натиснути кнопку «Створити».

2. Встановити **пароль** на файл.

3. Ваша база даних «Реєстр АМТ» буде містити 3 таблиці:

«Список власників АМТ»; «Моделі АМТ»; «Реєстрація власності на АМТ».

У режимі «Конструктор» створити таблицю ***«Список власників АМТ»***, яка має наступні поля:

Ім'я поля	Тип даних	Примітка
Номер власника з/п	Автонумерація	
Номер паспорта	Число	Ключове поле. 9 цифр
Прізвище	Короткий текст	
Ім'я	Короткий текст	
По батькові	Короткий текст	
Стать	Короткий текст	Словник (див. *)
Дата народження	Дата й час	
Тимчасові права	Так/ні	Словник (див. **)
Посада	Короткий текст	
Адреса	Короткий текст	
Телефон	Короткий текст	
Дата постановки на облік	Дата й час	
Фото	Об'єкт OLE	
Примітки	Довгий текст	Кількість порушень ПДД тощо

* Під час введення типу поля *Стать* треба у частині вікна «Властивості поля» у вкладці «Підстановка» вибрати «Тип елемента управління – Поле зі списком», «Тип джерела рядків – Список значень», «Джерело рядків» – набрати чол; жін.

** Під час введення типу поля *Тимчасові права* треба у частині вікна «Властивості поля» у вкладці «Підстановка» вибрати «Тип елемента управління – Поле зі списком», «Тип джерела рядків – Список значень», «Джерело рядків» – набрати так;ні.

4. Ввести дані 5 власників АМТ.

5. В режимі «Конструктор» створити таблицю ***«Моделі АМТ»***, яка має наступні поля та зміст (врахувати, що поле «Назва автомобіля» – це ключове поле):

Номер АМТ з/п	**Назва автомобіля**	**Маса (кг)**	**Кількість місць**	**Розгон до 100 км/год (сек)**	**Макс швидкість (км/год)**	**Обсяг двигуна ($см^3$)**	**Вартість (грн)**	**Фото АМТ**
1	ЗАЗ-1102	710	5	17	145	1091	24 000	
2	Maserati Coupe GT	1670	4	4,9	285	4244	84 0000	
3	Mazda 3 Sport	1290	5	9	208	1999	141 000	
4	Mazda RX-8	1380	4	6,4	235	2654	222 000	
5	Ssang Yong Actyon	1903	5	14,2	160	2000	172 000	
6	Land Rover Defender110	2055	9	16,8	130	2495	315 000	
7	Lexus LX500D	2575	5	7	210	3346	4670000	

6. Ввести дані цих 7 автомобілів до таблиці «Моделі АМТ».

7. В режимі «Конструктор» створити таблицю ***«Реєстрація власності на АМТ»***, яка має наступні поля:

Ім'я поля	**Тип даних**	**Примітка**
Номер реєстрації з/п	Автонумерація	
Назва автомобіля	Короткий текст	Ключове поле
Номер паспорта	Число	

8. Ввести назви 7 автомобілів з таблиці «Моделі АМТ» та розподілити їх між 5 власниками з таблиці «Список власників АМТ».

Практичне заняття № 4.4 (продовження № 4.3)

Мета заняття: отримання здобувачами магістратури знань, умінь і навичок щодо створення та використання баз даних (зв'язків між таблицями, форм та запитів) на прикладі MS Access.

Завдання:

1. За допомогою команди «Схема даних» вкладки «Робота з базами даних» встановити такі ***зв'язки між таблицями***:

1.1) поля «Номер паспорта» із таблиці «Список власників АМТ» з полем «Номер паспорта» із таблиці «Реєстрація власності на АМТ»;

1.2) поля «Назва автомобіля» із таблиці «Моделі АМТ» з полем «Назва автомобіля» із таблиці «Реєстрація власності на АМТ».

2. Створити ***форми для перегляду таблиць***: «Список власників АМТ», «Моделі АМТ», «Реєстрація власності на АМТ» та відповідно їх назвати.

3. Створити ***запит по власникам АМТ*** з такими полями: «Номер власника з/п», «Прізвище», «Ім'я», «По-батькові», «Фото», «Назва автомобіля», «Фото АМТ». Назвати цей запит **«Запит 1** – Всі власники АМТ».

4. Створити форму для перегляду цього запиту і відповідно її назвати.

5. Створити ***запит для однієї конкретної особи*** з такими полями: «Прізвище», «Ім'я», «По-батькові», «Фото», «Назва автомобіля», «Фото АМТ». Назвати цей запит **«Запит 2** – Власник АМТ Прізвище».

6. Створити форму для перегляду цього запиту і відповідно її назвати.

7. Створити ***запит з параметром по прізвищу*** (прізвище власника АМТ кожен раз потрібно вводити у діалогове вікно) з такими полями: «Прізвище», «Ім'я», «По-батькові», «Фото», «Назва автомобіля», «Фото АМТ».

Задайте умови селекції для поля «Прізвище»: в рядку «Умова відбору» введіть наступний текст, взятий в квадратні дужки: [введіть Прізвище].

Назвати цей запит **«Запит 3** – Власник АМТ з параметром».

8. Створити форму для перегляду цього запиту і відповідно її назвати.

9. Створити ***запит по АМТ*** з такими полями: «Номер АМТ з/п», «Назва автомобіля», «Вартість (грн)», «Фото АМТ», «Прізвище», «Ім'я», «По-батькові», «Фото». Назвати цей запит **«Запит 4** – Всі АМТ».

10. Створити форму для перегляду цього запиту і відповідно її назвати.

11. Створити ***запит для конкретного АМТ*** з такими полями: «Назва автомобіля», «Вартість (грн)», «Фото АМТ», «Прізвище», «Ім'я», «По-батькові», «Фото». Назвати цей запит **«Запит 5** – Назва конкретного АМТ».

12. Створити форму для перегляду цього запиту і відповідно її назвати.

13. Створити ***запит з параметром по назві АМТ*** (назву АМТ кожен раз потрібно вводити у діалогове вікно) з такими полями: «Назва автомобіля», «Вартість (грн)», «Фото АМТ», «Прізвище», «Ім'я», «По-батькові», «Фото». Назвати цей запит **«Запит 6** – АМТ з параметром».

14. Створити форму для перегляду цього запиту і відповідно її назвати.

15. Створити запит для пошуку всіх жінок – власників АМТ. Назвати цей запит **«Запит 7** – Всі жінки – власники АМТ».

16. Створити форму для перегляду цього запиту і відповідно її назвати.

17. Створити запит для пошуку всіх водіїв з тимчасовими правами. Назвати цей запит **«Запит 8** – Власники АМТ з тимчасовими правами».

18. Створити форму для перегляду цього запиту і відповідно її назвати.

19. Створити запит для пошуку водіїв, які народились після 01.01.2000 року. Назвати цей запит **«Запит 9** – Власники АМТ народились після 2000 року».

20. Створити форму для перегляду цього запиту і відповідно її назвати.

21. Створити запит для пошуку АМТ, розгон яких до 100 км/год не перевищує 10 сек. Назвати цей запит **«Запит 10** – АМТ з розгоном до 10 сек».

22. Створити форму для перегляду цього запиту і відповідно її назвати.

23. Створити запит для пошуку АМТ, максимальна швидкість яких більше 170 км/год. Назвати цей запит **«Запит 11** – АМТ з макс. швидкістю більше 170 км/год».

24. Створити форму для перегляду цього запиту і відповідно її назвати.

25. Створити запит для пошуку АМТ вартістю від 100 000 до 300 000 грн. Назвати цей запит **«Запит 12** – АМТ вартістю від 100 000 до 300 000 грн».

26. Створити форму для перегляду цього запиту і відповідно її назвати.

27. Створити запит для пошуку АМТ з кількістю місць 4 або 5. Назвати цей запит **«Запит 13** – АМТ з кількістю місць 4 або 5».

28. Створити форму для перегляду цього запиту і відповідно її назвати.

29. Створити запит для пошуку АМТ, назви яких починаються з літери «L». Назвати цей запит **«Запит 14** – АМТ назва яких з літери L».

30. Створити форму для перегляду цього запиту і відповідно її назвати.

31. Створити комплексний запит для пошуку АМТ: маса більше 1000 кг, кількість місць – 5, розгон до 10 сек, максимальна швидкість більше 200 км/год, обсяг двигуна не перевищує 2000 $см^3$, вартість до 150 000 грн. Назвати цей запит **«Запит 15** – АМТ за комплексом вимог».

32. Створити форму для перегляду цього запиту і відповідно її назвати.

Список використаних і рекомендованих джерел

1. Система електронного документообігу FossDoc. URL: https://fossdoc.com/elektronniy-dokumentooborot.
2. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV.
3. Про Національну програму інформатизації : Закон України від 1 груд. 2022 р. № 2807-IX.
4. Про авторське право і суміжні права : Закон України від 23 груд. 1993 р. № 3792-XII.
5. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 лип. 1994 р. № 80/94-ВР.
6. Кудінов В. А., Смаглюк В. М., Хахановський В. Г. Інформаційне забезпечення ОВС : навч. посіб. Київ, 2015. 108 с.

РОЗДІЛ V
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

5.1. Основні напрями застосування штучного інтелекту в юридичній діяльності

З моменту запуску в листопаді 2022 року ChatGPT – чат-бот, який використовує штучний інтелект (ШІ) для відповідей на запитання або створення тексту чи навіть коду на вимогу користувачів, – став інтернет-додатком із найшвидшими темпами зростання в історії. Лише за два місяці він мав 100 мільйонів активних користувачів. За даними компанії з моніторингу технологій Sensor Town, щоб досягти цієї віхи, Instagram знадобилося два з половиною роки.

Величезна популярність ChatGPT, який розробила компанія OpenAI за фінансової підтримки Microsoft, викликала інтенсивні дебати щодо впливу штучного інтелекту на майбутнє людства.

Тексти (від есе, віршів і жартів до комп'ютерного коду) і зображення (такі як діаграми, фотографії та ілюстрації), створені інструментами ШІ, такими як ChatGPT, DALL-E, Bard і AlphaCode, може бути неможливо відрізнити від роботи людини.

Штучний інтелект – організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [1].

Використання штучного інтелекту (ШІ) в юридичній діяльності відкриває перед юристами нові можливості для покращення ефективності, точності та доступності юридичних послуг. Ось деякі способи, які ШІ може бути використаний у юридичній сфері:

1. Автоматизація рутинних завдань: ШІ може бути використаний для автоматизації рутинних юридичних завдань, таких як перевірка документів на відповідність правовим нормам, підготовка стандартних договорів, заповнення форм та ін.
2. Аналіз доказів: ШІ може допомагати адвокатам аналізувати великі обсяги доказів у судових справах, виявляти закономірності та робити прогнози щодо винесення рішення.
3. Пошук правової інформації: ШІ може допомагати знаходити та аналізувати правову інформацію з різних джерел, включаючи закони, судову практику та наукові статті.
4. Підтримка прийняття рішень: ШІ може надавати аналітичні звіти та рекомендації юристам щодо можливих стратегій та ризиків у справах.

5. Прогнозування рішень суду: З використанням алгоритмів машинного навчання й нейромереж, ШІ може аналізувати судову практику та прогнозувати можливі рішення суду у подібних справах.

6. Взаємодія з клієнтами: ШІ може служити засобом комунікації між адвокатами та клієнтами, відповідаючи на загальні запитання, надаючи інформацію про правові процедури тощо.

7. Попередження ризиків: ШІ може допомагати виявляти потенційні правові ризики для бізнесу та надавати рекомендації щодо їх уникнення.

8. Обробка документів: ШІ може виявляти та виділяти важливі елементи в текстах договорів, угод та інших документів, полегшуючи їх аналіз.

9. Медіація та альтернативні методи вирішення спорів: ШІ може допомагати усунути розбіжності між сторонами та рекомендувати компромісні рішення у справах.

10. Забезпечення конфіденційності даних: При використанні ШІ важливо забезпечувати високий рівень захисту конфіденційної інформації та дотримання норм щодо обробки особистих даних.

Важливо зауважити, що використання штучного інтелекту в юридичній діяльності також ставить перед собою етичні, правові та безпекові виклики, які потребують уважного вирішення.

Зокрема, потенційну загрозу правам громадян і демократії становлять певні програми ШІ:

– системи біометричної категоризації, які використовують чутливі характеристики (наприклад, політичні, релігійні, філософські переконання, сексуальну орієнтацію, расу);

– нецілеспрямоване копіювання зображень обличчя з Інтернету або записів камер відеоспостереження для створення баз даних розпізнавання облич;

– розпізнавання емоцій на робочому місці та в навчальних закладах;

– соціальна оцінка на основі соціальної поведінки або особистих характеристик;

– системи ШІ, які маніпулюють поведінкою людей, щоб обійти їх свободу волі;

– системи ШІ, які використовують вразливі місця людей (через їхній вік, інвалідність, соціальне чи економічне становище).

5.2. Класифікація систем штучного інтелекту

Системи штучного інтелекту (ШІ) можна класифікувати за різними критеріями, такими як функціональність, спосіб навчання, архітектура та багато інших. Ось деякі з найбільш поширених способів класифікації ШІ:

1. За функціональністю:

– Слабкий штучний інтелект: системи, що спеціалізуються на вирішенні конкретних завдань і не володіють загальною інтелектуальною здатністю. Це можуть бути системи, які відповідають на питання, розпізнають образи або

керують рухом роботів. Прикладом можуть бути шахові програми, здатні перемогти чемпіона світу, але не здатні виконувати інші завдання.

У смартфонах є безліч додатків, які використовують цю технологію – від GPS-карт до музичних і відеопрограм, які знають ваші смаки та дають рекомендації.

Навіть більш складні системи, такі як безпілотні автомобілі та ChatGPT, є формами вузького штучного інтелекту. Вони не можуть діяти за межами встановленого набору завдань, тому не можуть самостійно ухвалювати рішення.

– Сильний (загальний) штучний інтелект: системи, які володіють загальною інтелектуальною здатністю, аналогічною людському розуму. Прикладом може бути теоретичний розум, який вміє вирішувати різноманітні задачі.

– «Штучний суперінтелект» (ШС). Це станеться, коли штучний інтелект буде вищим за людський.

2. За способом навчання:

– Навчання з вчителем (наглядне навчання): системи навчаються на основі набору прикладів, де кожен приклад має відповідний «правильний» результат. Цей підхід використовується, наприклад, в задачах класифікації та регресії.

– Навчання без вчителя: системи аналізують дані без попереднього навчання на зразках. До цієї категорії належать методи кластеризації, зменшення розмірності тощо.

– Підсилене навчання: системи навчаються через взаємодію з оточенням, отримуючи нагороди або покарання за свої дії. Цей підхід популярний в задачах навчання агентів для гри.

3. За архітектурою:

– Нейронні мережі: системи, що моделюють структуру та функціонування нервової системи, використовуючи штучні нейрони та зв’язки між ними.

– Експертні системи: базуються на правилах, встановлених експертами в певній галузі. Вони використовують правила для вирішення задач, але не володіють «розумінням» у широкому сенсі.

4. За областю застосування:

– Обробка природної мови: системи, що аналізують та генерують людську мову.

– Комп’ютерний зір: системи, що розпізнають та аналізують зображення.

– Автономні системи: роботи та автономні агенти, що взаємодіють з фізичним середовищем.

Вищеозначені класифікації можуть перетинатися, існує багато інших способів розподілу ШІ на категорії в залежності від контексту та точки зору.

5.3. Навчання систем штучного інтелекту

Ключем до всього машинного навчання є процес, який називається тренуванням, під час якого комп'ютерна програма отримує велику кількість даних (іноді з поясненнями, що це за дані), і набір інструкцій.

Інструкція може бути, приміром, такою: «знайти всі зображення, що містять обличчя» або «розподілити ці звуки за категоріями».

Потім програма шукатиме закономірності у наданих їй даних, щоб досягти поставлених цілей.

Щоб зрозуміти, як цей тренувальний процес може створити різні типи ШІ, уявімо різних тварин. Протягом мільйонів років природне середовище існування змусило тварин розвивали певні здібності – так само мільйони разів, які ШІ переглядає наданий йому тренувальний матеріал, формують спосіб його розвитку та створюють спеціалізовані моделі штучного інтелекту.

Зокрема, чатботи є різновидом штучного інтелекту, відомого як великі мовні моделі (ВММ), і тренуються на величезних обсягах тексту. ВММ здатні враховувати не лише окремі слова, а й цілі речення, та порівнювати використання слів і фраз в уривку з іншими прикладами в усьому масиві тренувальних даних.

За допомогою цих мільярдів порівнянь слів та фраз, ВММ може прочитати запитання та згенерувати відповідь – як предиктивне введення тексту у вас на телефоні, але у значно більшому масштабі.

Дивовижна річ великих мовних моделей полягає в тому, що вони можуть вивчати правила граматики та розуміти значення слів самостійно, без допомоги людини.

ШІ записує звуки, коли ви говорите, видаляє фоновий шум, розділяє вашу мову на фонетичні одиниці – окремі звуки, які складають вимовлене слово – і потім зіставляє їх із бібліотекою звуків мови.

Потім ваше мовлення перетворюється на текст, у якому будь-які потенційні помилки сприйняття на слух можна виправити до того, як ШІ дасть відповідь.

Цей тип штучного інтелекту називається обробка природної мови.

Цю технологію використовують у багатьох ситуаціях – від того, як ви говорите «так», щоб підтвердити транзакцію у мобільному банкінгу, до того, як цікавитеся у свого смартфона про погоду на наступні кілька днів у місті, куди зібралися поїхати.

Помічали, як ваш телефон створює альбоми фотографій з назвами на кшталт «На пляжі» або «Вечірки»? Алгоритм ШІ виявив закономірності у ваших фото і згрупував їх для вас.

Такі програми тренували шляхом перегляду купи зображень, які супроводжував простий опис. Якщо ви надасте такому типу ШІ достатньо зображень із позначкою «велосипед», зрештою він почне розпізнавати, як виглядає велосипед і чим він відрізняється від човна чи автомобіля.

Іноді штучний інтелект тренують виявляти крихітні відмінності в подібних зображеннях. Так працює технологія розпізнавання обличчя, яка виявляє

найменші дрібниці рис вашого обличчя, які роблять його унікальним у порівнянні з будь-яким іншим обличчям на планеті.

Такі ж алгоритми навчалися виявляти небезпечні для життя пухлини на рентгенівських знімках чи томографіях - вони можуть опрацювати тисячі знімків за той час, за який людина перегляне лише один.

Генератори зображень на базі ШІ можуть за допомогою складних візуальних шаблонів, які вони збирають із мільйонів фотографій і малюнків, створювати абсолютно нові зображення.

Ви можете попросити штучний інтелект створити фотографічне зображення чогось, чого насправді ніколи не було – наприклад, фотографію людини, яка йде поверхнею Марса.

Або ж ви можете проявити творчість і вказати стиль майбутнього зображення: «Зроби мій портрет, намальований у стилі Пікассо».

Тисячі годин тренування, спрямованого на те, щоб зрозуміти, як виглядає правильне керування автомобілем, дозволили ШІ керувати автомобілем і уникати зіткнень в реальному світі.

Модель штучного інтелекту використовує дані зі своїх датчиків, щоб ідентифікувати об’єкти та з’ясувати, чи рухаються вони, і якщо так, то який це рухомий об’єкт – інша машина, велосипед, пішохід чи щось інше.

Алгоритми прогнозування багато років намагалися упоратися з часто непередбачуваною поведінкою реальних водіїв, однак тепер безпілотні автомобілі вже зібрали мільйони кілометрів даних на реальних дорогах. У Сан-Франциско такі авто вже возять пасажирів за гроші.

Автономне керування також є яскравим прикладом того, як новим технологіям доводиться долати не тільки технічні перешкоди.

Законодавство щодо правил безпеки, а також глибоко вкорінене відчуття тривоги з приводу того, що станеться, коли ми передаємо керування машинам, досі є потенційними перешкодами для повністю автоматизованого майбутнього на наших дорогах.

Ймовірно, у світовому павутинні вже є кілька профілів щодо вашої фінансової та соціальної активності, які можна використовувати для прогнозування вашої поведінки.

Ваша картка лояльності в супермаркеті відстежує ваші звички та смаки через ваші щотижневі закупи. Кредитні агенції відстежують, скільки грошей ви маєте в банку та боргів за кредитними картками.

І йдеться не лише про вас – ці цифри існують щодо всіх, що дозволяє моделям штучного інтелекту працювати з ними, шукаючи соціальні тенденції.

Мультимодальний ШІ дозволяє переглядати різні типи даних, такі як зображення, текст, аудіо чи відео, і виявляти нові зв’язки між ними.

Цей мультимодальний підхід став однією з причин величезного стрибка в можливостях ChatGPT після оновлення з версії ChatGPT3.5, яка тренувалася лише на текстах, до версії ChatGPT4, яка навчалася також і на зображеннях.

