МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА ТА ПСИХОЛОГІЇ
Кафедра інформаційних технологій

Присвячується
105-річниці НАВС
від дня заснування

Кудінов В.А., Пакриш О.Є.

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Навчально-практичний посібник

Київ
2026

УДК 351.74:004](07)
К887

Авторський колектив:

Кудінов В. А. – кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ

Пакриш О. Є. – кандидат технічних наук, доцент, доцент кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ

Рецензенти:

Галицька І. Є. – кандидат технічних наук, доцент, доцент кафедри математичних методів захисту інформації ННФТІ Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Школьніков В. І. – доктор філософії з галузі знань «Право», доцент, завідувач кафедри кримінології та інформаційних технологій Національної академії внутрішніх справ

Рекомендовано до Вченою радою Національної академії внутрішніх справ 30 грудня 2025 року (протокол № 25/4-9)

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

К887 **Інформаційно-аналітичне забезпечення правоохоронної діяльності [Текст] : навч.-практ. посіб. / [В. А. Кудінов, О. Є. Пакриш]. Київ : Нац. акад. внутр. справ, 2026. 116 с.**

У навчально-практичному посібнику висвітлено теми, охоплені навчальною дисципліною «Інформаційно-аналітичне забезпечення правоохоронної діяльності», яку викладають для здобувачів ступеня вищої освіти магістра спеціальності «Правоохоронна діяльність» в Національній академії внутрішніх справ.

Видання призначене для здобувачів ступеня вищої освіти магістра, науково-педагогічних працівників закладів вищої освіти системи МВС України, а також може бути корисним для слухачів аспірантури (ад'юнктури) і докторантури, наукових і практичних працівників правоохоронних органів.

УДК 351.74:004](07)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

OSINT – Open Source Intelligence (розвідка з відкритих джерел)
БД – База даних
Європол – Європейський поліцейський офіс
ЄДРСР – Єдиний державний реєстр судових рішень
ЄІС – Єдина інформаційна система
ЄРДР – Єдиний реєстр досудових розслідувань
ІАЗ – Інформаційно-аналітичне забезпечення
ІАС – Інформаційно-аналітична система
ІБ – Інформаційна безпека
ІКС – Інформаційно-комунікаційна система
Інтерпол – Міжнародна організація кримінальної поліції
ІПНП – Інформаційний портал Національної поліції
ІПС – Інформаційно-пошукова система
ІС – Інформаційна система
ІТ – Інформаційні технології
КК – Кримінальний кодекс
КМУ – Кабінет Міністрів України
КПК – Кримінальний процесуальний кодекс
КСЗІ – Комплексна система захисту інформації
КУпАП – Кодекс України про адміністративні правопорушення
МВС – Міністерство внутрішніх справ
НАВС – Національна академія внутрішніх справ
НПУ – Національна поліція України
НЦБ – Національне центральне бюро
ОС – Операційна система
ПЗ – Програмне забезпечення
СІЗ – Система інформаційного забезпечення
СППР – Система підтримки прийняття рішень
СУБД – Система управління базами даних
ТЗІ – Технічний захист інформації
ФП – Функціональна підсистема
ЦП – Центральна підсистема
ЦУНАМІ – Централізоване управління нарядами патрульної служби
ЧЧ – Чергова частина
ШІ – Штучний інтелект
ШПЗ – Шкідливе програмне забезпечення

ПЕРЕДМОВА

Даний навчально-практичний посібник висвітлює зміст основних тем дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності», яка викладається кафедрою інформаційних технологій для здобувачів ступеня вищої освіти магістра в навчально-науковому інституті права та психології Національної академії внутрішніх справ (далі – НАВС).

Історія становлення кафедри інформаційних технологій містить цікавий та насичений різними подіями шлях, який безпосередньо пов'язаний з історією становлення провідного закладу вищої освіти системи Міністерства внутрішніх справ (далі – МВС) – Національної академії внутрішніх справ (11.06.1921).