Ідея єдиної моделі штучного інтелекту, здатної обробляти будь-які дані і, отже, виконувати будь-які завдання, від перекладу між мовами до розробки

нових ліків, відома як штучний загальний інтелект (ШЗІ) або сильний штучний інтелект (СШІ).

Багато з останніх проривів у ШІ стали можливими завдяки спонтанному навчанню, або навчанню без учителя. Завдяки використанню складних алгоритмів і величезних наборів даних штучний інтелект може навчатися без будь-якої допомоги людини.

Найвідоміший приклад – ChatGPT. Обсяги тексту в інтернеті та оцифрованих книгах настільки величезні, що за багато місяців ChatGPT зміг навчитися самостійно поєднувати слова в осмислений спосіб, а люди потім допомагали точніше налаштувати його відповіді.

Уявіть, що у вас є велика купа книг іноземною мовою, можливо, деякі з них – з ілюстраціями. Зрештою ви побачите, що щоразу, коли ви бачите у книзі зображення дерева, на сторінці поряд із ним з'являється одне й те саме слово, а коли фото будинку – то слово інше.

Поступово ви виявите й інші закономірності. ChatGPT провів такий ретельний аналіз зв'язків між словами, щоб створити величезну статистичну модель, яку потім можна використовувати для прогнозування та створення нових речень.

Вона покладається на величезну обчислювальну потужність, яка дозволяє ШІ запам'ятовувати величезну кількість слів – поодинці, групами, реченнями – а потім читати та порівнювати, як вони вживаються, і робити це знову і знову лише за частку секунди.

Основною задекларованою ціллю є створення безпечного, прозорого, прогнозованого та екологічно чистого штучного інтелекту.

5.4. Експертні системи як особливий вид систем штучного інтелекту

Експертна система (ЕС) – це обчислювальна система, де зібрані знання фахівців про деяку вузькоспеціалізовану предметну область і яка у межах цієї області здатна приймати експертні рішення на рівні експерта-професіонала та на вимогу користувача надавати пояснення ходу своїх міркувань зрозумілим для користувача способом.

Типи завдань, що вирішуються експертними системами:

– *інтерпретація* (аналіз результатів спостереження з метою встановлення властивостей досліджуваної системи об'єктів);

– *прогноз* (на основі моделей минулого і сучасного робиться прогнозування подій майбутнього);

– *діагностика* (встановлення несправностей у технічній системі або виявлення захворювання в живому організмі, що базується на інтерпретації даних);

– *моніторинг (стеження)* (спостереження за параметрами об'єктів і видача повідомлень у випадку виходу параметрів об'єктів стеження за допустимі межі);

– *планування* (формування плану дій, які слід виконати для досягнення поставленої мети);

– *налагодження* (надання рекомендацій для усунення несправностей чи помилок);

– *ремонт* (виправлення виявленого дефекту);

– *керівництво* (управління поведінкою систем об'єктів, наприклад, аеропорт, залізничний транспорт);

– *проектування* (побудова певних конфігурацій об'єктів, які задовольняють заданим вимогам).

Загалом ЕС являє собою програмно-технічний засіб, який дозволяє користувачу в діалоговому режимі отримувати консультаційну допомогу в конкретній предметній галузі, де сконцентровані досвід і знання експертів (фахівців у певній галузі). В основі функціонування ЕС лежить використання знань, а маніпулювання ними здійснюється на базі евристичних правил, сформульованих експертами.

Сьогодні ЕС застосовуються у різноманітних сферах людської діяльності, в тому числі і в правоохоронній. Основним технологічним чинником, який стримує масове виробництво і розповсюдження ЕС, є унікальність розробки кожної окремої прикладної ЕС. У порівнянні з традиційним підходом до створення програмних комплексів, в основі яких лежить алгоритмізація, ЕС мають низку особливостей. Це можливість внесення змін і розширення системи при зміні предметної галузі, розвинуті інтерфейси, орієнтовані на користувачів, які не вміють програмувати, а також здатність до обґрунтування своїх дій (рішень).

Класифікація експертних систем. За метою функціонування ЕС поділяються на: керуючі; консультативні; консультативно-керуючі.

За характером задач, які розв'язуються: аналізуючи; синтезуючи.

За моделями предметної галузі: статичні; динамічні.

За складністю структури: поверхневі; глибинні.

Існує також розподіл ЕС на традиційні та інтегральні.

Особливості експертних систем. На відміну від традиційних програм, які орієнтовані на розв'язання формальних завдань, характеризуються такими особливостями:

1) алгоритм одержання розв'язку невідомий наперед, але будується самими експертними системами за допомогою суджень у символьному вигляді на основі знань експерта;

2) отримані розв'язки обґрунтовуються експертною системою, тобто вона «усвідомлює» в термінах користувача, як було отримано розв'язання задачі;

3) експертні системи спроможні аналізувати і пояснювати свої дії і знання;

4) експертні системи можуть накопичувати нові знання і міняти у відповідності з ними свою поведінку;

5) експерти, які вводять знання в експертні системи, можуть і не мати знань з програмування.

Можливості використання баз знань та експертних систем у галузі права досить широкі. Перспективними напрямами використання таких систем є:

– пошук нормативних актів та судових рішень, які мають відношення до визначеного набору фактів, що описують правову ситуацію;

– розробка, пояснення або розпізнання ходу міркувань, які складають обґрунтування судового рішення або висновку, які містяться у тому чи іншому процесуальному документі;

– складання нормативних актів з дотриманням правил законодавчої техніки;

– підготовка оперативно-розшукових, тактичних, кримінально-процесуальних рішень при розкритті та розслідуванні злочинів.

У процесі розробки ЕС, заснованих на використанні знань в галузі права, найчастіше використовують два підходи до моделювання міркувань. Перший використовує «ієрархічні міркування», що відштовхуються від правової норми (міркування від загального до часткового), другий використовує «міркування за зразком», коли ситуація аналізується на основі пошуку прецеденту.

Нині гостро відчувається необхідність в ЕС, яка змогла б вже на ранній стадії розробки певного нормативного документа виявити, чи відповідає він чинному законодавству, а також розкрити внутрішні суперечності і прогалини в самому документі.

Питання для самоконтролю

1. Що таке штучний інтелект ?
2. Основні напрямки використання штучного інтелекту в юридичній діяльності
3. Класифікація систем штучного інтелекту за функціональністю
4. Класифікація систем штучного інтелекту за способом навчання
5. Класифікація систем штучного інтелекту за архітектурою
6. Що таке експертна система ?
7. Дайте визначення поняттям: «База знань» та «Система управління базами знань».
8. Назвіть головні компоненти ідеальної експертної системи.
9. Поясніть призначення та функції головних компонентів експертної системи.
10. Поясніть призначення системи підтримки прийняття рішень.

Практичні завдання до розділу V

Практичне заняття № 5.1

Мета: Ознайомитись з роботою деяких Вебсервісів, що надають послуги з використанням систем штучного інтелекту (ШІ) і можуть бути використані в професійній діяльності спеціалістів в галузі права та правоохоронної діяльності.

Для виконання даної роботи потрібно мати поштову адресу на вебресурсі gmail.com. Використання деяких ресурсів потребує проходження попередньої безкоштовної реєстрації.

Завдання 1. За допомогою штучного інтелекту ChatGPT (https://chat.openai.com/) виконайте наступні завдання:

А) Напишіть про себе коротку інформацію, а саме: ПІБ, де народилися, де навчалися, в якій галузі хочете працювати, які Ваші захоплення. Перекладіть цей текст за допомогою ChatGPT на англійську та японську мови. Вставте нижче скріншоти з перекладами

Місце для скріншотів [💻]

Б) За допомогою відповідних інтернет-ресурсів створіть QR код свого резюме на англійській мові

Місце для QR-коду [💻]

В) Визначте за допомогою ChatGPT «Як найшвидше доїхати з Києва до європейського міста N залізничним транспортом» та вставте скріншот відповіді нижче (місто N повинно знаходитись на території однієї з країн Євросоюзу, а його назва починатися з тієї ж букви, що і Ваше прізвище)(Київ можете замінити місцем свого проживання)

Місце для скріншоту [💻]

Г) Задайте штучному інтелекту ChatGPT питання з юридичної тематики, що Вас цікавить та вставте скріншот відповіді нижче

Місце для скріншоту [💻]

Завдання 2. Перейдіть за посиланням www.myheritage.com.ua/deep-nostalgia і заванажте фотографію людини (потрібно пройти безкоштовну реєстрацію на сайті). Створіть анімацію і вставте нижче посилання на цю анімацію

Місце для посилання на анімацію➲

Завдання 3. Опишіть свій зовнішній вигляд англійською мовою (особливо зверніть увагу на характерні риси обличчя). Згенеруйте за описом 3 власні зображення, використовуючи сервіси

www.artbreeder.com

www.deepdreamgenerator.com

www.getimg.ai

Скріншоти зображень разом з описом додайте нижче

Місце для скріншотів [💻]

Завдання 4. Використавши одну з програм штучного інтелекту (посилання – Nightcafe, OpenArt, Dream, https://labs.openai.com/) намалюйте картину з професійної тематики для обкладинки підручника «Сучасні інформаційні технології в юридичній діяльності».

(Більшість програм зі штучним інтелектом, які перетворюють текст на зображення, працюють практично однаково. Все, що вам потрібно зробити – це ввести текст з описом змісту картини і чекати, доки програма видасть результат. Допомогти зробити ШІ свою картину краще, можна максимально

чітко написавши текстове повідомлення. Потрібно вказати, що саме ви хочете бачити на зображенні, аж до художнього стилю, кольору і навіть матеріалу, з якого буде створена картина. Оскільки багато генераторів зображень із штучним інтелектом навчаються з використанням відомих художніх стилів, вони можуть розуміти такі терміни, як «імпресіонізм», «цифрове мистецтво» чи «акварельний малюнок». Ви навіть можете попросити програму створити картину в стилі робіт відомого художника, наприклад Ван Гога або Пікассо. Генерація картини після запиту користувача з'являється досить швидко, іноді менш ніж за хвилину.)

Завдання 5. За допомогою сервісу Gamma (www.gamma.app) створіть презентацію щодо застосування Smart технологій в галузі професійної діяльності з Вашої майбутньої спеціальності. Оберіть оформлення, узгодьте план презентації. На першому слайді додайте своє прізвище, при необхідності, виконайте редагування. Скопіюйте посилання на презентацію та вставте його нижче

Місце для посилання на презентацію➲

Завдання 6. За допомогою сервісу www.steve.ai створіть сторітелінг (storytelling) на 5-6 сцен, а саме: опишіть на англійській мові 5-6 сцен (які стосуються Вашої теперішньої роботи або навчання або відпочинку). Обов'язково в розділі тип анімації оберіть Animation Video. Зробіть скріншот екрану, щоб було видно і сцени, і превью.

Місце для скріншотів [💻]

Практичне заняття № 5.2

Мета заняття: Отримати практичні навички щодо створення баз знань з професійної тематики для малої експертної системи

Завдання: Ознайомитись зі теоретичними відомостями щодо структури бази знань та створити базу знань з визначеної тематики.

Порядок виконання:

Теоретичні відомості. База знань для Малої експертної системи являє собою текстовий файл, що складається з трьох секцій. **Секції одна від одної відділяються пустим рядком.**

Перша секція містить назву бази, прізвище автора, коментарі та іншу будь-яку інформацію до 10000 символів. Секція може займати кілька рядків і закінчується пустим рядком.

Друга секція має наступний вигляд:

Питання № 0 (будь який текст до 1000 символів, закінчується символом перенесення строки)

Питання № 1

Питання № 2

…….

Питання № N (після останнього питання йде пустий рядок, що завершує другу секцію).

Третя секція має такий вигляд:

Подія № 0, P [, i, P_{yes}, P_{no}]

Подія № 1, P [, i, P_{yes}, P_{no}]

Подія № 2, P [, i, P_{yes}, P_{no}]

……

Подія № M, P [, i, P_{yes}, P_{no}]

Ця секція містить правила виведення, кожне з яких розміщується в окремому рядку. Секція завершується кінцем файлу.

На початку опису правила виведення задається конкретна подія, ймовірність якої змінюється з даним правилом (Ймовірність – це чисельний показник, що може лежати в межах від 0 до 1 і показує ступінь очікування, що певна подія відбудеться. Значення ймовірності 0 відповідає неможливій події, значення 1 відповідає достовірній події – яка обов'язково відбудеться). Опис події може містити будь-які символи, крім коми.

Після коми вказується ймовірність даної події у випадку відсутності будь-якої додаткової інформації (*P*). Далі, після коми, йде сукупність з трьох чисел, яка може повторюватись кілька разів (в залежності від кількості питань, відповіді на які впливають на міру невизначенності щодо завершення даної події). Перше число (i) – це номер відповідного питання; друге число (P_{yes}) – ймовірність отримати відповідь «Да» на питання з номером i, якщо відповідна подія має місце; третє число (P_{no}) – ймовірність отримати відповідь «Да» на питання з номером i, якщо відповідна подія не має місця.

Приклад:

Нехай секція 2 містить 3 питання:

1. У Вас висока температура?

2. У Вас ломота у м'язах?

3.Хворобливий стан спостерігається у Вас на протязі місяця?

Третя секція містить одну подію (діагноз):

Ви хворі на грип, 0.01, 1,0.9,0.02, 2,1,0.03, 3,0,0.01

Число 0.01 після тексту події «Ви хворі на грип» означає ймовірність того, що навмання узята людина виявиться хворою на грип. Далі йде номер питання 1. Числа 0.9 та 0.01 означають, що якщо у пацієнта грип, то він в 9 випадках з 10 відповість «Да» на перше питання і тільки в двох випадках зі ста відповість «Да», якщо він не хворіє грипом.

Число 1 після номера 2 (друге питання) означає, що даний симптом обов'язково спостерігається при захворюванні на грип. Якщо людина не хворіє на грип, то ломота в м'язах може спостерігатись в трьох випадках зі ста.

Число 0 після номера 3 (третє питання) виключає наявність грипа у пацієнта при відповіді «Да».

Для визначення ймовірностей в третій секції використовуються експертні оцінки.

Покрокове завдання щодо створення бази знань:

1. Відкрити файл MKBEditor.hlp та продивіться довідку щодо роботи з програмой MKBEditor.exe.

2. Запустіть програму MKBEditor.exe, відкрийте для редагування базу знань щодо грибів Mushrooms.mkb.

3. Доповніть третю секцію бази грибами (подіями) «Бліда поганка» та «Дощовик» (можна якимись іншими), задавши відповідні ймовірності, пов’язані з відповідями на існуючі питання.

4. Доповніть другу секцію кількома питаннями, що дозволять більш точно розпізнавати гриби з третьої секції.

5. Доповніть всі події (гриби) третьої секції трійками чисел, пов’язаних з відповідями на новоутворені питання.

6. Скорегуйте першу секцію, додавши своє прізвище.

7. Збережіть базу знань під назвою MyGrib.mkb та перевірте коректність її функціонування за допомогою програми MiniES.exe.

8. Покажіть результати роботи викладачу.

Завдання на самостійну роботу до теми 5

Створити базу знань, пов’язану з Вашою майбутньою професійною діяльністю.

Список використаних і рекомендованих джерел

1. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 2 груд. 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

2. Хахановський В. Г., Кудінов В. А., Смаглюк В. М. Інформаційні технології у правозастосовній практиці : посібник. Київ : Нац. акад. внутр. справ, 2014. 103 с.

3. Ткаченко Р. О., Кустра Н. О., Павлюк О. М., Поліщук У. В. Засоби штучного інтелекту : навч. посіб. Львів : Львів. політехніка, 2014. 204 с.

4. Новожилова М. В., Петрова О. О. Розробка експертних систем в середовищі CLIPS : навч. посіб. Харків : ХНУМГ ім. О. М. Бекетова, 2019. 130 с.

5. Штучний інтелект. Простий путівник, який допоможе зрозуміти ШІ. URL: https://www.bbc.com/ukrainian/resources/idt-74697280-e684-43c5-a782-29e9d11fecf3.

6. Три стадії штучного інтелекту: чи може він знищити людство? URL: https://www.bbc.com/ukrainian/features-65728291.

РОЗДІЛ VI
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ СТАТИСТИЧНОГО АНАЛІЗУ ПРАВОВИХ ДАНИХ

Використання методів статистичної обробки та аналізу даних має важливе значення в підготовці висококваліфікованих фахівців у галузі права та правоохоронної діяльності, оскільки для науково обґрунтованого пізнання тенденцій і закономірностей розвитку суспільного життя, до якого належать і правові явища, потрібно вміти їх аналізувати. Прийоми і засоби такого аналізу розробляє саме статистична наука. Тому майбутній юрист повинен орієнтуватися в методах статистичного аналізу розвитку суспільних явищ і прийомах такого аналізу в усіх галузях правової науки.

Використання інформаційних технологій значно спрощує рутинну роботу щодо виконання обчислень під час статистичної обробки та аналізу даних. Існує багато різноманітних пакетів програм статистичного аналізу даних. По функціональності програми для статистичного аналізу можна розділити на 3 основних групи: універсальні пакети, або пакети загального призначення; професійні пакети; спеціалізовані пакети. Наприклад, професійні пакети – SAS, BMDP; універсальні пакети – STADIA, STATGRAPHICS, SPSS, STATISTICA; спеціалізовані – BIOSTAT, MESOSAUR, DATASCOPE.

У даному посібнику ми розглянемо використання інформаційних технологій статистичного аналізу даних на базі електронних таблиць MS Excel. MS Excel – це електронна таблиця з досить потужними математичними можливостями, де деякі статистичні функції є просто додатковими вбудованими формулами.

6.1. Теоретичні основи кореляційного та регресійного аналізів

Для статистичного аналізу даних використовуються методи математичної статистики, зокрема, кореляційний та регресійний аналізи.

Дві випадкові величини Y та X можуть бути пов'язані або функціональною залежністю, або залежністю іншого роду, що називається статистичною, або бути незалежними. Чітка функціональна залежність реалізується рідко.

Статистичною називають залежність, під час якої зміна однієї із величин викликає зміну розподілу іншої.

Зокрема, у випадку, якщо під час зміни однієї з величин змінюється середнє значення другої, *статистичну залежність називають кореляційною.*

Кореляційний аналіз досліджує наявність і характер зв'язків між випадковими величинами X та Y – ознаками генеральної сукупності.

Підставою для аналізу залежності між випадковими величинами X та Y є дані вибірки, утвореної внаслідок незалежних спостережень над двовимірною величиною (X, Y).

Елементами вибірки є впорядковані пари чисел (x_i, y_i), $i = \overline{1, n}$, де x_i, y_i – вибіркові значення ознак X та Y, відповідно, що отримують у результаті i-го спостереження, n – обсяг вибірки. Вихідні статистичні дані, як правило,

подаються у вигляді таблиці, рядки (або стовпці) якої закріплені за вибірковими значеннями ознак X та Y.

Якщо обсяг вибірки n достатньо великий, то статистичні дані групують.

Припустимо, що серед вибіркових значень ознаки X можна виділити m різних значень або частинних інтервалів, а серед вибіркових значень ознаки Y є k різних значень або частинних інтервалів. Потім переходять до побудови таблиці. *У випадку дискретної випадкової величини* (X, Y) у першому рядку записують проранжовані варіанти випадкової величини X, а у першому стовпці записують проранжовані варіанти випадкової величини Y. Через $n_{x_i y_j}$ позначимо *частоту появи події* $(X = x_i, Y = y_j),\ i = \overline{1, m},\ j = \overline{1, k}.$ Частоти $n_{x_i y_j}$, які розташовані у внутрішніх клітинах таблиці разом із відповідними їм парами чисел (x_i, y_j), становлять емпіричну (статистичну) структуру закону сумісного розподілу випадкових величин X та Y. В останньому рядку (стовпці) таблиці записують частоти варіант x_i (y_j), які позначають через n_{x_i} (n_{y_j}). Частоти варіант пов'язані між собою співвідношеннями:

$$n_{x_i} = \sum_{j=1}^{k} n_{x_i y_j};\ i = \overline{1, m}; \quad n_{y_j} = \sum_{i=1}^{m} n_{x_i y_j};\ j = \overline{1, k}.$$

Виконується також очевидна рівність:

$$\sum_{i=1}^{m}\sum_{j=1}^{k} n_{x_i y_j} = \sum_{i=1}^{m} n_{x_i} = \sum_{j=1}^{k} n_{y_j} = n.$$

Частоти n_{x_i} та n_{y_j} разом із відповідними варіантами x_i і y_j характеризують емпіричні (статистичні) закони розподілу одновимірних випадкових величин X та Y.

Побудовану таким чином таблицю називають *кореляційною*.

Якщо для побудови кореляційної таблиці замість варіант візьмемо *частинні інтервали*, то в кожному з них необхідно обрати свого «представника», тобто середину відповідного інтервалу, тоді числа x_i (y_j) означають середини відповідних інтервалів.

Із теорії ймовірностей відомо, що ступінь зв'язку між випадковими величинами X і Y визначається такими числовими характеристиками їх сумісного розподілу, як *коваріація* $\operatorname{cov}(X, Y)$ і *коефіцієнт кореляції* $\rho(X, Y)$, які обчислюються за формулами:

$$\operatorname{cov}(X, Y) = M(X \cdot Y) - M(X) \cdot M(Y);$$

$$\rho(X, Y) = \frac{\operatorname{cov}(X, Y)}{\sigma(X) \cdot \sigma(Y)}.$$

Основне завдання кореляційного аналізу полягає у виявленні залежностей між випадковими величинами X та Y і може бути розв'язане шляхом побудови статистичних оцінок коефіцієнта кореляції.

Статистичну точкову оцінку для коефіцієнта кореляції обчислюють за формулою:

$$r = r(X, Y) = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} = \frac{\sum_{i=1}^{n} x_i y_i - n\,\bar{x}\cdot\bar{y}}{\sqrt{(\sum_{i=1}^{n} x_i^{\,2} - n\bar{x}^2)(\sum_{i=1}^{n} y_i^{\,2} - n\bar{y}^2)}}. \qquad (3.1)$$

Вибірковим коефіцієнтом кореляції називається статистична точкова оцінка r коефіцієнта кореляції між випадковими величинами X і Y, яка обчислюється за формулою (3.1).

Вибірковий коефіцієнт кореляції характеризує зв'язок між випадковими величинами X і Y – ознаками генеральної сукупності:

а) якщо $r > 0$, то зв'язок між X і Y є додатним і вони зменшуються або збільшуються одночасно;

б) якщо $r < 0$, то зв'язок між X і Y є від'ємним – із збільшенням однієї з них друга зменшується або навпаки; якщо $r = 0$, то випадкові величини X і Y – некорельовані, і це не означає лише відсутність лінійного зв'язку між ними.

Вибірковий *коефіцієнт кореляції задовольняє нерівність*

$| r | \le 1.$

На практиці користуються також коефіцієнтом детермінації.

Коефіцієнтом детермінації називається квадрат вибіркового коефіцієнта кореляції (r^2).

Приклад. За даними 20-ти туристичних фірм були встановлені витрати на рекламу x_i (ум. од.) і кількість туристів y_i (чол.), що скористалися послугами кожної фірми. Дослідити залежність між цими ознаками (у таблиці 6.1 подані дані, що проранжовані за величиною витрат на рекламу).

Таблиця 6.1

№ з/п	x_i	y_i
1	8	800
2	8	850
3	8	720
4	9	850
5	9	800
6	9	880
7	9	950
8	9	820
9	10	900
10	10	1 000
11	10	920
12	10	1 060
13	10	950
14	11	900
15	11	1 200
16	11	1 150
17	11	1 000
18	12	1 200
19	12	1 100
20	12	1 000

Розв'язання. Із таблиці 3.1 можна бачити, що взагалі збільшення витрат на рекламу призводить до збільшення кількості туристів, що користуються послугами фірми, хоча в окремих випадках наявність такої залежності може й не простежуватися. У кожному окремому випадку кількість туристів, що скористалися послугами фірми, залежатиме не тільки від розміру витрат фірми на рекламу, а й від того, як спрацюють інші фактори, що визначають цю величину.

Перевіримо наявність прямої залежності між досліджуваними ознаками.

Для цього обчислимо вибірковий коефіцієнт кореляції. Для його розрахунку складемо таблицю 6.2 і скористаємося формулою (6.1).

Таблиця 6.2

№ пор.	x_i	y_i	x_i^2	y_i^2	$x_i y_i$
1	8	800	64	640 000	6 400
2	8	850	64	722 500	6 800
3	8	720	64	518 400	5 760
4	9	850	81	722 500	7 650
5	9	800	81	640 000	7 200
6	9	880	81	774 400	7 920
7	9	950	81	902 500	8 550
8	9	820	81	672 400	7 380
9	10	900	100	810 000	9 000
10	10	1 000	100	1 000 000	10 000
11	10	920	100	846 400	9 200
12	10	1 060	100	1 123 600	10 600
13	10	950	100	902 500	9 900
14	11	900	121	810 000	9 900
15	11	1 200	121	1 440 000	13 200
16	11	1 150	121	1 322 500	12 650
17	11	1 000	121	1 000 000	11 000
18	12	1 200	144	1 440 000	14 400
19	12	1 100	144	1 210 000	13 200
20	12	1 000	144	1 000 000	12 000
$\sum_{i=1}^{20}$	199	19 050	2 013	18 497 700	192 310

У результаті отримаємо: $r = 0{,}8105$. Отримана величина є свідченням наявності досить тісної прямої залежності між досліджуваними ознаками. Коефіцієнт детермінації обчислюємо як квадрат вибіркового коефіцієнта кореляції $(r^2) = (0{,}8105)^2 = 0{,}6569$, а це означає, що 65,69 % варіації кількості клієнтів, що скористалися послугами фірми, пояснюється варіацією витрат фірм на рекламу своїх послуг.

На відміну від кореляційного аналізу, який досліджує наявність і характер зв'язків між випадковими величинами X і Y – ознаками

генеральної сукупності, регресійний аналіз встановлює аналітичну форму цієї залежності.

Якщо $r(X,Y)\neq 0$, то X і Y – корельовані випадкові величини. Із наближенням величини $|r(X,Y)|$ до одиниці залежність між цими випадковими величинами наближається до лінійної залежності вигляду $Y=\alpha X+\beta$.

Як відомо, рівняння лінійної регресії Y на X має вигляд:

$$y=\alpha x+\beta, \tag{6.2}$$

де $\alpha=\rho(X,Y)\dfrac{\sigma(Y)}{\sigma(X)}$, $\beta=M(Y)-\alpha M(X)$. (6.3)

Вибірковим рівнянням лінійної регресії Y на X називається рівняння (6.2), якщо коефіцієнти в ньому вибрано у вигляді точкових оцінок α і β, визначених співвідношеннями (3.3).

Припустимо, що X – незалежна змінна (факторна ознака), а Y – залежна змінна (результативна ознака). Для отримання повного опису залежності між випадковими величинами X і Y потрібно знайти аналітичний вираз сумісного розподілу цих величин, тобто функцію: $F(x,y)=P(x<X,y<Y)$, що, як правило, практично неможливо. Тому під час дослідження аналітичної залежності між випадковими величинами X і Y обмежуються вивченням залежності між однією з них і умовним математичним сподіванням іншої, зокрема залежністю виду:

$\bar{y}_x=f^*(x)$ – вибіркове рівняння регресії Y на X; $\overline{y_x}=M(Y\mid X=x)$;

$\bar{x}_y=g^*(y)$ – вибіркове рівняння регресії X на Y; $\overline{x_y}=M(X\mid Y=y)$.

У наведених вибіркових рівняннях регресії $\bar{y}_x$ і $\bar{x}_y$ – вибіркові умовні математичні сподівання, відповідно, Y на X та X на Y, а $f^*(x)$ і $g^*(y)$ – вибіркові функції регресії, відповідно. Аналітичні вирази для функцій $f^*(x)$ і $g^*(y)$ будуємо на підставі проведеної вибірки $(x_1,y_1),(x_2,y_2),\ldots,(x_n,y_n)$. Характер відповідної регресійної моделі допомагає вибрати діаграма розсіювання точок (x_i,y_i) на площині.

Припускаючи, що: ознака Y у генеральній сукупності розподілена нормально; дисперсія результативної ознаки Y не залежить від факторної ознаки X; характер зв'язку між результативною та факторною ознаками – лінійний, тоді маємо найпростішу регресійну модель – *лінійної регресії*, коли *вибіркове рівняння регресії Y на X має такий вигляд:*

$$\bar{y}_x=\alpha\cdot x+\beta.$$

У цьому випадку для точкових оцінок α і β можна побудувати довірчі інтервали і оцінити їх значущість.

Основним методом отримання точкових оцінок для параметрів α і β рівняння регресії є *метод найменших квадратів.*

Припустимо, що вибірка $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ обсягу n – *не згрупована*. Оскільки ми припустили існування лінійного зв'язку між результативною та факторною ознаками, то діаграма розсіювання точок (x_i, y_i) має вигляд (рис. 6.4):

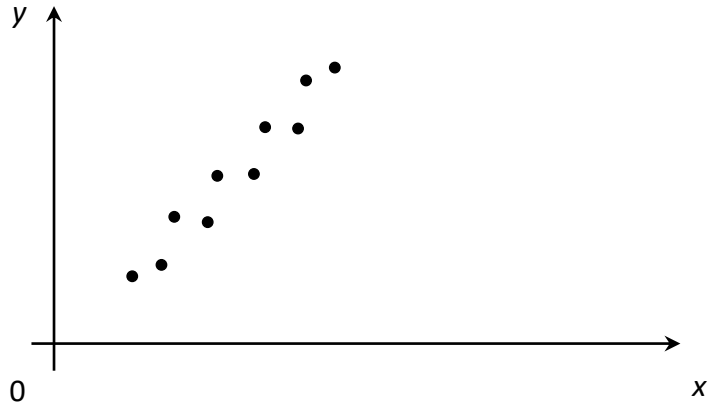


Рис 6.4. Діаграма розсіювання точок

Основна ідея методу найменших квадратів полягає в тому, що точковими оцінками $\overline{\alpha}$ і $\overline{\beta}$ параметрів α і β вибирають такі числа, для яких пряма $\overline{y}_x = \alpha x + \beta$ є "найближчою" до точок $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$.

Мірою відхилення шуканої прямої від точок (x_i, y_i) вибирають величину:

$$S(\alpha, \beta) = \sum_{i=1}^{n} [y_i - (\alpha x_i + \beta_i)]^2,$$

тобто суму квадратів різниць між ординатами прямої та ординатами точок (x_i, y_i) для одних і тих самих значень $x = x_i$.

Якщо числа α і β – такі, що функція $S(\alpha, \beta)$ має найменше значення, то пряма $\overline{y}_x = \alpha x + \beta$ найменше відхиляється від точок (x_i, y_i).

Методом найменших квадратів називається метод знаходження статистичних оцінок $\overline{\alpha}$ і $\overline{\beta}$ параметрів α і β за допомогою функції $S(\alpha, \beta)$, виходячи з рівності:

$$S(\overline{\alpha}, \overline{\beta}) = \min S(\alpha, \beta).$$

Для знаходження мінімуму функції $S(\alpha, \beta)$ маємо розв'язати систему рівнянь:

$$\begin{cases} \dfrac{\partial S(\alpha, \beta)}{\partial \alpha} = 2\sum\limits_{i=1}^{n} [y_i - (\alpha x_i + \beta)] \cdot (-x_i) = 0, \\ \dfrac{\partial S(\alpha, \beta)}{\partial \beta} = (-2)\sum\limits_{i=1}^{n} [y_i - (\alpha x_i + \beta)] = 0, \end{cases}$$

яку елементарними перетвореннями зводимо до такого вигляду:

$$\begin{cases} \alpha(\sum_{i=1}^{n} x_i^2) + \beta(\sum_{i=1}^{n} x_i) = \sum_{i=1}^{n} x_i y_i, \\ \alpha(\sum_{i=1}^{n} x_i) + \beta \cdot n = \sum_{i=1}^{n} y_i. \end{cases}$$

У випадку *згрупованої вибірки* для визначення невідомих параметрів α *і* β маємо систему двох рівнянь:

$$\begin{cases} \alpha(\sum_{i=1}^{m} n_{x_i} x_i^2) + \beta(\sum_{i=1}^{m} n_{x_i} x_i) = \sum_{i=1}^{m}\sum_{j=1}^{k} n_{x_i y_j} x_i y_j, \\ \alpha(\sum_{i=1}^{m} n_{x_i} x_i) + \beta \cdot n = \sum_{i=1}^{k} n_{y_j} y_i, \end{cases}$$

де n_x, n_y $(i = \overline{1, m};\ j = \overline{1, k})$ – частоти відповідних варіант x_i та y_j;

$n_{x_i y_j}$ – частота появи події $(X = x_i, Y = y_j)$.

Припускаючи, що ознака X не є сталою, тобто серед варіант $x_1, x_2, ..., x_n$ обов'язково є різні числа, робимо висновок про визначник системи:

$$\begin{vmatrix} \sum_{i=1}^{n} x_i^2 & \sum_{i=1}^{n} x_i \\ \sum_{i=1}^{n} x_i & n \end{vmatrix} = n\sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2 > 0.$$

Звідси випливає, що досліджувана система рівнянь має єдиний розв'язок:

$$\alpha = \frac{\overline{xy} - \bar{x} \cdot \bar{y}}{\bar{\sigma}_x^2} = \bar{\alpha}, \quad \beta = \bar{y} - \bar{\alpha} \cdot \bar{x} = \bar{\beta},$$

де $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i, \quad \bar{y} = \frac{1}{n}\sum_{i=1}^{n} y_i, \quad \bar{\sigma}_x^2 = \bar{D}_x = \frac{1}{n}\sum_{i=1}^{n} x_i^2 - (\bar{x})^2, \quad \overline{xy} = \frac{1}{n}\sum_{i=1}^{n} x_i y_i.$

Таким чином, шукане рівняння регресії набуває такого вигляду:

$$\bar{y}_x = \bar{\alpha} x + \bar{\beta}.$$

Коефіцієнт $\bar{\alpha}$ *називають коефіцієнтом регресії, який характеризує відношення величини приросту результативної ознаки* $\Delta\bar{y}_x$ *до величини приросту факторної ознаки* Δx.

Лінійне рівняння регресії можна подати в іншому вигляді через статистичну оцінку коефіцієнта кореляції:

$$\bar{y}_x - \bar{y} = r_{xy}^* \frac{\bar{\sigma}_y}{\bar{\sigma}_x}(x - \bar{x}).$$

Необхідно зауважити, що в разі порушення припущення про лінійність зв'язку між результативною та факторною ознаками, а про це можна зробити висновок із діаграми розсіювання вибірки, використовують нелінійні регресійні моделі. У нелінійних регресійних моделях зв'язок може виражатися, наприклад, такими рівняннями: $\bar{y}_x = ax^2 + bx + c$ або $\bar{y}_x = ax^3 + bx^2 + cx + d$,

або $\bar{y}_x = a/x + b$. Статистичні оцінки параметрів у цих нелінійних моделях також можна знайти за допомогою методу найменших квадратів.

Приклад. Знайти рівняння регресії *Y* на *X* на підставі вибірки:

*x*i	11,2	11,5	11,8	22,1	22,3	33,0	33,6	44,2	55,7	66,3
*y*i	55,6	66,8	77,8	99,4	110,3	111,4	112,9	114,8	115,2	118,5

Розв'язання. Для знаходження рівняння регресії проведемо необхідні обчислення:

$$\bar{x}_B = \frac{1{,}2 + 1{,}5 + \ldots + 6{,}3}{10} = 3{,}17; \quad \bar{y}_B = \frac{5{,}6 + 6{,}8 + \ldots + 18{,}5}{10} = 11{,}27.$$

$$D_B(X) = 0{,}1(1{,}2^2 + 1{,}5^2 + \ldots + 6{,}3^2) - 3{,}17^2 = 2{,}7921;$$

$$\sigma_X = \sqrt{2{,}7921} = 1{,}671.$$

$$D_B(Y) = 0{,}1(5{,}6^2 + 6{,}8^2 + \ldots + 18{,}5^2) - 11{,}27^2 = 15{,}146;$$

$$\sigma_Y = \sqrt{15{,}146} = 3{,}892.$$

Для обчислення вибіркового коефіцієнта кореляції обчислимо попередньо:

$$\sum_{i=1}^{10} x_i y_i = 1{,}2 \cdot 5{,}6 + 1{,}5 \cdot 6{,}8 + \ldots + 6{,}3 \cdot 18{,}5 = 420{,}38.$$

Тоді $r_B = \dfrac{420{,}38 - 10 \cdot 3{,}17 \cdot 11{,}27}{10 \cdot 1{,}671 \cdot 3{,}892} = 0{,}97.$

Отже, рівняння регресії Y на X, одержане на підставі вибірки:

$$y - 11{,}27 = 0{,}97 \cdot \frac{3{,}892}{1{,}671}(x - 3{,}17), \text{ або } y = 2{,}26x - 4{,}104.$$

6.2. Програмна реалізація методів статистичного аналізу

Кількісний (числовий) аналіз дає можливість правильно інтерпретувати результати наукових досліджень і експериментів: висновки стають більш незалежними від особистості дослідника і забезпечується можливість їхньої перевірки. Такий аналіз можна проводити засобами пакету Microsoft Excel або спеціалізованими статистичними пакетами: STADIA, STATGRAPHICS, SPSS, ЭВРИСТА.

Переваги використання пакету Microsoft Excel щодо проведення статистичного аналізу даних наукових досліджень:

– широке розповсюдження (практично безкоштовний);
– легкий у вивченні та використанні;
– наявність русифікованих версій з відповідною електронною довідкою.

Недоліки використання пакету Microsoft Excel в статистичних дослідженнях:

– якщо обчислення найпростіших статистик виконується бездоганно, то в більш складних задачах можливі помилки;

– принципи замовчання, покладені в інтерпретацію змісту клітинок, можуть призвести до неможливості автоматичного розпізнавання помилки під час заповнення вхідних діапазонів статистичних даних;

– деякі задачі статистичного аналізу (факторний, кластерний, дискримінантний аналізи) не можуть в автоматичному режимі бути вирішені засобами Microsoft Excel.

Деякі вбудовані статистичні функції пакету Microsoft Excel:

– **МОДА** – обчислює значення моди M_0 – значення ознаки, яка найчастіше трапляється в даній сукупності.

– **МЕДІАНА** – обчислює значення медіани M_e – значення ознаки, яка ділить розподіл (площу під кривою розподілу) на дві рівні частини.

– **СРЗНАЧ** повертає середнє арифметичне своїх аргументів.

Синтаксис **СРЗНАЧ**(число1; число2; ...)

Число1, число2, ... – це від 1 до 30 аргументів, для яких обчислюється середнє за формулою: $M_x = \frac{\sum_{i=1}^{n} x_i}{n}$.

Зауваження: пусті клітинки ігноруються, нульові – враховуються.

– Функція **ДИСПР** повертає значення дисперсії. Передбачається, що аргументи функції являють собою усю генеральну сукупність. Якщо дані мають тільки вибірку з генеральної сукупності, то дисперсію треба обраховувати за допомогою функції **ДИСП**.

Рівняння для **ДИСПР** має наступний вигляд:

$$\overline{D}_x = \frac{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2}{n^2}.$$

– **ДИСП** оцінює дисперсію за вибіркою

$$D_x = \frac{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2}{n\cdot(n-1)}.$$

– **СТАНДВІДХИЛП** повертає значення стандартного відхилення для генеральної сукупності $\sigma_x = \sqrt{\frac{n\sum x_i^2 - \left(\sum x_i\right)^2}{n^2}}$.

– **СТАНДВІДХИЛ** оцінює стандартне відхилення за вибіркою

$$\sigma_x = \sqrt{\frac{n\sum x_i^2 - \left(\sum x_i\right)^2}{n\cdot(n-1)}}.$$

– Функція **НОРМСТРОЗП** повертає стандартний нормальний інтегрований розподіл, середнє значення якого дорівнює нулю і стандартне відхилення дорівнює одиниці.

Функція має синтаксис **НОРМСТРОЗП(z)**, де **z** – значення, для якого будуємо розподіл.

Рівняння щільності стандартного нормального розподілу має наступний вигляд: $f(z;0,1)=\frac{1}{\sqrt{2\pi}}e^{-\frac{z^2}{2}}$.

– Функція **НОРМРОЗП** повертає нормальну функцію розподілу для вказаного середнього і стандартного відхилення.

Функція має синтаксис **НОРМРАСП(x;μ;σ;інтегральна)**, де:

x – значення, для якого будуємо розподіл;

μ – середнє арифметичне (математичне очікування) розподілу;

σ – стандартне відхилення (середнє квадратичне відхилення) розподілу.

Інтегральна – логічне значення, що визначає форму функції. Якщо інтегральна має значення TRUE (1), то функція НОРМРОЗП повертає інтегральну функцію розподілу; якщо цей аргумент має значення FALSE (0), то повертається функція щільності розподілу.

Рівняння щільності нормального розподілу має вигляд:

$$f(x;\mu,\sigma)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\left(\frac{(x-\mu)^2}{2\sigma^2}\right)}.$$

Якщо випадкова величина X розподілена за нормальним законом з математичним очікуванням **μ** та середнім квадратичним відхиленням **σ**, то ймовірність того, що X буде належати інтервалу (α,β) визначається за формулою: $P(\alpha<X<\beta)=\Phi\left(\frac{\beta-\mu}{\sigma}\right)-\Phi\left(\frac{\alpha-\mu}{\sigma}\right)$, де Φ(z) – функція Лапласа.

Значення функції Лапласа в точці z може бути обраховане за формулою: Φ(z)= НОРМСТРОЗП(z) – 0,5.