ДАТА	***НАЗВА КАФЕДРИ***	
25.06.1988	кафедра технічних засобів попередження та розкриття злочинів	Київської вищої школи МВС СРСР ім. Ф.Е. Дзержинського
01.05.1990	кафедра інформаційно-обчислювальної техніки	
01.09.1991	кафедра технічних засобів попередження та розкриття злочинів	
27.01.1992	кафедра технічних засобів попередження та розкриття злочинів	Української академії внутрішніх справ
10.01.1996	кафедра оперативної техніки	
20.12.1996	кафедра оперативної техніки	Національної академії внутрішніх справ України
30.08.1999	кафедра інформаційних технологій	Інституту підготовки управлінських кадрів НАВС України
21.07.2000		Інституту управління НАВС України
15.01.2003		НАВС України
08.09.2005		Київського національного університету внутрішніх справ

ДАТА	*НАЗВА КАФЕДРИ*	
27.08.2010	кафедра інформаційних технологій	НАВС
19.07.2013		навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції НАВС
07.11.2015		навчально-наукового інституту № 1 НАВС
01.09.2017	кафедра інформаційних технологій та кібернетичної безпеки	навчально-наукового інституту № 1 НАВС
17.10.2018	кафедра інформаційних технологій та кібербезпеки	
01.09.2024	кафедра інформаційних технологій	навчально-наукового інституту права та психології НАВС

Кафедра інформаційних технологій та кібербезпеки
30 років (*25.06.2018*)

Кафедра інформаційних технологій та кібербезпеки
35 років (*25.06.2023*)

Кафедра інформаційних технологій ННІ права та психології

Секція кафедри кримінології та інформаційних технологій

(*01.09.2024*)

Вадим Анатолійович
КУДІНОВ

Олександр Євгенійович
ПАКРИШ

ЕПІГРАФИ ДО ДИСЦИПЛІНИ

Хто володіє інформацією – той володіє світом

(У. Черчіль, 1946)

Хто своєчасно володіє достовірною та повною інформацією, правильно її застосовує – той володіє ситуацією

(Кудінов В.А., 2012)

Хто має та вміло використовує інформаційні технології – той володіє інформацією

(Кудінов В.А., 2006)

Хто володіє сучасними інформаційними технологіями, той може отримати відповідь майже на будь-яке запитання

(Кудінов В.А., 2025)

В сучасному глобалізованому, технологізованому світі роль інформаційно-аналітичної діяльності об'єктивно зростає. Це обумовлено насамперед швидким розвитком усіх процесів і явищ як в економіці, політиці, так і в інших сферах суспільного життя, зокрема і в діяльності правоохоронних органів, в яких стрімкий розвиток інформаційних технологій (далі – ІТ) призвів до накопичення та зберігання великих обсягів інформації.

Як відомо, діяльність будь-яких структур сьогодні потребує хоча б мінімального прогнозованого розвитку, захисту від ризиків, небезпек і викликів. Саме таким універсальним засобом в інформаційному суспільстві є аналітика. Без використання інформаційно-аналітичного забезпечення правоохоронної діяльності, в реаліях сьогодення, неможливе якісне виконання правоохоронцями своїх функцій із захисту суспільства та забезпечення верховенства права.

Аналіз даних та підтримка ухвалення рішень є ключовими аспектами ефективного управління в діяльності Національної поліції України (далі – НПУ), Служби безпеки України, судів та інших правоохоронних органів. Вони дозволяють правоохоронним структурам своєчасно отримувати необхідну інформацію для прийняття обґрунтованих рішень, що, в свою чергу, підвищує ефективність їх роботи в умовах глобалізації та цифрових трансформацій. Це критично важливо для забезпечення належного виконання функцій, що охоплюють не лише забезпечення верховенства права, боротьбу зі злочинністю, а й покращення безпеки держави, громадської безпеки та взаємодію з іншими державними органами [15].

В сучасних умовах специфіка інформаційно-аналітичної роботи полягає в забезпеченні особи, яка приймає рішення, тобто управлінця, необхідною і достатньою кількістю аналітичної інформації для прийняття правильного та ефективного, в умовах непередбаченості і кризових явищ, управлінського рішення.

Таким чином, інформаційно-аналітична діяльність певною мірою убезпечує, захищає керівників, управлінців від ризиків, небезпек і викликів сьогодення, рекомендуючи те чи інше ефективне управлінське рішення, прогнозуючи наперед наслідки його прийняття чи неприйняття, чи бездіяльності [18, с. 15].