– **СКОС** повертає асиметрію розподілу. Асиметрія характеризує ступінь несиметричності розподілу відносно його середнього.

$$A_s=\frac{n}{(n-1)\cdot(n-2)}\cdot\sum\left(\frac{x_i-M_x}{\sigma_x}\right)^3.$$

– **ЕКСЦЕСС** повертає ексцесс розподілу, що характеризує гостровершинність (+) чи плосковершинність (-) кривої розподілу.

$$E_x=\frac{n(n+1))}{(n-1)(n-2)(n-3)}\sum\left(\frac{x_i-M_x}{\sigma_x}\right)^4-\frac{3(n-1)^2}{(n-2)(n-3)}.$$

– **БІНОМРОЗП** – повертає окреме значення біноміального розподілу. Функція БІНОМРОЗП використовують в задачах з фіксованою кількістю тестів або випробувань, коли результат кожного випробування може приймати тільки одне з двох значень: успіх або невдача, випробування незалежні і ймовірність успіху постійна на протязі всього експерименту.

Наприклад, БІНОМРОЗП може обрахувати ймовірність того, що двоє з трьох наступних новонароджених будуть хлопчики.

Синтаксис:

БІНОМРОЗП(кількість_успіхів;кількість_випробувань;ймовірність_успіху;інтегральна)

Кількість_успіхів – це кількість успішних випробувань.

Кількість_випробувань – це кількість незалежних випробувань.

Ймовірність_успіху – це ймовірність успіху під час кожного випробування.

Інтегральна – це логічне значення, що визначає форму функції. Якщо аргумент інтегральна має значення ИСТИНА, то функція БИНОМРАСП повертає інтегральну функцію розподілу, а саме ймовірність того, що кількість успішних випробувань не менш ніж значення аргументу кількість_успіхів; якщо цей аргумент має значення ЛОЖЬ, то повертається функція розподілу, а саме ймовірність того, що кількість успішних випробувань точно дорівнює значенню аргументу число_успіхів.

Біноміальна функція розподілу має наступний вигляд:

$$b(m;n,p) = C_n^m p^m (1-p)^{n-m}$$, де:

C_n^m обраховується за допомогою функції ЧИСЛКОМБ(n;m).

Інтегральний біноміальний розподіл має вигляд:

$$B(m;n,p) = \sum_{x=0}^{m} b(x;n,p).$$

– **ДОВЕРИТ** – повертає довірчий інтервал для середнього генеральної сукупності. Довірчий інтервал – це інтервал з обох сторін від середнього вибірки. Наприклад, при замовленні товару по пошті можливо визначити з певним рівнем достовірності саму ранню та саму пізню дати прибуття товару.

Синтаксис: **ДОВЕРИТ(α; σ;n)**, де:

α – це рівень значимості, що використовується для обчислення рівня надійності. Рівень надійності дорівнює 100*(1 – α) відсоткам, або, іншими словами, α, що дорівнює 0,05, означає 95-відсотковий рівень надійності;

σ – це стандартне відхилення генеральної сукупності для інтервалу даних, вважається відомим;

n – це розмір вибірки.

Зауваження: якщо вважати, що α дорівнює 0,05, то треба визначити ту частину стандартної нормальної кривої, яка дорівнює (1 – α), або 95 відсоткам.

Це значення дорівнює ±1,96. Довірчий інтервал в цьому випадку визначається наступним чином: $\bar{x} \pm 1{,}96\left(\frac{\sigma}{\sqrt{n}}\right)$.

Надбудова «Аналіз даних»: підключення та використання. До складу Microsoft Excel входять засоби статистичного аналізу даних (так званий пакет аналізу), призначений для вирішення статистичних та інженерних задач. Для аналізу даних за допомогою цих інструментів треба вказати вхідні дані і вибрати параметри; аналіз буде виконано за допомогою відповідної статистичної або інженерної макрофункції, а результат буде розміщено у вихідному діапазоні. Інші засоби дозволяють представити результати аналізу в графічному вигляді.

Якщо в меню **Сервіс** (для Microsoft Excel версії 2003 та попередніх) або на стрічці Дані (для Microsoft Excel версії 2007 та наступних) відсутній пункт **Аналіз даних**, то треба:

- (для пакетів Microsoft Office версії 2003 та більш ранніх) клацнути покажчиком миші по **Сервіс-Надбудови...** та встановити прапорець **Пакет аналізу**;
- (для пакетів Microsoft Office версії 2007 та наступних) клацнути покажчиком миші по **Файл-Параметри-Надбудови** та встановити у списку **Керування** значення **Надбудови Excel**, після чого клацнути по кнопці **Перейти** та встановити прапорець **Пакет аналізу**.

Розглянемо деякі інструменти пакету аналізу, що використовуються при обробці даних наукових експериментів.

Дисперсійний аналіз. Існує декілька типів дисперсійного аналізу. Потрібний варіант вибирається з урахуванням числа факторів та наявних виборок з генеральної сукупності.

Однофакторний дисперсійний аналіз. Застосовують для перевірки гіпотези щодо подібності середніх значень двох або більшої кількості виборок, що належать до однієї генеральної сукупності. Цей метод розповсюджується також на тести для двох середніх (до яких відноситься, наприклад, t-критерій).

Двофакторний дисперсійний аналіз з повтореннями. Являє собою більш складний варіант однофакторного аналізу з кількома вибірками для кожної групи даних.

Двофакторний дисперсійний аналіз без повторень. Являє собою двофакторний аналіз дисперсії, що не містить більш однієї вибірки на групу. Використовується для перевірки гіпотези щодо однаковості середніх значень двох або кількох вибірок (вибірки належать до однієї генеральної сукупності). Цей метод розповсюджується також на тести для двох середніх, таких як t-критерій.

Кореляційний аналіз. Кореляційний аналіз застосовується для кількісної оцінки взаємозв’язку двох наборів даних, представлених в безрозмірному вигляді. Коефіцієнт кореляції вибірки являє відношення коваріації двох наборів даних до добутку їх стандартних відхилень і обраховується за формулами:

$$\rho_{x,y} = \frac{\text{cov}(X,Y)}{\sigma_X \cdot \sigma_Y}, \text{ де:}$$

$$\sigma_X = \frac{1}{n}\sum (X_j - \mu_X)^2,\ \sigma_Y = \frac{1}{n}\sum (Y_j - \mu_Y)^2.$$

Кореляційний аналіз дає можливість встановити асоційовані набори даних по величині, тобто, більші значення з одного набора даних пов'язані з більшими значеннями другого набору (позитивна кореляція) чи, навпаки, малі значення одного набору пов'язані з більшими значеннями другого (негативна кореляція), чи дані двох діапазонів ніяк не пов'язані (нульова кореляція).

Примітка. Для обчислення коефіцієнту кореляції між двома наборами даних на аркуші використовується статистична функція КОРРЕЛ.

Коваріаційний аналіз. Коваріація є мірою зв'язку між двома діапазонами даних. Використовується для обчислення середнього добутку відхилень точок даних від відносних середніх за наступною формулою:

$$\text{cov}(X,Y) = \frac{1}{n}\sum (x_j - \mu_x)(y_j - \mu_y).$$

Описова статистика. При роботі з різними даними часто необхідно знайти головну тенденцію і зрозуміти значимість змін. Інструмент описової статистики обчислює кілька параметрів основної тенденції і кілька параметрів дисперсії для одного набору даних або для змінної.

Цей засіб аналізу використовують для створення одновимірного статистичного звіту, що містить інформацію щодо центральної тенденції і мінливості вхідних даних.

Тести Z, T та F. Ці тести використовуються для порівняння середніх і дисперсій. Z-тест призначений для великих вибірок, T-тест краще підходить для невеликих вибірок (менш 30 значень). Передбачається, що обидві вибірки узяті з набору даних з нормальним розподілом.

T-тест існує в двох варіантах: 1) дисперсії двох вибірок рівні; 2) дисперсії не рівні. F-тест перевіряє припущення про те, що дисперсії двох вибірок, на відміну від середнього, рівні.

Двовибірковий F-тест для дисперсії. Двовибірковий F-тест використовують для порівняння дисперсій двох генеральних сукупностей.

Наприклад, F-тест можна використати для виявлення відмінностей в дисперсіях часових характеристик, обчислених по двом вибіркам.

T-тест. Цей вид аналізу використовується для перевірки середніх для різних типів генеральних сукупностей.

Двовибірковий t-тест з однаковими дисперсіями. Двохвибірковий t-тест Стьюдента слугує для перевірки гіпотези щодо тотожності середніх для двох вибірок. Ця форма t-тесту передбачає співпадання дисперсій генеральних сукупностей і звичайно зветься гомоскедастическим t-тестом.

Двохвибірковий t-тест з різними дисперсіями. Двохвибірковий t-тест Стьюдента слугує для перевірки гіпотези щодо тотожності середніх для двох вибірок даних з різних генеральних сукупностей. Ця форма t-тесту передбачає

відмінність дисперсій генеральних сукупностей і звичайно зветься гетероскедастическим t-тестом. Якщо тестується одна і та ж генеральна сукупність, використовуйте парний тест.

Для визначення тестової величини t використовується наступна формула:

$$t' = \frac{\bar{x} - \bar{y} - \Delta_0}{\sqrt{\frac{S_1^2}{m} + \frac{S_2^2}{n}}}.$$

Наведена нижче формула використовується для апроксімації числа ступенів свободи. Як правило, результатом обчислень є дійсне число, тому проводьте округлення до найближчого цілого, щоб отримати критичне значення t з таблиці.

$$\partial f = \frac{\left(\frac{S_1^2}{m} + \frac{S_2^2}{n}\right)}{\frac{(S_1^2/m)^2}{m-1} + \frac{(S_2^2/n)^2}{n-1}}.$$

Парний двовибірковий t-тест для середніх. Парний двовибірковий t-тест Стьюдента використовують для перевірки гіпотези щодо відмінності середніх для двох вибірок даних. В ньому не передбачується рівність дисперсій генеральних сукупностей, з яких вибрані дані. Парний тест використовується, коли існує природня парність спостережень у вибірках, наприклад, коли генеральна сукупність тестується двічі – до і після експерименту.

Z-тест. Двовибірковий z-тест для середніх з відомими дисперсіями. Використовується для перевірки гіпотези щодо відмінності між середніми двох генеральних сукупностей.

Наприклад, цей тест може бути використаний для визначення відмінності між характеристиками двох моделей автомобілей.

Гістограма. Використовується для обчислення вибіркових та інтегральних частот розподілу експериментальних даних у вказані інтервали значень. При цьому розраховують числа влучень для заданого діапазону клітинок.

Наприклад, треба виявити тип розподілу успішності в групі з 20 курсантів. Таблиця гістограми складається з границь шкали оцінок і кількостей студентів, рівень успішності яких знаходиться між самою нижньою границею і поточною границею. Рівень, що найбільш часто зустрічається, є модою інтервалу даних.

Змінне середнє. Змінне середнє використовують для розрахунку значень в прогнозуємому періоді на основі середнього значення змінної для заданої кількості попередніх періодів. Змінне середнє, на відміну від простого середнього для всієї вибірки, містить відомості щодо тенденцій зміни даних. Цей метод може бути застосований для прогнозу збуту, запасів та інших процесів. Розрахунок прогнозуємих значень виконується за наступною формулою:

$$F_{t+1} = \frac{1}{N}\sum_{j=1}^{N} A_{t-j+1}$$

де:

- N – число попередніх періодів, що входить до змінного середнього;
- A_j – фактичне значення в момент часу j;
- F_j – прогнозуєме значення в момент часу j.

Генерація випадкових чисел. Використовуються для заповнення діапазону випадковими числами, узятими з одного або кількох розподілів. За допомогою даної процедури можна змоделювати об’єкти, що мають випадковий характер, по відомому розподілу ймовірностей.

Наприклад, можна використати нормальний розподіл для моделювання сукупності даних щодо росту індивідуумів або використати розподіл Бернуллі для двох рівноймовірних результатів, щоб описати сукупність результатів кидання монети.

Ранг і персентиль. Використовується для виведення таблиці, що містить порядковий і відсотковий ранги для кожного значення в наборі даних. Означена процедура може бути застосована для аналізу відносного взаєморозташування даних в наборі.

Регресія. Лінійний регресійний аналіз полягає в підбиранні графіку для набору спостережень за допомогою методу найменших квадратів. Регресія використовується для аналізу впливу на окрему залежну змінну значень однієї чи більше незалежних змінних.

Наприклад, на спортивні якості атлета впливають кілька факторів, зокрема: вік, зріст та вага. Регресія пропорційно розподіляє міру якості по цим трьом факторам на основі його спортивних досягнень. Результати регресії в подальшому можуть бути використані для прогнозування якостей нового, неперевіреного атлету.

Вибірка. Створює вибірку з генеральної сукупності, вважаючи вхідний діапазон як генеральну сукупність. Якщо сукупність завелика для обробки або побудови діаграми, можна використовувати репрезентативну вибірку.

Більш детальна інформація щодо застосування Microsoft Excel в якості інструменту для проведення кореляційного та регресійного аналізів наведена в практичному завданні 6.2 в кінці даної глави.

Питання для самоконтролю

1. Поняття про кореляцію
2. Поняття рангової кореляції.
3. Кореляційне поле
4. Коефіцієнт кореляції як міра кореляційного зв’язку
5. Вибірковий коефіцієнт лінійної парної кореляції Пірсона.
6. Вибіркове рівняння регресії.
7. Оцінка значення досліджуваної ознаки на основі рівняння регресії.
8. Яка залежність між випадковими величинами називається статистичною?
9. В якому випадку статистичну залежність називають кореляційною?
10. В чому полягає основне завдання кореляційного аналізу?

11. Що таке коефіцієнт детермінації?
12. В якому діапазоні знаходиться значення коефіцієнта кореляції?
13. Що таке вибіркове рівняння лінійної регресії?
14. В чому полягає основна ідея методу найменших квадратів?
15. Який вигляд має рівняння лінійної регресії?

Практичні завдання до розділу VI

Практичне заняття № 6.1

Мета заняття: навчитись здобувачам магістратури прогнозувати перебіг подій засобами програми MS Excel.

Завдання:

1. Створити за допомогою програми Excel файл з назвою **Ваше прізвище_П.з. 6.1**.
2. Встановити **пароль** на файл.
3. Лист 1 назвати «Головна таблиця».

Лист 2 назвати «Дані за наслідками НП».

Лист 3 назвати «Прогноз надзвичайних подій».

4. На листі «Головна таблиця» засобами Excel створити таблицю:
5. Провести розрахунки даних для стовпця 5 і рядків «Всього (1-10):», «Середнє (1-10):».

- Для рядка «Всього (1-10):» встановити 0 десяткових розрядів у числах.
- Для рядка «Середнє (1-10):» встановити 1 десятковий розряд у числах.
- Виділити дані стовпця 5 і рядків «Всього (1-10):», «Середнє (1-10):» напівжирним накресленням.

6. На листі «Дані за наслідками НП» створити діаграму «Графік» по заданій таблиці для рядків 1-10 та стовпців 2-4.

На створеній діаграмі:

- вказати назву діаграми;
- вказати назву осей X, Y;
- створити легенду з назвами кривих;
- вказати на кривих мітки даних (шрифт Arial, курсив, розмір 8 пт);
- вказати лінії трендів для кривих.

7. Скопіювати діаграму «Графік» з листа «Дані за наслідками НП» на лист «Прогноз надзвичайних подій».

На діаграмі для кожної лінії тренду у контекстному меню вибрати команду «Формат лінії тренду», де вказати прогноз вперед на 2 періоди та встановити прапорець «Показувати рівняння на діаграмі».

8. З використанням отриманих формул заповнити рядки 11 та 12 таблиці на листі «Головна таблиця» (примітка: замість змінної «х» у формулах вказати 11 або 12, відповідно).

Встановити 0 десяткових розрядів у числах.

9. Провести розрахунки даних для стовпця 5 і рядків «Всього (1-12):», «Середнє (1-12):».

- Для рядка «Всього (1-12):» встановити 0 десяткових розрядів у числах.
- Для рядка «Середнє (1-10):» встановити 1 десятковий розряд у числах.
- Виділити дані стовпця 5 і рядків «Всього (1-12):», «Середнє (1-12):» напівжирним накресленням.

10. На листі «Прогноз надзвичайних подій» у контекстному меню діаграми вибрати команду «Вибрати дані» та розширити перелік полів для побудови діаграми у полі «Діапазон даних для діаграми».

(Зразок: =‘Головна таблиця’!$D$11:$F$20;’Головна таблиця’!$D$24:$F$25)

11. Для стовпця 6 записати формулу, яка відповідає критеріям:

- якщо «Всього надзвичайних подій» >= 100, то записати «Високий»;
- якщо «Всього надзвичайних подій» >= 80, но < 100, то записати «Середній»;
- якщо «Всього надзвичайних подій» < 80, то записати «Низький».

Для клітинок з написом «Високий» вибрати колір заливки «Червоний», «Середній» – «Жовтий», «Низький» – «Зелений».

(Примітка: використовуйте функцію IF)

Практичне заняття № 6.2 (4 години)

Завдання № 1

Необхідно проаналізувати залежність для статистичних об’єктів «*Рівень тяжких та особливо тяжких злочинів»* та «*Зареєстрована кількість хворих на нарко-токсикоманію*» відповідно до даних таблиці 1.

Порядок виконання:

1. Створити на диску d:\ за допомогою програми Excel файл з назвою **Ваше прізвище_П.з. 6.2**.
2. Встановити **пароль** на файл.
3. Скопіювати таблицю 1 на перший аркуш робочої книги таким чином, щоб заголовок таблиці був розташований в клітинках A1, B1, C1, D1, E1, F1, а вся таблиця займала діапазон клітинок A1:F43.

Таблиця 1

Назва регіону	X_i Рівень тяжких та особливо тяжких злочинів на 100 тис. населення	Y_i Зареєстрована кількість хворих на нарко-токсикоманію на 100 тис. населення	X_i^2	Y_i^2	$X_i * Y_i$
АР Крим	395,23	215,89			
Вінницька	289,23	68,95			
Волинська	318,97	178,90			
Дніпропетровська	492,83	350,19			
Донецька	463,39	224,65			
Житомирська	286,19	123,65			
Закарпатська	163,41	18,01			
Запорізька	590,16	301,62			
Івано-Франківська	181,13	52,58			
Київська	322,60	77,78			
місто Київ	434,40	334,17			
Кіровоградська	323,25	235,00			
Луганська	454,16	188,55			
Львівська	303,82	39,72			
Миколаївська	389,17	222,57			
Одеська	396,82	325,97			
Полтавська	404,54	162,13			
Рівненська	242,40	108,07			
місто Севастополь	528,68	184,58			
Сумська	357,23	89,80			
Тернопільська	255,31	43,23			
Харківська	332,65	57,60			
Херсонська	352,20	229,09			
Хмельницька	319,49	155,22			
Черкаська	283,96	142,51			
Чернігівська	314,53	184,07			
Чернівецька	230,23	85,80			
КОРЕЛЯЦІЙНИЙ АНАЛІЗ					
Сума:					
Середнє:					
Квадрат середнього:					
Коефіцієнт кореляції Пірсона (r)					
Коефіцієнт детермінації ($\mathbf{r^2}$):					
Коефіцієнт кореляції згідно пакету «Аналіз даних» (r)					
РЕГРЕСІЙНИЙ АНАЛІЗ					
Параметри лінії тренду:	**Рівняння лінії тренду (регресії)**			**Коефіцієнт детермінації (r^2):**	
експоненціальна:					
лінійна:					
логарифмична:					
поліноміальна:					
степенева:					
ВИСНОВКИ:					

3. Заповнити поля синього кольору для стовпців X_i^2 , Y_i^2 , $X_i * Y_i$ за допомогою відповідних формул (*Допомога*: для знаходження X_i^2 в клітинці D2 можна використовувати формулу =B2^2 або =B2*B2).

4. Заповнити поля жовтого кольору для рядків 30 (Сума:), 31 (Середнє:) та 32 (Квадрат середнього:).

5. У рядку 33 підрахувати коефіцієнт кореляції Пірсона **(r)** за другою формулою:

$$r = r(X, Y) = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} = \frac{\sum_{i=1}^{n} x_i y_i - n\,\bar{x} \cdot \bar{y}}{\sqrt{(\sum_{i=1}^{n} x_i^2 - n\bar{x}^2)(\sum_{i=1}^{n} y_i^2 - n\bar{y}^2)}}.$$

Допомога:

1) $\sum_{i=1}^{27} X_i Y_i$ знаходиться в комірці F30;
2) $n = 27$;
3) $\bar{X}$ знаходиться в комірці B31;
4) $\bar{Y}$ знаходиться в комірці C31;
5) $\sum_{i=1}^{27} X_i^2$ знаходиться в комірці D30;
6) $\bar{X}^2$ знаходиться в комірці B32;
7) $\sum_{i=1}^{27} Y_i^2$ знаходиться в комірці E30;
8) $\bar{Y}^2$ знаходиться в комірці C32;
9) знаходження квадратного кореня: (вираз)^(1/2)

Тобто, скелет формули такий:

=(чисельник дробу)/(вираз у знаменнику під коренем)^(1/2)

6. У рядку 34 підрахувати коефіцієнт детермінації (**r^2**).