У навчально-практичному посібнику розглянуто найважливіші теоретичні та практичні питання інформаційно-аналітичного забезпечення правоохоронної діяльності, основні принципи, методики, програмні та інформаційні компоненти застосування інформаційно-аналітичного забезпечення для прийняття ефективних управлінських рішень. Особливу увагу приділено розвитку нових засобів інтелектуалізації інформаційно-аналітичної діяльності, специфіці професії аналітика, інформаційній революції, викликаній появою штучного інтелекту (далі – ШІ), загрозам, що виникають у зв'язку з цим та сучасним концепціям розвитку інформаційного суспільства.

Навчально-практичний посібник розрахований на здобувачів ступеня вищої освіти магістра спеціальності «Правоохоронна діяльність», але може бути корисний викладачам, аспірантам, практичним працівникам правоохоронних органів та всім, хто цікавиться аналітикою.

Завідувач кафедри
інформаційних технологій ННІ права та психології
Національної академії внутрішніх справ
кандидат фізико-математичних наук, доцент **Вадим КУДІНОВ**

РОЗДІЛ І
ОСНОВИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОБОТИ, ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКИ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

1.1. Мета, завдання та основні поняття навчальної дисципліни

Предметом вивчення навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності» є основи організації інформаційно-аналітичної діяльності, захисту інформації та забезпечення кібербезпеки на об'єктах інформаційної діяльності Національної поліції України, принципи роботи з державними реєстрами, відомчими інформаційними системами (далі – ІС), загальний порядок використання сучасного програмного забезпечення (далі – ПЗ) для здобуття, обробки та аналізу інформації.

Метою викладання навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності» є надання слухачам магістратури теоретичних положень та набуття ними практичних умінь і навичок з ведення інформаційно-пошукової та інформаційно-аналітичної роботи із застосуванням державних реєстрів, відомчих інформаційних систем та мережі Інтернет.

Основними завданнями вивчення дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності» є здобуття слухачами магістратури теоретичних знань та практичних умінь і навичок з таких питань, як:

– основи поводження з інформацією та її захисту на об'єктах інформаційної діяльності Національної поліції України;

– основи організації інформаційно-пошукової роботи із застосуванням державних реєстрів, відомчих інформаційних систем та мережі Інтернет;

– основи застосування сучасних програмних засобів для обробки, аналізу та візуалізації здобутої оперативної інформації за допомогою сучасних інформаційних технологій.

Правоохоронна діяльність – це діяльність органів державної влади, яка спрямована на попередження і припинення правопорушень та притягнення правопорушників до юридичної відповідальності шляхом застосування заходів фізичного і юридичного впливу.

При цьому варто враховувати, що серед видів правоохоронної діяльності виокремлюються такі: забезпечення громадського порядку, оперативно-розшукова діяльність, досудове розслідування. Крім цього, до правоохоронної діяльності можна віднести: а) діяльність із забезпечення охорони учасників кримінального судочинства; б) діяльність органів прокуратури, поліції, пенітенціарних органів тощо; в) діяльність із виявлення, запобігання та розслідування кримінальних правопорушень, оскільки і оперативно-розшукова діяльність забезпечує ці види діяльності; г) діяльність із захисту національної безпеки, державного кордону та правопорядку на всіх рівнях і всіма органами держави та певними службовими особами [28].

Інформаційно-аналітичне забезпечення (далі – ІАЗ) правоохоронної діяльності – це процес створення умов для задоволення інформаційних потреб службових осіб певного структурного підрозділу державної установи, які задіяні в процесі здійснення правоохоронної діяльності, шляхом збору, обробки, аналізу та використання даних для прийняття управлінських рішень. ІАЗ складається з двох основних етапів: *інформаційного* (збір і накопичення даних) та *аналітичного* (їх обробка, аналіз, створення висновків і прогнозів).

Основні складові ІАЗ:

- *інформаційна діяльність*: зосереджена на пошуку, зборі, класифікації, зберіганні та поширенні даних;
- *аналітична діяльність*: використовує зібрану інформацію для її глибокого аналізу, узагальнення та перетворення на нове знання у вигляді висновків, пропозицій або прогнозів.