7. За допомогою пакету **Аналіз даних**, що входить до складу Microsoft Excel, обрахувати емпіричне значення коефіцієнту лінійної кореляції Пірсона між рівнем тяжких та особливо тяжких злочинів та зареєстрованою кількістю хворих на нарко-токсикоманію.

(***Примітка:*** Якщо в меню «Дані» відсутній пункт «Аналіз даних», то треба клацнути покажчиком миші по «Файл» -> «Інші» -> «Параметри» -> «Надбудови» -> «Перейти» -> «Доступні надбудови» та встановити прапорець «Пакет аналізу» і натиснути на кнопку «ОК»).

За допомогою «Дані» -> «Аналіз даних» -> «Кореляція» -> «ОК» відкрити вікно «**Кореляція»**. У вікні встановити вхідний інтервал **$B$1:$C$28**,

групування – **по стовпчикам**, встановити прапорець **Меткі в першому рядку** та перемикач **Новий робочий лист**.

На новому аркуші (**Лист 2**) з'явиться таблиця, в якій на перетині рядку *Зареєстрована кількість хворих на нарко-токсикоманію* та стовпчика *Рівень тяжких та особливо тяжких злочинів* знаходиться значення **коефіцієнту лінійної кореляції Пірсона**. Вставити його до рядку 35.

8. На аркуші, що містить таблицю з даними експериментів, виділити діапазон B2:C28. Побудувати діаграму Вставка -> Рекомендовані діаграми -> **Крапкова** (Точечна), що дозволяє порівнювати пари значень. Задайте розташування діаграми на тому ж аркуші, що і таблиця.

Привласніть назву діаграми «*Кореляційне поле*», назву осі X /категорій/ - «*Рівень тяжких та особливо тяжких злочинів*», назву осі У /значень/ - «*Зареєстрована кількість хворих на нарко-токсикоманію*».

9. Клацніть правою кнопкою миші по маркеру будь-якої точки з ряду даних Вашої діаграми. В контекстному меню, що з'явиться, виберіть пункт **Добавити лінію тренду**.

У вікні **Лінія тренду**, що відкрилося, виберіть у вкладці **Тип**: ***експоненціальна***, у вкладці **Параметри** встановіть прапорці: **показати рівняння на діаграмі** та **помістити на діаграму величину достовірності апроксимації /R^2/ -** коефіцієнт детермінації R^2. Закрийте вікно.

З діаграми скопіюйте отримані дані до комірок рядка 38 (якщо безпосередньо до цих комірок система відмовиться копіювати, то можна це зробити через копіювання в клітинки стовпчика G, а потім в потрібні клітинки). Після чого за допомогою клавіші **Delete** видаліть отриману лінію тренду.

10. Послідовно повторюйте пункт 9 для ліній тренду з типом: ***лінійна, логарифмічна, поліноміальна (ступінь 2), степенева***. Для кожного типу лінії скопіюйте отримані рівняння та значення коефіцієнту детермінації до полів рядків 39, 40, 41, 42, відповідно.

У якості остаточного варіанту лінії регресії виберіть лінію тренду, що має найбільший коефіцієнт детермінації. Цю лінію слід залишити на діаграмі «Кореляційне поле».

11. На підставі отриманих даних заповнити поле «Висновки» в рядку 43 щодо сили та напрямку залежності між означеними показниками, яка лінія тренду найкраще її описує.

Завдання № 2

Аналогічно до завдання 1 проаналізуйте залежність для статистичних об'єктів «*Рівень тяжких та особливо тяжких злочинів»* та «*Зареєстрована кількість хворих на алкоголізм»* відповідно до даних таблиці 2.

Таблиця 2

Назва регіону	X_i Рівень тяжких та особливо тяжких злочинів на 100 тис. населення	Y_i Зареєстрована кількість хворих на алкоголізм на 100 тис. населення	X_i^2	Y_i^2	$X_i * Y_i$
АР Крим	395,23	1163,52			
Вінницька	289,23	1348,32			
Волинська	318,97	1167,03			
Дніпропетровська	492,83	1308,32			
Донецька	463,39	1428,63			
Житомирська	286,19	1489,02			
Закарпатська	163,41	1432,37			
Запорізька	590,16	1402,10			
Івано-Франківська	181,13	1203,20			
Київська	322,60	1602,83			
місто Київ	434,40	764,27			
Кіровоградська	323,25	1556,30			
Луганська	454,16	1740,50			
Львівська	303,82	1266,35			
Миколаївська	389,17	783,05			
Одеська	396,82	1488,99			
Полтавська	404,54	1548,23			
Рівненська	242,40	1204,18			
місто Севастополь	528,68	954,53			
Сумська	357,23	1355,59			
Тернопільська	255,31	1182,91			
Харківська	332,65	1515,38			
Херсонська	352,20	1729,22			
Хмельницька	319,49	1816,19			
Черкаська	283,96	1441,52			
Чернігівська	314,53	1726,06			
Чернівецька	230,23	1209,91			
КОРЕЛЯЦІЙНИЙ АНАЛІЗ					
Сума:					
Середнє:					
Квадрат середнього:					
Коефіцієнт кореляції Пірсона (r)					
Коефіцієнт детермінації ($\mathbf{r^2}$):					
Коефіцієнт кореляції згідно пакету «Аналіз даних» (r)					
РЕГРЕСІЙНИЙ АНАЛІЗ					
Параметри лінії тренду:	**Рівняння лінії тренду (регресії)**			**Коефіцієнт детермінації (r^2):**	
експоненціальна:					
лінійна:					
логарифмічна:					
поліноміальна:					
степенева:					
ВИСНОВКИ:					

Завдання № 3

Стан злочинності в місті N за період 2014–2023 рр. характеризується такими даними:

Роки:									
2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Число зареєстрованих злочинів:									
990	848	905	945	950	1180	1155	1090	1014	996
Кількість населення:									
123800	123500	123300	122500	120400	118700	119300	117800	118000	116800

На основі цих даних на окремому аркуші побудуйте графік динаміки кількості злочинів на 1000 чоловік населення і на його основі зробіть прогноз кількості злочинів на 1000 чоловік населення на 2024 та 2025 роки.

Список використаних і рекомендованих джерел

1. Кудінов В. А., Пакриш О. Є., Смаглюк В. М., Хахановський В. Г. Інформаційні технології в правозастосовній діяльності : підручник / за заг. ред. В. А. Кудінова. Київ : Нац. акад. внутр. справ, 2018. 176 с.
2. Огірко О. І., Галайко Н. В. Теорія ймовірностей та математична статистика : навч. посіб. Львів : ЛьвДУВС, 2017. 292 с.
3. Шпігельхальтер Д. Мистецтво статистики. *Прийняття аргументованих рішень на основі даних – КМ-БУКС.* 2023. 384 с.
4. Виганяйло С. М. Правова статистика : навч. посіб. Суми, 2019. 145 с.

РОЗДІЛ VII
ОСНОВИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

7.1. Основні поняття у сфері кібербезпеки як складової національної безпеки держави

У світі поняття «безпека держави» стала однією з ключових категорій, адже після багатотисячної історії людства, яка постійно супроводжувалась кровопролитними війнами, проблема забезпечення безпеки громадян та їх держав завжди турбувала людство у процесі його цивілізаційного розвитку.

Національна безпека держави – це здатність країни своєчасно виявляти, запобігати і нейтралізувати реальні та потенційні загрози своїм національним інтересам, реалізація яких забезпечує її державний суверенітет, прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян. Національна безпека держави – це головний аспект її існування не тільки як суб'єкта міжнародного права, а і як захисника прав і свобод своїх громадян.

Законодавче визначення поняття «національна безпека України» наводиться у однойменному Законі Україні «Про Національну безпеку України», за яким під даним терміном розуміють «*захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз*».

Державна політика у сферах національної безпеки спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури України та на інші її напрями.

Забезпечення недоторканості та безпеки кордонів держави (в усіх їх вимірах) теж є важливим завданням забезпечення національної безпеки. Людство завжди прагнуло як найповніше опанувати всі доступні йому простори і включити їх до свого володіння. Після освоєння ще у доісторичні часи часток суші та води (перший та другий простір) людина завдяки розвитку авіаційних і ракетних технологій опанувала у XX сторіччі повітря й космос (третій і четвертий простори).

У XXI сторіччі людство масово освоює новий п'ятий простір – кіберпростір, винятковість якого пов'язана з тим, що він разом з космосом є простором, опанованим людиною, що практично позбавлений географічних обмежень.

Адже слово «кіберпростір» є сполученням двох слів «кібер» та «простір». Слово «кібер» походить від грецького «κυβερ» та означає «над». А ще «кібер» – це префікс, взятий від слова «кібернетика», що означає «наука про загальні закони одержання, зберігання, передавання та перетворення інформації у складних керуючих системах, пов'язаних з комп'ютерами». Згідно з одним з визначень, наданому у великому тлумачному словнику сучасної української мови, під поняттям «простір» розуміють вільний великий обшир, просторінь

або територію. Таким чином, буквально кіберпростір – це якась комп'ютерна надтериторія.

Поняття «кіберпростір» (англ. *Cyberspace*) вперше використано канадським письменником-фантастом Уільямом Гібсоном (англ. William Gibson) у 1982 р. в новелі «Пекучий Хром» («Burning Chrome»), а у 1984 р. у своєму романі «Нейромант» (англ. «Neuromancer») він використав його для позначення всієї сукупності інформації як світу штучної реальності, що міститься у всіх комп'ютерних мережах світу.

В офіційних документах уперше термін «кіберпростір» було використано (але не надано визначення) у так званій «Окінавській хартії глобального інформаційного суспільства», що була прийнята на 26-му саміті лідерів держав Великої вісімки (G8) в ході зустрічі в м. Наґо (острів Окінава, Японія) в липні 2000 року.

У рекомендації «Про розвиток та використання багатомовності та загальному доступі до кіберпростору», прийнятій на 32-й сесії Генеральної конференції ЮНЕСКО у 2003 році, кіберпростір визначається як віртуальний світ цифрової та електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою.

Перше офіційне визначення кіберпростору з точки зору військових операцій було дано військовими експертами Збройних сил США у «Настанові з інформаційних операцій» (Joint publication 3-13 «Information operations») 2006 року, де зазначалось, що кіберпростір – це сфера, в якій застосовуються різні радіоелектронні засоби (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління і наведення), що використовують широкий діапазон електромагнітного спектра частот для прийому, передачі, обробки, зберігання, перетворення й обміну інформацією, і пов'язана з ними інформаційна інфраструктура Збройних сил США.

А в 2018 році у «Настанові з кібероперацій» (Joint publication 3-12 «Cyberspace operations») Збройних сил США вже було визначено, що кіберпростір – це глобальний домен в інформаційному середовищі, що складається зі взаємозалежних мереж інфраструктури, інформаційних технологій і резидентних даних, включаючи Інтернет, комунікаційні мережі, комп'ютерні системи та вбудовані процесори та контролери. При чому зазначалось, що кіберпростір може бути описаний в термінах трьох взаємопов'язаних шарів: фізичної мережі, логічної (віртуальної) мережі, і окремих користувачів (кібер-персон).

У національному законодавстві визначення «кіберпростір» було надано у 2017 році в Законі України «Про основні засади забезпечення кібербезпеки України» наступним чином: «*Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних*».

Тобто кіберпростір – це простір, сформований електронними комунікаціями (інформаційно-комунікаційними системами, локальними комп'ютерами, локальними та глобальними мережами), у яких здійснюється виготовлення, зберігання, обробка, обмін та знищення інформації в електронному вигляді. З іншого боку, кіберпростір – це сукупність інформаційних відносин між користувачами електронних комунікацій (інформаційно-комунікаційних систем), які формуються за допомогою послуг (сервісів) цих систем.

Кіберпростір є віртуальним (тобто не реальною, а штучною дійсністю), так як він є простором, де циркулює інформація як результат віртуального спілкування різних спільнот людей – груп людей з близькими інтересами і стилем життя. Але створений він на базі фізично або реально працюючих комп'ютерів, модемів, кабелів, маршрутизаторів, серверів та іншого обладнання. Тобто кіберпростір є віртуальним світом, що генерується комп'ютерами, в який занурюється користувач у режимі реального часу.

Кіберпростір можна охарактеризувати трьома основними ознаками: 1) це інформаційний простір; 2) він є комунікативним середовищем віртуального спілкування; 3) він утворюється за допомогою електронних комунікацій (інформаційно-комунікаційних систем).

Кіберпростір можна розглядати як: 1) локальне середовище, у випадку функціонування засобу комп'ютерної техніки, який не під'єднано до мережі; та як розосереджене середовище, яке виникає в разі підключення засобу комп'ютерної техніки до 2) локальної або 3) глобальної мережі передачі даних (Інтернет).

Як і для любого іншого простору стан безпеки кіберпростору – це такі умови, в яких перебуває цей простір, коли дія зовнішніх і внутрішніх загроз не призводить до процесів, що вважаються негативними по відношенню до його стану.

Тобто безпека стосовно до кіберпростору означає безпечне функціонування як електронних комунікацій, що його сформували, так і самої інформації, що забезпечує інформаційні відносини в кіберпросторі.

Стан безпеки (захищеності) кіберпростору прийнято називати терміном «кібербезпека» (англ. *Cyber Security, Cybersecurity*).

Законодавче визначення в Україні цього терміну надано в Законі України «Про основні засади забезпечення кібербезпеки України»: «*Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі*».

Кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання кіберпростору, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний

вплив; негативні наслідки функціонування електронних комунікацій та інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Забезпечення кібербезпеки є одним із важливих пріоритетів у системі національної безпеки України. Адже XXI століття знаменується активним формуванням нового цифрового укладу розвитку технологій та ризиками, з якими стикається цивілізація внаслідок упровадження цих цифрових технологій. При чому одним з театрів воєнних дій та загроз національній безпеці держави стає кіберпростір, що сформований як раз за рахунок цих новітніх цифрових технологій.

Тому в Стратегії національної безпеки України, що затверджена Указом Президента України від 14 вересня 2020 року № 392/2020, зазначається, що одним із напрямів діяльності держави для забезпечення її національних інтересів і безпеки є «*завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації*».

Кібербезпека – це захищеність від загроз інформації, що циркулює в кіберпросторі, що пов'язані з загрозами трьом основним властивостям інформації, а саме:

– конфіденційності – забезпечення доступу до інформації тільки уповноваженим на це користувачам;

– цілісності – гарантування точності та повноти інформації;

– доступності – забезпечення того, що уповноважені користувачі на вимогу отримують доступ до інформації.

Загрози кібербезпеці, а отже, інформації, яка циркулює в електронних комунікаціях (інформаційно-комунікаційних системах), що створюють кіберпростір, залежать від багатьох наступних чинників, а саме:

– дій авторизованих користувачів;

– дій «хакерів»;

– дій шкідливого програмного забезпечення;

– дій «спаму»;

– дій «фішингу»;

– дій «природних загроз» тощо.

Розглянемо їх більш детально.

До категорії внутрішніх загроз, що можуть здійснюватися авторизованими користувачами інформаційно-комунікаційних систем, належать:

– цілеспрямована крадіжка даних з системи;

– навмисне знищення даних на робочих станціях інших користувачів або серверному обладнанні тощо;

– ненавмисне пошкодження даних через необережні дії.

Окрема категорія зовнішніх загроз може здійснюватися ***хакерами*** (від англ. *Hack* – розрубувати) – кваліфікованими IT-фахівцями, які своїми навмисними діями несуть загрозу кібербезпеці. Хакер – це зловмисник, котрий використовує великі комп'ютерні знання для здійснення несанкціонованих,

іноді шкідливих дій в комп'ютері – злом комп'ютерів, написання та поширення комп'ютерних вірусів тощо. Зараз є багато різних видів хакерів. Є хакери, що вламуються в систему з метою розширення свого професійного кругозору; інші – заради забави, не спричиняючи відчутної шкоди електронним мережам і комп'ютерам; але більшість – заради руйнування систем або отримання кримінального заробітку.

До зовнішніх загроз відносять також комп'ютерні віруси та інше шкідливе програмне забезпечення.

Шкідливе програмне забезпечення (ШПЗ, англ. *Malware* – скорочення від malicious – зловмисний і software – програмне забезпечення) – це зловмисна програма або код, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до комп'ютерних систем. Якщо комп'ютерний пристрій уражено ШПЗ, може відбуватися несанкціонований доступ, ураження даних або його блокування.

До таких програмних засобів належать комп'ютерні віруси, хробаки, троянці, руткіти, клавіатурні логери, дозвонювачі, шпигунські програмні засоби, здирницькі програми, шкідливі плаґіни та інше зловмисне програмне забезпечення.

Комп'ютерний вірус (англ. *Computer Virus*) – комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макровіруси. Можливі також комбінації цих типів (рис. 7.1). Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу.

Рис. 7.1. Типи комп'ютерних вірусів

Комп'ютерний хробак або черв'як – це програма, яка, як правило, розповсюджується автономно від одного комп'ютера до іншого, вибираючи та атакуючи комп'ютери в повністю автоматичному режимі (звичайний хробак), або потребують певних дій користувача для поширення, наприклад, відкриття інфікованого повідомлення в клієнті електронної пошти або запуску відповідної інфікованої програми. Головною особливістю комп'ютерного хробака є те, що він поширюється не тільки по всьому комп'ютеру-жертві, але й автоматично розсилає свої копії на інші компютери, наприклад електронною поштою (рис. 7.2).

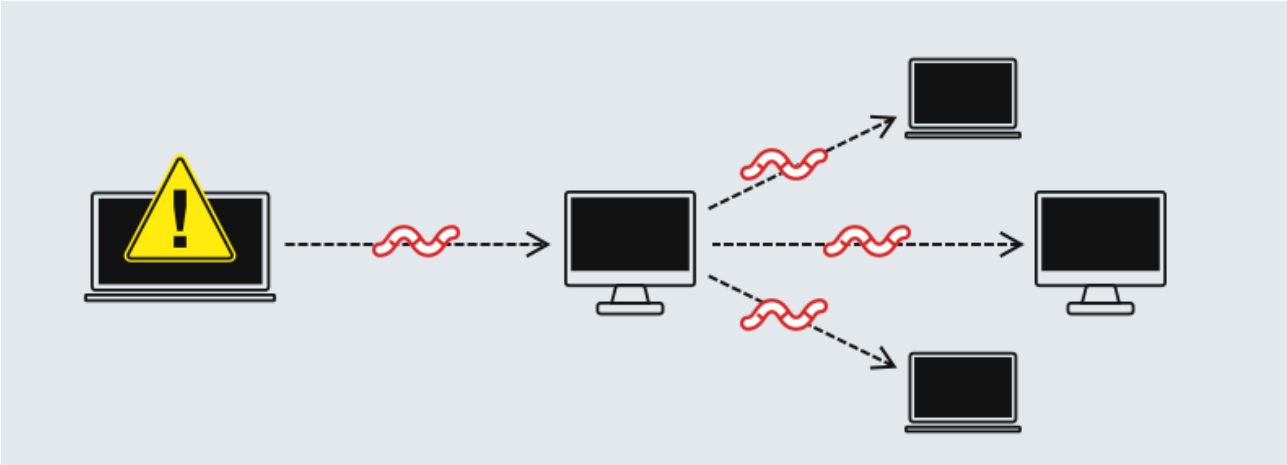


Рис. 7.2. Комп'ютерний хробак

Більшість поштових хробаків поширюються як один файл. Їм не потрібна окрема «інфекційна» частина, так як зазвичай користувач комп'ютера-жертви за допомогою поштового клієнта добровільно завантажує та запускає хробака.

Якщо код комп'ютерного хробака призначений на більше, ніж просте поширення хробака, його називають хробаком «корисного навантаження». Типові хробаки корисного навантаження можуть видаляти файли на хост-системі, шифрувати файли для отримання грошового викупу або копіювати дані, такі як паролі або конфіденційні документи. Найбільш поширене корисне навантаження для хробаків є встановлення у систему, так званих, бекдорів. Це дозволяє зловмиснику віддалено контролювати комп'ютером, створюючи «зомбі комп'ютер».

Хробаки можуть використовувати й інші різноманітні механізми («вектори») поширення. Хробаки майже завжди шкодять мережі, наприклад, споживаючи її пропускну здатність.

Троянські програми або «трояни» чи «троянці» (англ. *Trojan Horses, Trojans*) – різновид ШПЗ, яке не здатне поширюватися самостійно (відтворювати себе) на відміну від вірусів та хробаків, тому розповсюджується людьми. Вони надають сторонній доступ до комп'ютера для здійснення будь-яких дій з цим комп'ютером без попередження його власника або висилає за певною адресою зібрану з цього комп'ютера інформацію.

Дуже часто трояни потрапляють на комп'ютер разом з корисними програмами або популярними утилітами, маскуючись під них. При запуску троян встановлює себе в систему комп'ютера-жертви і потім стежить за нею, при цьому користувачеві не видається жодних повідомлень про ці дії. Як правило, троянська програма прикидається під що-небудь мирне і надзвичайно корисне (наприклад, нові версії популярних утиліт, ком'ютерних ігр тощо). Більш того, посилання на троянця може бути відсутнім в списку активних додатків або зливатися з ними.

Частина троянських програм обмежується тим, що відправляє знайдені на комп'ютері-жертві паролі електронною поштою людині, яка сконфігурувала цю програму (e-mail trojan). Однак найбільш небезпечні програми, що дозволяють отримати віддалений доступ до комп'ютера-жертви (BackDoor).

Так як троянські програми не можуть розповсюджуватися самостійно, тому вони використовують будь-яку з форм соціальної інженерії. Наприклад, коли користувач отримує електронного листа, то вкладення електронної пошти може бути замасковане (наприклад, звичайна форма для заповнення або писання на підроблений сайт). Троянська програма також може нести вірусне тіло – тоді запустив троянця комп'ютер перетворюється в осередок розповсюдженя «зарази».

Руткіт (англ. *Rootkit*) – програма або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі. Це такий спеціальний модуль ядра, який зламувач встановлює на зламаній ним комп'ютерній системі відразу після отримання прав суперкористувача до комп'ютера-жертви. Цей набір, як правило, включає всілякі утиліти для «замітання слідів» вторгнення в систему. Дозволяє зламувачеві закріпитися в зламаній системі і приховати сліди своєї діяльності шляхом приховування файлів, процесів, а також самої присутності руткіта в системі.

Назва «руткіт» походить з операційних систем Unix і Linux, де адміністратор облікового запису з найвищими привілеями називається «root», а група програм, які дозволяють доступ до пристрою на рівні адміністратора, називається «kit» («набір»).

Зазвичай руткіт забезпечує атакуючим доступ до зараженої системи комп'ютера навіть у разі перевстановлення операційної системи та повного видалення з нього даних, так як він завантажується до BIOS-прошивки на материнській платі, що надає йому можливість виконувати зловмисні дії вже при включенні комп'ютера, ще до завантаження операційної системи (ОС). При завантаженні ОС руткіт впроваджується в менеджер завантаження, що дозволяє йому модифікувати завантажувач ядра ОС. Наприклад, дістався до ядра ОС Windows, руткіт відключає систему PatchGuard, спрямовану саме на запобігання модифікації системних файлів Windows.

Сьогодні багато комп'ютерних вірусів, шпигунського програмного забезпечення, шифрувальників-вимагачів використовують його як окремий модуль, що надає можливість цьому ШПЗ максимально глибоко інтегруватися в систему зараженого комп'ютера.

Спам (від англ. *SPiced hAM*, тобто «пряна шинка») – це окрема категорія загроз, небажані повідомлення у будь-якій формі, які надсилаються у великій кількості, що заважають роботі. Найчастіше спам надсилається у формі комерційних електронних листів, надісланих на велику кількість адрес, а також через миттєві та текстові повідомлення, соціальні медіа або навіть голосову пошту. Один з найбільш поширених способів розповсюдження такого небажаного контенту – використання ботнет-мереж, великої кількості інфікованих «зомбі» пристроїв. Наприклад, це шахрайські «листи від нігерійського принца» (про надання $2000–$3000 для оформлення ймовірного спадку у кілька мільйонів доларів) або «спам технічної підтримки» (нав'язування оновлення програмного забезпечення, що призведе до зараження компютера, або нібито знайденого ШПЗ, що потребує зателефонувати в службу технічної підтримки) тощо.

Спам завжди здійснюється зловмисниками з єдиною кінцевою метою – заробляти гроші. Конкретний спосіб заробітку може бути різним – отримання комісії за кожен клік, за кожен перегляд або навіть за кожну установку якоїсь програми.

Іноді так звані «листи щастя» (повідомлення із закликом поширити його серед друзів, обіцяючи за це гроші/здоров'я/кохання чи навпаки невдачі), та Інтернет-розіграші також вважаються спамом, хоча вони й відрізняються тим, що найастіше надсилаюся з добрими намірами.

Фішинг (англ. *Phishing* – риболовля) – це вид соціальної інженерії (або соціотехніки), за якого кіберзлочинці втираються в довіру до користувачів і маскують електронні листи, текстові повідомлення або голосову пошту під надійне джерело, щоб переконати користувачів надати їм доступ до делікатної інформації (персональних даних, логинів, паролів, пін-кодів карт тощо) чи перейти за незнайомим посиланням. Під час таких атак зловмисники маскуються під відомий бренд, співробітників або друзів жертви та використовують психологічні прийоми, як-от відчуття нагальності, щоб маніпулювати людиною. Наприклад, зловмисник може замаскуватися під людину, яка шукає роботу, і обманом змусити роботодавця завантажити уражене резюме, або навпаки – змусити людину, яка шукає роботу, завантажити уражену рекламу від уявного роботодавця.

Загрозу кібербезпеці несе також так звана ***DoS-атака*** (англ. *Denial-of-Service attack*) – атака, що має на меті здійснити відмову в обслуговуванні авторизованих користувачів комп'ютерною системою. Принцип дії DoS-атаки полягає у відправці на сервер «жертви» великого потоку інформації, який по максимуму (наскільки дозволяють можливості хакера) завантажує обчислювальні ресурси процесора, оперативної пам'яті, забиває канали зв'язку або заповнює дисковий простір (рис. 7.3). Атакована машина не справляється з обробкою даних, що надходять і перестає відгукуватися на запити авторизованих користувачів.

Але найбільш небезпечна так звана ***DDoS-атака*** (англ. *Distributed Denial-of-Service attack*) – розподілена масована атака, для здійснення якої зловмисник

створює «зомбі-мережу» (ботнет), тобто групу «заражених» комп'ютерів, які знаходяться під його контролем (рис. 7.3). Контроль здійснюється за допомогою троянської програми, яка до пори до часу може ніяк себе не проявляти. При проведенні такої атаки хакер дає зараженим комп'ютерам команду посилати запити на сайт або сервер «жертви». Ввійти до складу такого ботнету може абсолютно будь-який комп'ютер або навіть смартфон. І його власник не буде про це навідь здогадуватися.

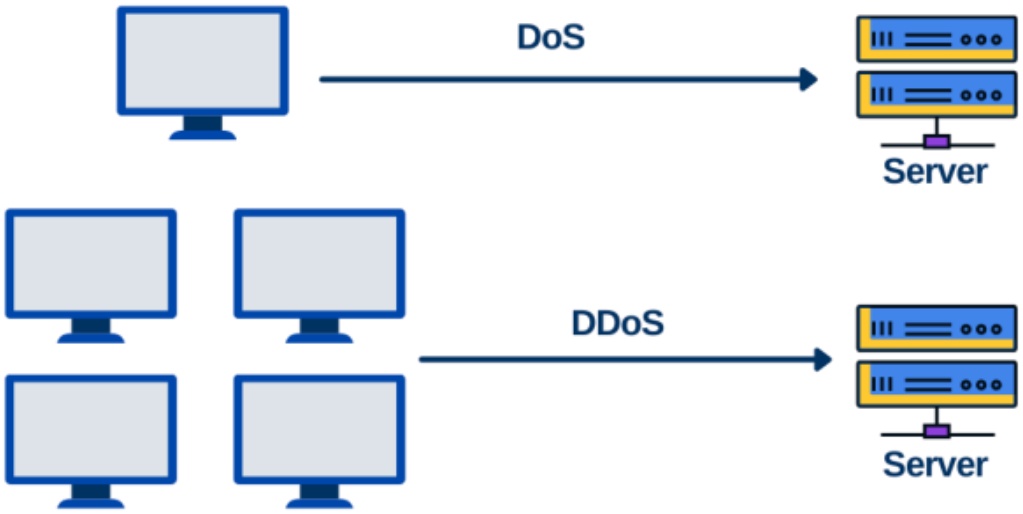


Рис. 7.3. DDoS-атака

У поєднанні з DoS- і DDoS-атаками хакери можуть знайти слабкі місця в системі та отримати конфіденційну інформацію, таємну переписку чи важливі документи, які потім продають на «чорному ринку» чи можуть вимагати за них викуп, доки служба безпеки намагається усунути наслідки DoS/DDoS-атаки.

Природні (об'єктивні) загрози кібербезпеці – загрози, викликані впливом на інформаційне середовище об'єктивних фізичних процесів (відмов та збоїв технічних засобів) або стихійних природних явищ (повенів, пожеж, ураганів тощо), що не залежать від волі людини.

Тобто наявні та потенційно можливі кіберзагрози створюють небезпеку життєво важливим національним інтересам держави у кіберпросторі, справляють негативний вплив на стан кібербезпеки України.

Окрему загрозу несуть кібератаки як спроби реалізації кіберзагрози.

Кібератака – це спрямовані (навмисні) дії в кіберпросторі з утручанням у роботу електронних комунікацій (інформаційно-комунікаційних систем) з метою порушення конфіденційності, цілісності, доступності, авторства інформації; або контролю, зміни в роботі, вимкнення, знищення обчислювальних механізмів чи інфраструктури електронних комунікацій, де циркулює інформація.

У Законі України «Про основні засади забезпечення кібербезпеки України» це поняття визначене наступним чином: «*кібератака – спрямовані (навмисні) дії в кіберпросторі, що становлять кіберзагрозу об'єкту (об'єктам)*

кіберзахисту, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні й технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що оброблюються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого і надійного функціонування, штатного режиму функціонування комунікаційних та/або технологічних систем; застосування комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту».

Розрізняють три основні типи кібератак за метою впливу на системи електронних комунікацій та їх компоненти, а саме:

– порушення конфіденційності – завданням атаки є отримання несанкціонованого доступу до інформації;

– порушення цілісності – передбачає несанкціоновану зміну в інформації чи програмних і технічних засобах системи;

– порушення доступності – метою атаки є дестабілізація роботи системи внаслідок створення перешкод для легітимних користувачів щодо доступу їх до системи або даних, необхідних для вирішення функціональних задач.

Розглянемо найбільш відомі (або резонансні) кібератаки на кіберпростір України під час російсько-української війни.

7.2. Огляд найбільш резонансних кібератак на кіберпростір України

У 2014 році, після анексії росією Криму та вторгнення на Донбас, гібридне протистояння між росією та Україною переросло у відкрите збройне протистояння – російсько-українську війну.

Після початку збройної агресії російської федерації (рф) проти України стали реєструвати значне зростання кількості кібератак на інформаційні системи в Україні. Зазвичай, кібератаки були націлені на приховане викрадення важливої інформації, ймовірніше для надання росії стратегічної переваги на полі бою. Жертвами російських кібератак ставали урядові установи України, оборонні структури, міжнародні та регіональні політичні організації, аналітичні центри, засоби масової інформації тощо.

З початком російсько-української війни стали з'являтись загони антиукраїнських хактивістів, які йменували себе «КіберБеркутом» та проукраїнська «Кіберсотня Майдану», «Анонімусами» з російською або українською «пропискою» тощо. Попри складності у визначенні ступеню співпраці хакерських угрупувань з державними органами, спираючись на зібрані докази можна стверджувати, що проросійські хакерські угрупування перебувають на території росії, і що їхня діяльність відбувається на користь кремлівського режиму.

Розглянемо деякі з найбільш резонансних кібератак на кіберпростір України у 2014–2023 роках.

Атаки на інформаційну систему ЦВК у травні 2014 року. Під час дочасних Президентських виборів в Україні, що проходили у травні 2014 року, було знешкоджено атаку на автоматизовану систему «Вибори».

21 травня 2014 року зловмисники з угрупування «КіберБеркут» здійснили успішну кібератаку на інформаційну систему «Вибори» Центральної виборчої комісії (ЦВК) України. Їм вдалось вивести з ладу ключові мережеві вузли корпоративної мережі та інші компоненти інформаційної системи ЦВК. Майже 20 годин поспіль програмне забезпечення, яке мало показувати поточні результати підрахунку голосів, не працювало як слід. В день виборів, 25 травня, за 12 хвилин до закриття виборчих дільниць (19:48), зловмисники спробували розмістити на серверах ЦВК так звану «картинку Яроша» (хибну інформацію про те, що перемогу отримав не Петро Порошенко, а Дмитро Ярош) – рис. 7.4.

Рис. 7.4

Увечері 25 травня на російських телеканалах анонсували новину про нібито виграш лідера українського національно-визвольного руху «Правий сектор» Дмитра Яроша на «президентських перегонах». З метою підтвердження цієї інформації на російському ТБ була продемонстровано «картинку Яроша». 25 травня, о 20:16:56 було зафіксоване перше звернення до вебсайту ЦВК виключно за IP-адресою внутрішнього вебсервера з вказівкою в GET-запиті повного шляху до картинки «result.jpg» з IP-адреси 195.230.85.129. Ця адреса входить до діапазону IP-адрес телеканалу російського каналу ОРТ.

В результаті «Перший канал» російського телебачення повідомив своїм глядачам про те, що найбільшу кількість голосів виборців в першому турі на виборах президента України набрав Дмитро Ярош як лідер «українського націського руху». Про це йшлося у випуску вечірніх новин, присвяченому позачерговим виборам президента України. Ведуча повідомила, що незважаючи на дані екзит-полів, які свідчать про перемогу Петра Порошенка в першому турі, на сайті ЦВК з’явилася так звана «картинка Яроша» (рис. 7.4). За

їхньою інформацією, Дмитро Ярош набрав 37,13 % голосів виборців, натомість за фаворита Петра Порошенка проголосувало лише 29,63 %.

Але росіяни не знали, що ця «картинка Яроша» була знайдена та знешкоджена фахівцями з кібербезпеки, які знаходились в ЦВК, ще до оприлюднення перших результатів виборів ЦВК.

Рано вранці наступного дня, 26 травня, сервери системи «Вибори», які приймали та обробляли дані про підрахунок голосів, зазнали також розподіленої DDoS-атаки, та були не доступні в проміжку між 1–3 годинами ранку.

Атаки на енергетичні компанії України у 2015–2016 роках. 23 грудня 2015 року сталась перша у світі підтверджена атака, спрямована на виведення з ладу енергосистеми: російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління в диспетчерській «Прикарпаттяобленерго», було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців Івано-Франківщіни залишались без світла протягом до шести годин. Атака відбувалась із використанням троянської програми BlackEnergy.

Водночас синхронних атак зазнали «Чернівціобленерго» та «Київобленерго», але з меншими наслідками. За інформацією одного з обленерго, підключення зловмисників до його інформаційних мереж відбувалося з підмереж глобальної мережі Internet, що належать провайдерам в російській федерації.

Загалом кібератака мала комплексний характер та складалась щонайменше з таких складових:

– попереднє зараження мереж за допомогою підроблених листів електронної пошти з використанням методів соціальної інженерії;

– захоплення управління АСДУ з виконанням операцій вимикань на підстанціях;

– виведення з ладу елементів IT-інфраструктури (джерела безперебійного живлення, модеми, RTU, комутатори);

– знищення інформації на серверах та робочих станціях (утилітою KillDisk);

– атака на телефонні номери кол-центрів, з метою відмови в обслуговуванні знеструмлених абонентів.

Загальний недовідпуск електроенергії склав 73 МВт·год (0.015 % від добового обсягу споживання України).

Наступна подібна кібератака сталась вночі з суботи на неділю, 17 на 18 грудня 2016 року: на підстанції «Північна» (с. Нові Петрівці Київської області) стався збій в автоматиці управління, через що споживачі північної частини правого берегу Києва та прилеглих районів області залишились без струму. Несправності були усунуті протягом 1 години 15 хвилин. Основною версією стала кібератака – зовнішнє втручання через мережі передачі даних.

Оператор підстанції, компанія «Укренерго» спочатку не стала підтверджувати кібератаку, проте залучені до розслідування фахівці з комп'ютерної безпеки підтвердили, що збій стався внаслідок кібератаки. Однак, нападники не стали завдавати істотної шкоди, натомість дана атака мала

послужити «демонстрацією сили». Як і у попередніх випадках, дана атака була частиною масштабнішої фішингової операції проти державних установ України.

Паралізування роботи фінансової системи України у грудні 2016 року. Починаючи з ночі з 5 на 6 грудня 2016 року хакерська атака на урядові сайти (Держказначейства України та інших) і на внутрішні мережі держорганів призвела до масштабних затримок бюджетних виплат на декілька днів.

«Крім пошкодження мережевого обладнання, установи втратили, за їхніми оцінками, 3 Терабайти інформації. Це колосальна цифра», – наголосив 16.12.2016 перший заступник директора Національного інституту стратегічних досліджень при Президенті України Олександр Власюк.

Для виведення з ладу серверів використовувався вірус KillDisk. Атака відбувалась із використанням троянської програми BlackEnergy, тої самої, що і в атаці на Прикарпаттяобленерго.

Масована хакерська атака у червні 2017 року. 27 червня 2017 року на підприємства різної форми власності та розміру, державні та недержавні установи була здійснена масштабна хакерська атака із використанням комп'ютерного хробака сімейства Petya. Новий зразок шкідливого програмного забезпечення отримав різні назви від різних дослідників, зокрема: Diskcoder.C, ExPetr, PetrWrap, Petya, або NotPetya та інші.

На думку дослідників фірми ESET, дана атака була здійснена угрупуванням TeleBots, яке має певні зв'язки з угрупуванням BlackEnergy-«Sandworm», відповідального за кібератаку на енергетичні підприємства України в грудні 2015 року. Попередні атаки цього угрупування були помічені ще в грудні 2016 року, коли проти фінансових компаній та об'єктів критичної інфраструктури України були здійснені атаки з використанням, в тому числі, варіанту програми KillDisk.

У проміжку між січнем та березнем 2017 року зловмисникам вдалось отримати несанкціонований доступ до комп'ютерної мережі українського розробника програмного забезпечення M.E.Doc та звідти отримати доступ до комп'ютерних мереж фінансових установ.

18 травня 2017 року розпочалась атака із використанням програми XData (також відома як Win32/Filecoder.AESNI.C), що мала здатність автоматичного поширення для впровадження в комп'ютери фінансових підрозділів установ України відповідного ШПЗ.

Початковим вектором атаки стала програма електронної фінансової звітності M.E.Doc, яка зв'язувала бухгалтерію цих установ з фіскальними органами України.

27 червня почалося масове поширення нової модифікації завірусованої програми M.E.Doc. На цей раз вірус здійснював зашифрування даних на комп'ютерах фінансових підрозділів, а через них і інших комп'ютерів, підключених до внутрішніх мереж установ. За відновлення доступу до даних пропонувалось відправити 300 доларів в біткоїнах на відповідні адреси.

Атака була в основному спрямована проти України, на яку припало 75 % всіх постраждалих від атаки комп'ютерів. Атаці піддалися енергетичні

компанії, українські банки, Аеропорт Харкова, Чорнобильська АЕС, урядові сайти, київський метрополітен. Пізніше стали з'являтися повідомлення про цю хакерську атаку на російські банки, компанії Хоум Кредит, Роснафта і Башнафта. Також повідомлення про зараження стали надходити з Італії, Ізраїлю, Сербії, Угорщини, Румунії, Польщі, Аргентини, Чехії, Німеччини, Великої Британії, США, Данії, Нідерландів, Іспанії, Індії, Франції та Естонії.

Жертвами атаки стали 64 держави й більше ніж 12,5 тис. комп'ютерів, збитки у світі оцінили в $8 млрд.

За офіційно не підтвердженими даними, ще в листопаді 2017 року ЦРУ дійшло остаточного висновку, що за атаками із використанням NotPetya стоять відповідні підрозділи під управлінням ГРУ ГШ рф.

Bad Rabbit (жовтень 2017). У жовтні 2017 року сталась доволі масова атака вірусом-хробаком BadRabbit. Спочатку зараження жертв відбувалось через низку скомпрометованих вебсайтів. Дослідники вважають, що за цим вірусом можуть стояти розробники вірусу NotPetya. Дещо згодом на той час голова кіберполіції України Сергій Демедюк заявив, що атака із застосуванням вірусу Bad Rabbit послужила прикриттям для набагато витонченішої атаки на підприємства-користувачів російських програм сімейства 1С.

Справжньою метою атаки було отримання несанкційованого доступу до конфіденційних та фінансових даних. Атака хробаком була лише яскравим прикриттям для відволікання уваги.

Масовані кібератаки на інформаційні ресурси України у 2022 році. В ніч на 14 січня українські урядові сайти зазнали масованої кібератаки. Хакерська атака зачепила близько 70 сайтів державних органів України. Зокрема, не працювали сайти: Урядовий портал; Міністерства освіти та науки; Міністерства закордонних справ України; Міністерства у справах ветеранів; Міністерства енергетики; Державної служби з надзвичайних ситуацій; Міністерства молоді та спорту; Державного казначейства України; Міністерства розвитку громад та територій; Міністерства екології; Міністерства аграрної політики та продовольства; Державної інспекції ядерного регулювання. Крім того, не працювали портал Судова влада України, Єдиний реєстр судових рішень, сайт Окружного адміносуду, розшукові обліки МВС тощо. Вранці були також проблеми з доступом до порталу «Дія».