Станом на сьогодення, ***основними тенденціями розвитку*** інформаційно-аналітичного забезпечення у правоохоронній діяльності можна вважати:

– вдосконалення засобів адміністрування та управління відомчими інформаційно-комунікаційними системами (далі – ІКС);

– централізацію та інтеграцію даних з наявних інформаційних, пошукових, аналітичних платформ та реєстрів;

– впровадження новітніх інформаційно-технічних інструментів для покращення методів взаємодії між співробітниками правоохоронних органів;

– застосування спеціалізованих засобів забезпечення кібербезпеки та захисту інформації;

– підвищення кваліфікації співробітників правоохоронних органів щодо використання сучасних інформаційно-технічних інструментів обробки службової інформації;

– налагодження ефективних механізмів доступу та використання інформації в частині дотримання прав людини;

– залучення експертів і науковців для постійного вдосконалення інформаційно аналітичних систем та проведення регулярного моніторингу тенденцій і загроз у сфері інформаційно-аналітичної та інформаційно-технічної підтримки правоохоронної діяльності.

Інформаційно-аналітичне забезпечення є не лише допоміжним інструментом у правоохоронній діяльності, а й стратегічним ресурсом, від якого залежить ефективність функціонування усієї системи захисту правопорядку. У сучасних умовах воєнних викликів та глобальної цифровізації саме здатність органів правопорядку швидко збирати, аналізувати й використовувати інформацію визначає рівень безпеки держави і суспільства [24].

1.2. Основні поняття про інформаційну діяльність окремих підрозділів правоохоронних органів

Основна діяльність правоохоронних органів включає інформаційне забезпечення, що передбачає збір, аналіз та використання відомостей для виконання своїх функцій, а також охорону цих даних. Інформаційна діяльність охоплює створення та використання інформаційних систем, мереж, баз та банків даних для задоволення інформаційних потреб як держави, так і громадян, і включає такі види, як набуття, використання, поширення, зберігання, охорона та захист інформації.

Зокрема, інформаційно-аналітична діяльність НПУ є основною складовою її роботи. Вона охоплює збір, обробку, аналіз та використання різноманітної інформації для забезпечення громадського порядку, протидії злочинності та забезпечення безпеки громадян. Завдяки інформаційно-аналітичній діяльності поліція може ефективно прогнозувати та запобігати злочинам, розкривати злочини швидше та ефективніше, а також сприяти здійсненню кримінального переслідування. Важливою складовою цієї діяльності є аналіз отриманої інформації з використанням сучасних методів та технологій, що дозволяє отримати об'єктивну та достовірну картину ситуації [21, с. 8].

Біометрична ідентифікація набуває дедалі більшого значення в інформаційно-аналітичному забезпеченні діяльності правоохоронних органів України. У сучасному світі, де інформація є однією з ключових цінностей, інтеграція біометричних технологій у процеси збору, обробки та використання даних стає невід'ємною частиною ефективного функціонування правоохоронних структур. Впровадження таких технологій дозволяє не лише підвищити рівень безпеки, а й забезпечити оперативність і точність прийняття рішень. Основним завданням біометричної ідентифікації є встановлення унікальності особи на основі її фізіологічних або поведінкових характеристик. В Україні до біометричних параметрів, що використовуються для ідентифікації особи, належать відбитки пальців, зображення обличчя, аналіз голосу, сітківки ока та інші методи. У поєднанні з сучасними інформаційними системами ці дані створюють потужний інструмент для ідентифікації, верифікації та моніторингу як громадян, так і осіб, що становлять загрозу національній безпеці.

В умовах воєнного стану та постійних загроз територіальній цілісності України біометричні технології демонструють свою ефективність у розв'язанні низки завдань. Одним із таких є ідентифікація осіб, які намагаються приховати свою особу або використовують фальшиві документи. Завдяки інтеграції біометричних даних до систем прикордонного контролю, правоохоронні органи отримують можливість швидкого і точного виявлення таких випадків. Це, у свою чергу, сприяє зміцненню обороноздатності держави.

Сучасні інформаційно-аналітичні системи (далі – ІАС) допомагають правоохоронним органам проводити глибокий аналіз поведінки осіб, що мають певний зв'язок з кримінальною діяльністю. Це дозволяє збирати й обробляти дані про кримінальні події, взаємодіючі з базами даних (далі – БД) на національному та міжнародному рівнях [17].

Психологічні профілі осіб, що стали жертвами чи кривдниками, можуть бути оброблені за допомогою спеціальних програмних засобів, що допомагають ідентифікувати потенційно небезпечних осіб або створити передбачуваний профіль злочинця.