На деяких сайтах зранку з'явилося відповідне повідомлення українською, російською та польською мовами, що було підготовлене начебто від імені польських хакактивістів (рис. 7.5). До того ж, як пишуть деякі польські ЗМІ (наприклад, Polskie Radio 24 та Rzeczpospolita), текст було написано з граматичними помилками. Тобто росіяни зімітували атаку від імені польських хакерів.

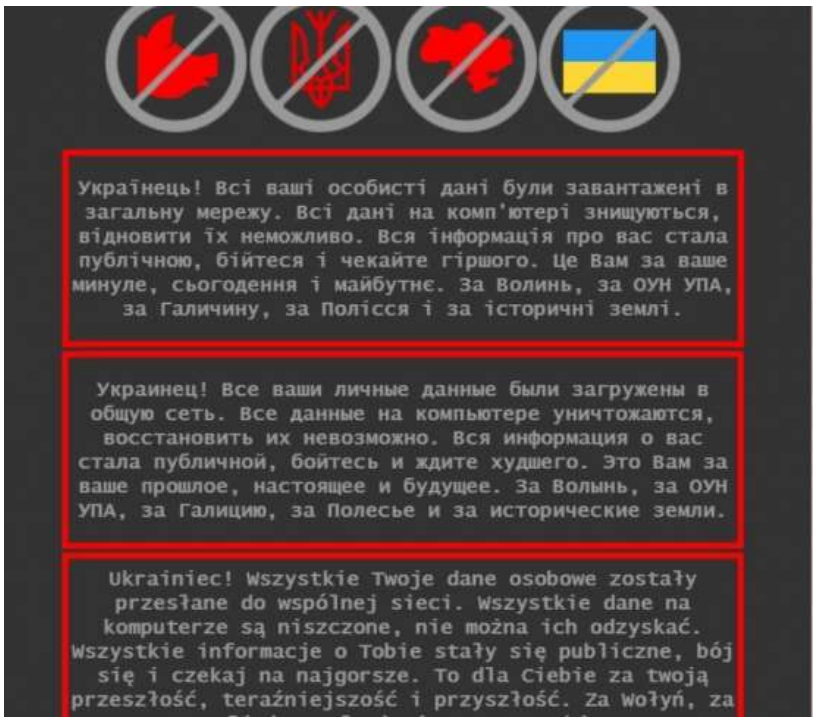


Рис. 7.5

Ця атака хакерів була найпотужнішою за останні чотири роки – щонайменше за охопленням державних вебресурсів. У той же час українські компетентні організації запевнили, що контент сайтів не було змінено та витоку персональних даних не сталося.

15 лютого 2022 р. російські хакери розпочали потужнішу DDoS-атаку, яка, серед іншого, була спрямована на фінансовий сектор (на 15 банківських сайтів, сайтів з доменом gov.ua, також сайтів Міноборони, Збройних сил та Міністерства з питань реінтеграції тимчасово окупованих територій, що тривала близько 5 годин).

23 лютого 2022 р., напередодні масового російського вторгнення в Україну, було повторно атаковано низку сайтів державних та банківських установ, енергооб'єктів. Пік кібератак проти енергетичного сектора припав на момент підключення української електромережі до європейської ENTSO-E (тобто в ніч на 23-24 лютого). Вночі та вранці 24 лютого 2022 року, сайт Київської ОДА був атакований, деякі ресурси були відключенні для збереження даних. На сайтах i.ua та meta.ua були виявлені масові e-mail листи з фішинговими посиланнями на приватні адреси українських військових та пов'язаних осіб. Під час деяких атак на Укренерго російські хакери навіть не намагались ховати своє походження і використовували російські IP-адреси для сканування мережі державного енергетичного оператора.

Грудень 2022 року – розсилання електронних листів з темою «Як розпізнати дрон-камікадзе», начебто, від імені Державної служби України з надзвичайних ситуацій. Для цього ще 08.11.2022 було зареєстровано відповідне підставне доменне ім'я dsns.com.ua, з адреси електронної пошти якої надсилалися ці листи.

У вкладенні до листа знаходиться RAR-архів «shahed-136.rar», що містить PPSX-документ «shahed.ppsx», який, у свою чергу, містить VBScript-код, призначений для створення запланованого завдання, а також дешифрування, створення на ЕОМ та запуску PowerShell-скрипта. Основним функціоналом якого є збір інформації про ЕОМ (ім'я хоста, ім'я користувача, розрядність, версія ОС, значення змінних середовища), запуск EXE/DLL файлів, відображення списку файлів та їх вивантаження, а також створення та ексфільтрація знімків екрану

У грудні 2022 року небезпечні листи надходили також начебто від імені головного органу в країні у сфері кіберзахисту – Держспецзв'язку (CERT-UA), – з темою «Увага! Шкідливе програмне забезпечення» та додаток з архівом «ESET_scanner.rar», що містив файл «ESET Online Scanner.exe» з начебто сканером вразливостей від фірми ESET. У випадку запуску цій файл імітує сканування комп'ютера на предмет виявлення та знешкодження вірусів та ШПЗ. Але після натискання на кнопки «Stop» і «OK» на комп'ютер жертви буде завантажено та виконано інший файл, що призведе до ураження пристрою шкідливою програмою.

Аналогічні фішинг-атаки були у 2022 році здійснені і від імені інших державних органів України. Наприклад, у лютому начебто від імені СБУ надходили електронні листи до організацій та установ з проханням надати дані щодо планів евакуації цих установ шляхом заповнення надісланих начебто від СБУ відповідних типових файлів-форм. Таким чином країна-агресор намагається встановити вірусне програмне забезпечення на комп'ютери українців та зібрати конфіденційну інформацію.

Всього у 2022 році від початку повномасштабного воєнного вторгнення росії з 24 лютого і до кінця 2022 року урядова команда реагування на комп'ютерні надзвичайні події CERT-UA опрацювала 2194 кіберінцидентів.

Найчастіше ворожі хакери атакували державний сектор: на нього припадає близько чверті всіх досліджених випадків. Під особливою увагою російських хакерів залишався також енергетичний сектор. Також під постійним прицілом – компанії, що є постачальниками послуг, апаратного і програмного забезпечення для енергокомпаній. Окрім того, ворожі хакери активно атакували логістичний, телекомунікаційний, оборонний сектори тощо.

У 2022 році CERT-UA відстежила зловмисну активність понад 85 хакерських груп, більшість з яких пов'язані з Росією. 90% хакерських угруповань РФ належать до силових структур і узгоджують дії з воєнним командуванням країни-агресора. Серед них найбільш активними є угрупування:

– ARMAGEDDON/GAMAREDON/PRIMITIVE BEAR (ФСБ рф, активність відслідковується за ідентифікатором UAC-0010);

– SANDWORM (ГУ ГШ ЗС рф (ГРУ), активність відслідковується за ідентифікатором UAC-0082);

– APT28/FANCY BEAR (ГУ ГШ ЗС рф (ГРУ), активність відслідковується за ідентифікатором UAC-0028);

– APT29/COZY BEAR (СЗР рф, активність відслідковується за ідентифікатором UAC-0029);

– UNC1151/ GHOSTWRITER (Міністерство оборони рб, активність відслідковується за ідентифікатором UAC-0051);

– XAKNET, KILLNET, Z-TEAM, CYBERARMYOFRUSSIA_REBORN (проросійські кібертерористи, активність відслідковується за ідентифікаторами UAC-0106, UAC-0108, UAC-0109, UAC-0107 відповідно).

Приклади деяких кібератак у 2023 році. ***Січень 2023 року – кібератака на інформаційну агенцію «Укрінформ»***. 17 січня в російському телеграм-каналі «CyberArmyofRussia_Reborn» було наголошено про злом комп'ютерної системи Українського національного інформаційного агентства «Укрінформ». Але CERT-UA було з'ясовано, що зловмисниками здійснено невдалу спробу порушення штатного режиму роботи комп'ютерів з використанням шкідливих програм-деструкторів CaddyWiper та ZeroWipe, а також легітимної утиліти SDelete (запуск якої передбачалося здійснити за допомогою «news.bat»). При цьому, з метою централізованого розповсюдження шкідливих програм, створено об'єкт групової політики, що, у свою чергу, забезпечував створення відповідних запланованих завдань.

CERT-UA з'ясовано, що етап розвідки «Укрінформ» було проведено не пізніше 07.12.2022. Встановлено, що завершальну стадію кібератаки ініційовано 17.01.2023, проте, вона мала лише частковий успіх, зокрема, у відношенні декількох систем зберігання даних.

Можливе стверджувати, що кібератаку здійснено групою UAC-0082 (Sandworm), діяльність якої асоціюється з ГУ ГШ ЗС рф.

Січень 2023 року – імітація справжнього сайту МЗС України. CERT-UA було виявлено розміщення в мережі Інтернет вебсторінки, що імітує офіційний вебресурс Міністерства закордонних справ (МЗС) України, на якому пропонується завантажити програмне забезпечення для «виявлення заражених комп'ютерів», перед тим як оглянути цей сайт.

У разі переходу за посиланням на комп'ютер буде завантажено bat-файл «Protector.bat», відкриття якого призведе до завантаження та запуску на комп'ютері PowerShell-скриптів, один з яких забезпечить рекурсивний пошук файлів з розширеннями: .edb, .ems, .eme, .emz, .key, .pem, .ovpn, .bat, .cer, .p12, .cfg, .log, .txt, .pdf, .doc, .docx, .xls, .xlsx, .rdg в каталозі робочого столу, створення знімків екрану та подальшу ексфільтрацію цих даних.

Масовані фішінг-атаки у лютому 2023 року. Масове розповсюдження електронних листів:

– начебто від імені Апарату РНБОУ з темою «RE: Критичне оновлення безпеки» та додатком у вигляді RAR-архіву «KB5017371 оновлення системи безпеки.rar». Згаданий файл містить зображення-приманку «інструкція Важливо прочитати.jpg» та спліт-архів, в якому знаходиться виконуваний файл «KB5017371.exe». Запуск останнього призведе не до оновлення системи безпеки операційної системи, а до встановлення на комп'ютері жертви програми для віддаленого управління Remote Utilities;

– начебто від АТ «Укртелеком» з темою «урядова претензія за Вашим особовим рахунком # 7192206443063763 от: 06.02.2023» та додатком у вигляді RAR-архіву «судовий лист, інформація щодо заборгування.rar», розархівація якого призведе до встановлення на комп'ютері жертви програми Remcos для віддаленого контролю та спостереження;

– начебто від імені Печерського районного суду міста Києва з темою «Печерський районний суд міста Києва» та додатком у вигляді RAR-архіву «електронний судовий запит № 7836071.rar», розархівація якого призведе до встановлення на комп'ютері програми для віддаленого контролю та спостереження Remcos для здобуття автентифікаційних даних та подальшого розвитку атаки вже на локальну мережу, до якої підключений цей комп'ютер.

23 лютого 2023 року – масована кібератака, спрямована на порушення цілісності та доступності державних інформаційних ресурсів. 23 лютого, з 16 години на Україну розпочалася чергова масова DDoS-атака. Станом на 16:30 не відкривалися сайти: Кабінету міністрів, Верховної Ради, Міністерства закордонних справ України. Також із труднощами працював сайт Служби безпеки України. Всього було виявлено проблеми у роботі десятка інших сайтів органів державної влади та місцевого самоврядування.

17 березня 2023 року відбувалася масована кібератака на державні інформаційні ресурси України. DDoS-атаки відбувалися в тому числі на Єдині та Державні реєстри, сайти Міністерства юстиції України, ДП «Національні інформаційні системи» тощо. Користувачі спостерігали проблеми з отриманням доступу до цих сайтів через великий обсяг трафіку під час DDoS-атаки.

Головними об'єктами DDoS-атак у першому півріччі 2023 року в Україні стали: держава, фінансова сфера, медіа, IT, телеком та логістика. Найбільше атак було зафіксовано на державний сектор, а кількість атак на логістичну галузь зросла на 900 %.

Кібератаки жовтня 2023 року. В період від 2 по 6 жовтня 2023 року в України здійснили щонайменше чотири хвилі кібератак. Атаки були здійснені угрупуванням UAC-0006 із застосуванням ШПЗ SmokeLoader. Типовий зловмисний задум угрупування UAC-0006 полягав в ураженні в основному бухгалтерських комп'ютерів, за допомогою яких здійснюється забезпечення фінансової діяльності, а також викраденні автентифікаційних даних та створенні несанкціонованих платежів.

12 грудня 2023 року стався масштабний збій у роботі найбільшого мобільного оператора України «Київстар». Збій стався вранці 12 грудня. Користувачі не мали доступу до послуг мобільного зв'язку, мобільного та домашнього інтернету. Проблеми виникли в користувачів у різних регіонах України. Через збій в роботі оператора «Київстар» також тимчасово не працювала система оповіщення про тривоги в деяких населених пунктах України.

Кібератака на Київстар була за двома напрямами: зруйнувати віртуальну інфраструктуру компанії (стерти сукупність програмного забезпечення, що створює віртуальні версії комп'ютерів мережі) та перепрограмувати програмне забезпечення більш як на 50 тис. базових станціях (БС) оператора. Основний

напрям атаки був на віртуальну інфраструктуру і він виявився успішним. Хоч мережу повністю вимкнули, проте хакери змогли знищили лише 40 % інфраструктури. Інший вектор атаки, що пов'язаний з перепрограмуванням БС, провалився.

За матеріалами слідства стало зрозуміло, що проникнення хакерів у систему «Київстар» сталося ще у травні 2022 року з акаунту третьої сторони, тобто однієї з фірм-партнерів, щоб отримати максимальний рівень доступу до мережі, що дозволило мати важливу інформацію та за потреби дати команду на знищення відповідного програмного забезпечення.

Відповідальність за атаку на «Київстар» взяли російські хакери з групи «Солнцепьок», яка пов'язана з елітними хакерами з колективу SANDWORM, що підпорядковується російським силовикам з ГРУ.

Всього, упродовж 2023 року українські аналітики з безпеки CERT-UA зафіксували та обробили на 62,5 % більше кіберінцидентів, ніж у 2022 році. Так, на українські портали було здійснено 2543 кібератаки. За даними CERT-UA, 347 кібератак було зафіксовано на уряд та урядові організації, 276 – на місцеві органи влади, 175 – на організації у секторі безпеки та оборони, 127 – комерційні організації. Ще 92 рази атакували енергетичний сектор, 81 – телеком, 38 – освітні установи, 32 – транспортна галузь, 30 – фінансовий сектор, 25 – IT-сектор, 15 – ЗМІ, 12 – медичні установи.

Таким чином, підводячи підсумки цього питання, можна стверджувати, що починаючи з 2014 року кіберпростір України став одним з активних театрів воєнних дій.

Російсько-українська війна у кіберпросторі перейшла із скритого стану у відкрите збройне протистояння з використанням новітніх цифрових технологій та методів, де проросійські хакерські угрупування та спеціальні військові підрозділи московії ведуть активну кібервійну проти України.

Тому Україна має бути готова до продовження та можливої активізації ворожих дій у кіберпросторі і забезпечити кібербезпеку держави за рахунок створення та вдосконалення відповідних заходів, структур та систем у цій сфері.

7.3. Сучасна система забезпечення кібербезпеки в Україні. Роль Національної поліції в забезпеченні кібербезпеки

Існуюча в Україні система забезпечення кібербезпеки. На даний час існуюча в Україні система забезпечення кібербезпеки визначена в таких основних нормативно-правових актах, як:

1. Закон України від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України».

2. Стратегія національної безпеки України : Затверджена Указом Президента України від 14 вересня 2020 року № 392/2020.

3. Стратегія кібербезпеки України : Затверджена Указом Президента України від 26 серпня 2021 року № 447/2021.

Відповідно до них правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Національна система кібербезпеки в Україні є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Координація діяльності в Україні у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України (РНБОУ).

Адже РНБОУ відповідно до ст. 107 Конституції України є координаційним органом з питань національної безпеки і оборони при Президентові України, координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони, до якої відносяться питання забезпечення кібербезпеки.

Для безпосереднього здійснення РНБОУ координації діяльності у сфері кібербезпеки у складі РНБОУ створений і працює відповідний Національний координаційний центр кібербезпеки (НКЦК або Центр). Він є робочим органом РНБОУ і здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

Керівником НКЦК за посадою є Секретар РНБОУ, а секретарем – керівник структурного підрозділу Апарату РНБОУ, до відання якого віднесені питання кібербезпеки – Служби інформаційної безпеки та кібербезпеки Апарату РНБОУ.

Членами Центру, які беруть участь у його засіданнях, є представники (перші заступники або заступники) суб'єктів сектору безпеки і оборони України у сфері кібербезпеки, до відання яких належать питання кібербезпеки: Міністра оборони України, начальника Генерального штабу Збройних Сил України, Голови Служби безпеки України, Голови Служби зовнішньої розвідки України, Голови Національної поліції України, Голови Національного банку України (за згодою), начальник Головного управління розвідки Міністерства оборони України, начальник Управління розвідки Адміністрації Державної

прикордонної служби України та Голова Державної служби спеціального зв'язку та захисту інформації України.

Для забезпечення безпосередньої повсякденної роботи Центру залучені інші представники зазначених вище державних структур. Також до роботи НКЦК залучено фахівців з приватного сектору, які спеціалізуються на кіберзахисті.

Серед основних завдань Центру: аналіз стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам; стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-комунікаційних системах тощо.

Центр прогнозує та виявляє потенційні та реальні загрози у сфері кібербезпеки України, узагальнює міжнародний досвід у сфері забезпечення кібербезпеки; оперативне, інформаційно-аналітичне забезпечення РНБО з питань кібербезпеки. Центр бере участь в організації і проведенні міжнаціональних і міжвідомчих кібернавчань та тренінгів, розробляє відповідні методичні документи і рекомендації.

НКЦК має право запитувати та одержувати від органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій статистичні дані, інформацію, довідкові та інші матеріали, необхідні для вирішення питань, що належать до його компетенції; користуватися інформаційними базами даних державних органів, державними, в тому числі урядовими, системами зв'язку і комунікацій, мережами спеціального зв'язку та іншими технічними засобами тощо.

Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).

Об'єктами кібербезпеки в Україні є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

А об’єктами кіберзахисту є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об’єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Суб’єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об’єктів критичної інфраструктури;

8) суб’єкти господарювання, громадяни України та об’єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов’язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Суб’єкти забезпечення кібербезпеки у межах своєї компетенції:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Основними суб’єктами національної системи кібербезпеки постійної готовності в Україні є Державна служба спеціального зв’язку та захисту інформації України, Служба безпеки України, Національна поліція України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України (рис. 7.6).

Рис. 7.6. Національна система кібербезпеки

Відповідно до Конституції і законів України вони виконують в установленому порядку такі основні завдання.

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної комунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту та Центру

активної протидії агресії у кіберпросторі, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Державний центр кіберзахисту, який функціонує у складі Держспецзв'язку, забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

Завданнями урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (англ. *Computer Emergency Response Team of Ukraine*) є:

– накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

– надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

– підготовка та розміщення на своєму офіційному вебсайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

– взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

– взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

– взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

– опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

– сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-

розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки.

Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану.

Розвідувальні органи України (Служба зовнішньої розвідки України, Головне управління розвідки МО України, Управління розвідки Адміністрації Державної прикордонної служби України) здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

Національний банк України (НБУ) визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює НБУ, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює центр кіберзахисту НБУ, забезпечує функціонування системи кіберзахисту для банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює НБУ, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює НБУ, операторах платіжних систем та/або учасниках платіжних систем, технологічних операторах платіжних послуг.

Роль Національної поліції в забезпеченні кібербезпеки України. Національна поліція України (НПУ) забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі.

Головним завданням НПУ є запобігання, виявлення, припинення та розкриття кіберзлочинів (або комп'ютерних злочинів) – суспільно небезпечних винних діянь у кіберпросторі та/або з їх використанням, відповідальність за які

передбачена законом України про кримінальну відповідальність та/або які визнано злочинами міжнародними договорами України.

Кіберзлочини – це кримінальні правопорушення, вчинені в кіберпросторі за допомогою спеціальних пристроїв (комп'ютерів, смартфонів, планшетів, терміналів та інших), автоматизованих систем, комп'ютерних мереж чи систем електронних комунікацій, та пов'язані з протиправним, несанкціонованим створенням, зберіганням, обробкою, підробкою, блокуванням, знищенням об'єктів інформаційної інфраструктури.

До кіберзлочинів відносять:

– правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, зокрема:

– незаконний доступ, наприклад, шляхом злому, обману та іншими засобами;

– нелегальне перехоплення комп'ютерних даних;

– втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

– втручання у систему, включаючи умисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру;

– зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу метою здійснення кіберзлочинів;

– правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів;

– правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія;

– правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.

Для забезпечення виконання завдань з кібербезпеки, що віднесені до повноважень НПУ, у її складі створена кіберполіція (Департамент кіберполіції Національної поліції України) – міжрегіональний територіальний орган НПУ, який входить до структури кримінальної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність.

Кіберполіція з'явилася у складі НПУ не на пустому місці.