Використання технологій для психологічного профілювання злочинців відкриває нові горизонти у правоохоронній діяльності. Завдяки аналізу поведінкових патернів, використовуючи алгоритми машинного навчання, можна створювати точніші прогнози щодо можливих дій підозрюваних. Це допомагає не тільки в розслідуваннях, але й у попередженні злочинів, адже психологічний профіль злочинця дозволяє передбачити ймовірні місця й способи скоєння правопорушень [16].

Важливе значення відіграють технології інформаційно-аналітичного забезпечення правоохоронної діяльності в сфері економічної безпеки держави. У статті 4 Закону України «Про Бюро економічної безпеки України» зазначено, що одним з завдань означеного органу є збирання та аналіз інформації, що впливають на економічну безпеку держави [3].

1.3. Інструментарій аналізу даних і підтримки прийняття рішень в правоохоронній діяльності

Аналіз даних в правоохоронній діяльності передбачає використання різних методів, від базових статистичних до більш складних моделей машинного навчання та використання систем ШІ, які дозволяють виявляти закономірності та робити прогнози. Останнім етапом є візуалізація даних у вигляді графіків або панелей для зручного сприйняття та інтерпретації, що забезпечує підтримку в прийнятті рішень для практичної діяльності правоохоронної структури.

Зокрема, аналіз даних у контексті НПУ є складним процесом, що охоплює кілька етапів. Початково здійснюється збір даних з різних джерел, як внутрішніх (звіти, БД), так і зовнішніх (ринкові дослідження, соціальні мережі), з використанням автоматизованих інструментів (веб-скрепінг, тобто автоматичне вилучення даних з вебсайтів за допомогою програм-скриптів або ботів) для ефективного збору великих обсягів інформації. На етапі обробки дані очищаються від непотрібних або застарілих записів, стандартизуються і агрегуються для подальшого аналізу. Стандартизувати дані допомагають спеціалізовані мови програмування.

Для ефективного аналізу інформації застосовуються як традиційні, так і новітні методи. Основні інструменти включають таке програмне забезпечення, як Power BI та Tableau для створення інтерактивних дашбордів, Google Data Studio для базової аналітики. Серед мов програмування популярними є Python з бібліотеками pandas, scikit-learn, matplotlib та мова програмування R, призначена для вирішення аналітичних задач. Технології великих даних, такі як Hadoop і Spark, дозволяють обробляти великі обсяги інформації, а алгоритми машинного навчання, зокрема регресії, дерева рішень та глибоке навчання, застосовуються для прогнозування та автоматизації процесів, що підвищує ефективність роботи правоохоронних органів [19].

Процес ухвалення рішень на основі аналізу даних включає кілька етапів. Спочатку визначається проблема, що дозволяє чітко сформулювати завдання, наприклад, покращення ефективності реагування на надзвичайні ситуації. Потім проводиться оцінка альтернатив, де порівнюються різні варіанти дій з урахуванням їхніх переваг та ризиків, що може бути здійснено за допомогою інструментів аналізу, таких як SWOT. Після цього приймається рішення з урахуванням різних критеріїв через методи багатокритеріального аналізу. Останнім етапом є моніторинг і корекція рішень, що включає оцінку ефективності реалізованих заходів та внесення коректівів для досягнення оптимальних результатів у діяльності правоохоронної структури [19].

Широке розповсюдження в галузі інформаційно-аналітичного забезпечення правоохоронної діяльності отримало ***IBM i2*** – сімейство програмних продуктів для візуального аналізу даних, яке допомагає аналітикам виявляти, аналізувати та візуалізувати зв'язки у великих та складних обсягах інформації. Основні компоненти, такі як IBM i2 Analyst's Notebook, дозволяють співставляти дані з різних джерел для розслідування злочинів, шахрайства та інших видів діяльності.

Головне завдання IBM i2 – це пошук прихованих взаємозв'язків та закономірностей серед великої кількості сутностей, що дозволяє використовувати його службам економічної та внутрішньої безпеки, ризик-менеджерами і розслідувальним управлінням. IBM i2 працює на стику трьох напрямків: виявлення та запобігання злочинній, терористичній та шахрайській діяльності; аналіз фінансових потоків та встановлення зв'язків між юридичними особами; швидкий пошук, аналіз та візуалізація складних даних з різних джерел.