27 липня 2009 року у складі Департаменту боротьби із злочинами, пов'язаними з торгівлею людьми, Міністерства внутрішніх справ України було створено відділ боротьби з кіберзлочинністю. А наприкінці 2012 року на його базі у складі кримінальної міліції Міністерства внутрішніх справ України було створено самостійний структурний підрозділ – Управління боротьби з кіберзлочинністю.

Вже при реформуванні в Україні міліції та створенні у вересні 2015 року Національної поліції, 13 жовтня того року був створений Департамент кіберполіції, як структурний підрозділ НПУ. Метою створення кіберполіції було реформування та розвиток відповідних підрозділів МВС України, що забезпечило підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, залучених у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

Спеціалізується кіберполіція на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), комунікаційних та комп'ютерних інтернет-мереж і систем.

Основними завданнями кіберполіції є:

– реалізація державної політики у сфері протидії кіберзлочинності;

– завчасне інформування населення про появу новітніх кіберзлочинів;

– впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини;

– реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів;

– участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності;

– участь у міжнародних операціях та співпраця в режимі реального часу. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу;

– протидія кіберзлочинам.

Протидія кіберполіцією кіберзлочинам полягає в наступних їх проявам:

– у сфері використання платіжних систем: скімінг (шимінг) – незаконне копіювання вмісту треків магнітної смуги (чипів) банківських карток; кеш-трепінг – викрадення готівки з банкомата шляхом установлення на шатер банкомата спеціальної накладки утримувача; кардинґ – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її власником; несанкціоноване списання коштів із банківських рахунків за допомогою систем дистанційного банківського обслуговування;

– у сфері електронної комерції та господарської діяльності: фітинг – виманювання в користувачів Інтернету їхніх логінів та паролів до електронних гаманців, сервісів онлайн-аукціонів, переказування або обміну валюти тощо; онлайн-шахрайство – заволодіння коштами громадян через інтернет-магазини, сайти та комунікаційні засоби зв'язку;

– у сфері інтелектуальної власності: піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті; кардшарінг – надання незаконного доступу до перегляду супутникового та кабельного телебачення;

– у сфері інформаційної безпеки: соціальна інженерія – технологія управління людьми в Інтернет-просторі; шкідливе програмне забезпечення –

створення та розповсюдження вірусів і шкідливого програмного забезпечення; протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства; рефайлінг – незаконна підміна телефонного трафіка.

В період дії воєнного стану, що був введений в Україні в 2022 році через російську агресію, кіберполіція у рамках своїх можливостей і спільних військових директив здійснює також інформаційний супротив, волонтерську діяльність, технічний супровід відновлення тимчасово окупованих територій, а також забезпечує безпеку та розслідування атак на державні інформаційні ресурси України, що стали мішенню проросійських хакерських груп тощо.

Підводячи підсумки, можна зробити наступні **висновки**:

1. Забезпечення кібербезпеки стає одним із головних пріоритетів із забезпечення національної безпеки України. Адже одним з театрів воєнних дій в наш час стає кіберпростір, що сформований за рахунок цих новітніх цифрових технологій.

2. Війна у кіберпросторі перейшла у наш час із скритого стану у відкрите збройне протистояння з використанням новітніх цифрових технологій та методів. Починаючи з 2014 року проросійські хакерські угрупування та спеціальні військові підрозділи московії ведуть активну кібервійну проти України.

3. Існують три рівня забезпечення кібербезпеки:

– кібербезпека на рівні держави – це формування та реалізація політики, фінансування заходів та міжнародна співпраця в цій сфері;

– кібербезпека на рівні об’єктів – це впровадження комплексних систем захисту інформації в системи електронних комунікацій, що формують кіберпростір;

– кібербезпека на рівні користувачів – це їх особиста кібергігієна, що полягає в заходах безпеки, розроблених для захисту комп’ютерних пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації.

Питання для самоконтролю

1. За рахунок чого створюється кіберпростір? Чому він є віртуальним?
2. В якому нормативно-правовому документі України наведено визначення поняття «кібербезпека»?
3. Яким властивостям інформації загрожують інциденти, що створюються в кіберпросторі та пов’язані з кібербезпекою?
4. Що таке фішінг як різновид кібератаки? В чому він полягає?
5. Яким державним органом в Україні здійснюється координація діяльності суб’єктів забезпечення кібербезпеки постійної готовності?
6. Які державні органи України є основними суб’єктами забезпечення кібербезпеки постійної готовності?
7. Які повноваження у сфері забезпечення кібербезпеки покладено законодавством України на Національну поліцію України?

8. В чому полягає забезпечення кібербезпеки на рівні держави?

9. В чому полягає забезпечення кібербезпеки на рівні об’єктів інформаційної діяльності?

10. В чому полягає забезпечення кібербезпеки на рівні користувачів комп’ютерної техніки?

Практичні завдання до розділу VII

Практичне заняття № 5.1. Блокчейн технологія захисту інформації.

Мета заняття: ознайомитись з технологією блокчейн та процесом майнінгу криптовалюти біткоін шляхом їх моделювання (засобами ОС Ubuntu).

Порядок виконання:

Завдання 1. Створити блокчейн-ланцюжок блоків, який містить інформацію щодо певних платіжних транзакцій, та перевірити його цілісність.

Завантажити з попередньо підготовленої флеш-памяті операційну систему Linux (ОС Ubuntu).

Зайти в домашню теку home/me (замість me може бути інше ім’я, пов’язане з конкретним користувачем) і створити в ній підтеку bin.

Перезавантажити операційну систему.

Зайти в теку home/me/bin і, послідовно створити в ній файли 1.txt, 2.txt, 3.txt, 4.txt , в кожен з яких помістити інформацію щодо кількох (2-3) платіжних транзакцій (одна транзакція - один рядок).

Приклад змісту такого файла:

Дмитро -> Маша :: 90 гривень
Жора -> Василь :: 1000 гривень
Аня -> Люда :: 600 гривень

(Важливо! Працюючи в стандартному текстовому редакторі системи Ubuntu, втановіть в меню **Налаштування** пункт **Номери лінійок.** Це дасть змогу уникнути випадкового додавання пустих рядків в кінець файла).

Зайти з терміналу в теку home/me/bin, де розташовані файли 1.txt, 2.txt, 3.txt, 4.txt і виконати команду

sha256sum 1.txt

Команда поверне значення хеш-функції для файлу 1.txt, яке слід скопіювати і вставити останнім рядком у файл 2.txt.

Потім знаходимо хеш файла 2.txt і вставляємо його у якості останнього рядка файла 3.txt.

Потім знаходимо хеш файла 3.txt і вставляємо його у якості останнього рядка файла 4.txt.

Потім знаходимо хеш файла 4.txt і зберігаємо його у новоствореному пустому файлі final.txt.

В результаті ми створили Блокчейн - ланцюжок криптографічнопов’язаних блоків.

Для перевірки цілісності ланцюжка (відсутності несанкціонованих змін в окремих файлах) можливо по черзі пройти по всім файлам ланцюжка, знайти хеш кожного і порівняти зі значенням хешу, що знаходиться в наступному файлі ланцюга.

Але на практиці таку перевірку виконують програмними засобами. Для цього пропонується файл b.sh (надається викладачем), який слід скопіювати в теку home/me/bin і виконати з термінала команду

chmod 755 b.sh

(встановлює дозвіл на виконання для файла b.sh).

Потім запустити b.sh на виконання з вікна терміналу командою:

bash b.sh

Якщо блоки ланцюжка не змінювались, скрипт дасть повідомлення «chain is flawless» і поверне значення хеша, який співпаде зі значенням у файлі final.txt.

Спробуйте в одному з блоків змінити певну транзакцію (видалити або поміняти суму або ім'я людини).

Тоді при виконанні скрипт видасть повідомлення «chain is corrupted».

Анулюйте зроблені зміни транзакції, скрипт при запуску знову видасть «chain is flawless».

Продемонструйте роботу скрипта викладачу.

Завдання 2. Змоделювати спрощений процес майнінгу криптовалюти біткоїн.

Видаліть з файлів 2.txt, 3.txt, 4.txt , final.txt рядки зі значеннями хеша.

Додайте до файлу 1.txt перший рядок, що містить якусь специфічну інформацію, наприклад, рядок з десяти нулів 0000000000 (в реалізації блокчейна біткоін таке поле називають Nonce).

Також додайте це поле з десяти нулів у якості першого рядка файлів 2.txt,3.txt, 4.txt (потім знадобиться).

Отримайте хеш файлу 1.txt (як це робили в першій частині). Якщо значення хешу починається з трьох нулів «000«, то можна вставляти його у файл 2.txt, якщо ні, то збільшуємо поле Nonce на 1: "0000000001" і повторюємо процедуру.

І так повторюємо доти, поки не отримаємо 000 на початку хеша.

Хто має підозру, що цей процес затягнеться до кінця навчального року, може скористатися скриптом m.sh (надається викладачем).

Скрипт слід скопіювати в теку home/me/bin і виконати з терміналу команду:

chmod 755 m.sh

Потім запустіть m.sh з вікна терміналу, вказавши параметр 1.txt :

bash m.sh 1.txt

Отримане значення хешу з трьома нулями на початку додайте останнім рядком до файлу 2.txt. Збережіть зміни.

Запустіть m.sh з вікна терміналу, вказавши параметр 2.txt

Отримане значення хешу з трьома нулями на початку додайте останнім рядком до файлу 3.txt. Збережіть зміни.

Запустіть m.sh з вікна терміналу, вказавши параметр 3.txt

Отримане значення хешу з трьома нулями на початку додайте останнім рядком до файлу 4.txt. Збережіть зміни.

Запустіть m.sh з вікна терміналу, вказавши параметр 4.txt

Отримане значення хешу з трьома нулями на початку додайте до файлу final.txt.

Застосуйте скрипт b.sh до отриманого нового ланцюжка блоків та перевірте його цілісність.

Спробуйте (не перемайнюючи весь ланцюг від початку до кінця) внести зміни до якоїсь з транзакцій таким чином, щоб хеш у файлі final.txt починався з 000 і ланцюг успішно проходив перевірку скриптом b.sh

Список використаних і рекомендованих джерел

1. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
3. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України 23 лют. 2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.
4. Стратегія національної безпеки України : Указ Президента України від 14 верес. 2020 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037.
5. Стратегія кібербезпеки України : Указ Президента України від 26 серп. 2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013.
6. Науково-практичний коментар до Закону України «Про основні засади забезпечення кібербезпеки України» / за заг. ред. В. Л. Грохольського. Одеса : ОДУВС, 2020. 142 с. URL: http://dspace.oduvs.edu.ua/ handle/123456789/1741.

Підручники та навчальні посібники

7. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони : підручник. Вид. 2-ге, переробл. та доповн. Одеса : ОНАЗ ім. О. С. Попова, 2019. 320 с.
8. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.
9. Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. / під. ред. В. М. Богуша. Київ : Ліра-К, 2020. 554 с.
10. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту : навч. посіб. для студ. вищ. навч. закл. Львів : Новий Світ-2000, 2020. 678 с.
11. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : навч. посіб. / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. Київ : ДУТКНУ, 2016. 178 с.

Додаткові Інтернет-джерела

12. Російсько-українська кібервійна. URL: https://uk.wikipedia.org/wiki.
13. Комп'ютерна безпека. URL: https://uk.wikipedia.org/wiki.
14. Що таке кібербезпека? URL: https://nordvpn.com/uk/cybersecurity.

ДОДАТОК

ВІДКРИТІ РЕЄСТРИ ТА БАЗИ ДАНИХ УКРАЇНИ

Список відкритих реєстрів та баз даних України, які допоможуть запобігти шахрайським діям, виявити фіктивні підприємства, фірми, приватних підприємців, з'ясувати ряд інших питань в юридичній діяльності:

1. База даних Верховної Ради України «Законодавство України»
http://zakon.rada.gov.ua/laws
2. Офіційні документи Президента України
http://www.president.gov.ua/documents
3. Пошук нормативно-правових документів Кабінету Міністрів України (Урядовий портал)
http://www.kmu.gov.ua/control/npd/search
4. «Єдиний державний реєстр нормативно-правових актів» (Міністерство юстиції України)
http://www.reestrnpa.gov.ua/REESTR/RNAweb.nsf/vWWWGroupParam1/searchext?OpenDocument
5. «Єдина база даних електронних адрес, номерів факсів суб'єктів владних повноважень»
http://email.court.gov.ua
6. «Поштові індекси та відділення поштового зв'язку України» (Українське державне підприємство «Укрпошта»)
http://services.ukrposhta.com/postindex_new
7. «Національний реєстр електронних інформаційних ресурсів» (Державний центр інформаційних ресурсів України)
http://e-resurs.gov.ua
8. Кабінет електронних сервісів (Міністерство юстиції України): «Державний реєстр речових прав на нерухоме майно»; «Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство»; «Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців»; «Реєстр громадських об'єднань»; «Державний реєстр друкованих ЗМІ та інформаційних агентств, як суб'єктів інформаційної діяльності»; «Єдиний реєстр громадських формувань»; «Єдиний реєстр арбітражних керуючих»; «Єдина база даних електронних адрес, номерів факсів, телефаксів суб'єктів владних повноважень»; «Єдиний державний реєстр судових рішень»; «Електронний реєстр апостилів»; «Єдиний державний реєстр осіб, які вчинили корупційні правопорушення»; «Єдиний державний реєстр осіб, щодо яких застосовано положення Закону України "Про очищення влади"»; «Єдиний реєстр нотаріусів»
https://kap.minjust.gov.ua/services/registry
9. Національний портал відкритих даних: «Реєстр громадських організацій»; «Реєстр операторів, постачальників комунікацій» та інші
http://data.gov.ua

10. Перелік електронних інформаційних БД державних установ України
https://uk.wikipedia.org/wiki/Державний_реєстр
11. «Єдиний державний реєстр судових рішень»
http://www.reyestr.court.gov.ua
12. МВС України. Розшук: «Зниклі громадяни»; «Неопізнані трупи»; «Культурні цінності»; «Мобільні телефони»; «Зброя у розшуку»; «Транспортні засоби у розшуку»; «Особи, які переховуються від органів влади»; «Особи, що не можуть надати про себе відомостей внаслідок хвороби або неповнолітнього віку»; «Перевірка легітимності довідки про судимість»; «Пошук паспорта громадянина України серед викрадених та втрачених»
http://mvs.gov.ua/mvs/control/uk/investigation
13. «Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань» (Міністерство юстиції України)
https://usr.minjust.gov.ua/ua/freesearch
14. База даних ДФСУ: «Дізнайся більше про свого бізнес-партнера» (Державна фіскальна служба України)
http://sfs.gov.ua/businesspartner
15. «Єдиний ліцензійний реєстр»; «Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань»; «Реєстр документів дозвільного характеру» (Державне підприємство «Інформаційно-ресурсний центр»)
http://irc.gov.ua/ua/Poshuk-v-YeLR.html
16. Реєстри Нацкомфінпослуг: «Єдиний реєстр бюро кредитних історій»; «Державний реєстр страхових та перестрахових брокерів»; «Реєстр аудиторських фірм та аудиторів, які можуть проводити аудиторські перевірки фінансових установ» та інші
http://nfp.gov.ua/content/inshi-reestri-ta-pereliki.html
17. «Реєстр аудиторських фірм та аудиторів» (Аудиторська палата України)
http://apu.com.ua/reestr-auditorskikh-firm-ta-auditoriv
18. «Реєстр платників ПДВ» (Електронний кабінет платника)
http://sfs.gov.ua/reestr
19. «Державний реєстр фінансових установ» (Комплексна інформаційна система Держфінпослуг)
http://kis.nfp.gov.ua
20. «Структури власності банків України» (Національний банк України)
http://bank.gov.ua/control/uk/publish/article?art_id=6738234&cat_id=51342
21. «База жителів України»
http://www.nomer.org/allukraina
22. «Єдиний реєстр адвокатів України» (Національна асоціація адвокатів України)
http://erau.unba.org.ua
23. «Реєстр адвокатів, які надають безоплатну вторинну правову допомогу» (Координаційний центр з надання правової допомоги)
http://legalaid.gov.ua/ua/reiestry-advokativ

24. «Єдиний реєстр нотаріусів»
http://ern.minjust.gov.ua/pages/default.aspx
25. «Єдиний реєстр спеціальних бланків нотаріальних документів» (Державне підприємство «Національні інформаційні системи»)
http://rnb.nais.gov.com
26. «Реєстр атестованих судових експертів» (Мінюст України)
http://rase.minjust.gov.ua
27. «Реєстр методик проведення судових експертиз» (Міністерство юстиції України)
http://rmpse.minjust.gov.ua
28. «Інформація про стан розгляду заяви (запиту)» (Державний реєстратор речових прав на нерухоме майно)
http://rrp.informjust.ua
29. «Реєстр громадських об'єднань»
http://rgo.informjust.ua
30. «Єдиний реєстр громадських формувань»
http://rgf.informjust.ua/home/index
31. «Державний реєстр друкованих ЗМІ та інформаційних агентств, як суб'єктів інформаційної діяльності»
http://dzmi.informjust.ua
32. «Автоматизована система виконавчого провадження» (Міністерство юстиції України)
https://asvpweb.minjust.gov.ua/#/search-debtors
33. «Єдиний державний реєстр декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування» (Національне агенство з питань заплбігання корупції)
https://public.nazk.gov.ua
34. Відкрита база декларацій чиновників «Декларації»
http://declarations.com.ua
35. Реєстри Єдиного державного порталу адміністративних послуг
http://poslugy.gov.ua
36. «Реєстр послуг для всіх (по категоріях)» (Офіційний вебпортал адміністративних послуг міста Києва)
http://ac.dozvil-kiev.gov.ua
37. «Перевірка коду IMEI мобільних телефонів» (Український державний центр радіочастот)
http://www.ucrf.gov.ua/baza-imei/perevirka-kodu-imei
38. Перевірка документа про освіту
https://osvita.net/ua/checkdoc
39. Он-лайн перевірка своїх даних в Державному реєстрі виборців
https://www.drv.gov.ua/apex/f?p=111:LOGIN
40. «Реєстр наукових організацій»
http://store.uintei.kiev.ua/reestr_new.html

41. Бази даних та інформаційно-довідкові системи: «Винаходи та корисні моделі», «Знаки для товарів і послуг», «Промислові зразки» та інші (Державне підприємство «Український Інститут промислової власності»)

http://www.uipv.org/ua/bases2.html

42. Бази даних та інформаційно-довідкові системи (Державна служба інтелектуальної власності України)

http://sips.gov.ua/ua/systems.html

43. Бази та реєстри Міністерства охорони здоров'я України

http://www.moz.gov.ua/ua/portal/ms_registers

44. «Державний реєстр лікарських засобів»

http://www.drlz.kiev.ua

45. «Національний перелік основних лікарських засобів і виробів медичного призначення»

http://www.moz.gov.ua/ua/portal/register_naclist

46. Бази та реєстри Держсанепідемслужби

http://www.dsesu.gov.ua/ua/normativna-pravova-baza/bazi-ta-reestri

47. «Державний реєстр потенційно шкідливих об'єктів» (Державна архівна служба України)

http://sfd.archives.gov.ua/RUS/page4.html

48. «Електронний реєстр суб'єктів, які надають послуги, пов'язані з ЕЦП» (Центральний засвідчувальний орган)

http://czo.gov.ua/ca-registry

49. Довідник вантажних станцій Укрзалізниці

http://uz.gov.ua/cargo_transportation/general_information/cargo_stations

50. «Єдина база тварин з чипом»

http://www.tracer.com.ua/index.php?lang=ua

51. Судна, сертифіковані Регістром судноплавства України

http://shipregister.ua/ism.html

52. Публічна кадастрова карта України

http://www.map.land.gov.ua/kadastrova-karta

53. Реквізити аеропортів, аеродромів, вертодромів та ЗПМ України (Державна авіаційна служба України)

http://avia.gov.ua/documents/airports/certification/Aerodrome_ZPM_MTR/24145.html

54. «Реєстр цивільних повітряних суден» (Державна авіаційна служба України)

http://avia.gov.ua/documents/rcps/vrcps/24020.html

55. Он-лайн інформація про рейси цивільних літаків та їх історію

http://www.flightradar24.com

56. Он-лайн інформація про рух морського транспорту

http://www.marinetraffic.com/ua/ais/home

Навчальне видання

КОРНЕЙКО Олександр Васильович,
КУДІНОВ Вадим Анатолійович,
ПАКРИШ Олександр Євгенійович,
ХАХАНОВСЬКИЙ Валерій Георгійович

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Навчальний посібник

Комп’ютерна верстка *Яни ШУМКО*

Свідоцтво про внесення суб’єкта видавничої справи до державного реєстру видавців, виготовників і розповсюджувачів видавничої продукції Дк № 4155 від 13.09.2011.
Підписано до друку 02.04.2024. Формат 60х84/16. Папір офсетний.
Обл.-вид. арк. 12,75. Ум. друк. арк. 11,86.
Тираж 30 прим.