IBM i2 робить процес аналізу простим і наочним. Вирішення завдання безпеки інформації реалізується за допомогою візуалізації прихованих зв'язків і статистичних закономірностей між даними. IBM i2 дозволяє представити результати обробки в зручній формі, роблячи їх презентабельними і наповненими вичерпною інформацією.

Система IBM i2 складається з різних компонентів, які, в залежності від розв'язуваних завдань, можуть бути налаштовані і застосовані в різних комбінаціях:

1) ***Analyst's Notebook*** − візуальне аналітичне середовище, яке дозволяє максимально ефективно використовувати величезні обсяги інформації, накопичені компаніями та установами. Analyst's Notebook, беручи логи (спеціальні файли або послідовності записів, що містять систематизовану, хронологічну інформацію про події, які відбуваються в комп'ютерній системі, програмі чи мережі) з цілого ряду джерел,− перетворює їх на цінну інформацію, що дає змогу побудувати повну картину для дослідження.

У Analyst's Notebook дані зберігаються як об'єкти, зв'язки та властивості. Завдяки простому та зрозумілому інтерфейсу аналітики можуть швидко зіставляти, аналізувати і наочно представляти дані, скорочуючи час на пошук важливої інформації в неструктурованих даних.

Сервіс забезпечує тимчасовий і геопросторовий аналіз завдяки інтеграції з геопросторовими функціями ArcGIS Server компанії Esri. Дане рішення надає актуальні і дієві аналітичні засоби, що допомагають виявляти, передбачати, запобігати і припиняти злочинну, терористичну і шахрайську діяльність.

Тож, серед задач, що вирішує IBM i2 Analyst's Notebook, можна виділити такі: швидка систематизація розрізнених даних і подання в єдиному узгодженому вигляді; визначення ключових осіб, подій, зв'язків і закономірностей, які не завжди можна виявити іншими засобами; покращене розуміння структури, ієрархії і способів дій злочинних, терористичних і шахрайських організацій; спрощення обміну складними даними, що дозволяє приймати своєчасні і точні оперативні рішення.

2) ***iBase*** – компонент, що представляє собою багатокористувацьку систему управління базами даних та дозволяє збирати й аналізувати дані з різних джерел, створюючи бази даних без глибоких знань реляційних систем управління базами даних (далі – СУБД). iBase є центральним вузлом системи, за допомогою якого здійснюється зберігання і аналіз інформації. Також за допомогою цього компонента здійснюється управління обліковими записами і правами доступу для багатокористувацьких систем.

iBase дозволяє: спроектувати базу даних, в якій буде згодом зберігатися інформація; формувати правила імпорту даних зі сторонніх джерел; здійснювати контроль доступу до даних і аудит подій такого доступу; централізовано зберігати результати аналізу.

3) ***i2 Analysis Hub*** – комплексне рішення, що об'єднує різні інструменти IBM i2 для створення централізованого аналітичного середовища, зокрема:

- *iBridge* – підключається до обраних корпоративних баз даних з можливостями пошуку/запиту для повернення даних, готових до аналізу. iBridge дозволяє: 1) безпосередньо підключатися до зовнішніх БД; 2) здійснювати пошук елементів в БД; 3) формувати візуальні запити на пошук інформації.
- *i2 Pattern Tracer* – оперативно аналізує великі обсяги телефонних записів, групує їх за спільними ознаками і виявляє ключових учасників, швидко ідентифікує потенційні цілі дзвінків, допомагає запобігти майбутнім інцидентам.
- *i2 Chart Reader* – дозволяє аналітикам обмінюватися результатами аналізу з тими, у кого немає доступу до i2 Analyst's Notebook.
- *i2 Text Chart* – інтуїтивно зрозуміле, кероване користувачем вилучення тексту та його візуалізація допомагає аналізувати неструктуровані дані.
- *i2 Text Chart Auto Mark* – автономний додаток, що автоматично виявляє і виділяє об'єкти, що вас цікавлять, в різноманітних документах.

Отже, система дозволяє отримувати реальну віддачу від інформаційно-аналітичних технологій обробки даних шляхом надання операційної аналітики, яка згодом може бути використана для поліпшення рівня обслуговування користувачів, скорочення експлуатаційних витрат, зниження ризиків інформаційній безпеці, створення нових продуктів і послуг, а також здатна протидіяти кіберзлочинності, розслідувати факти неправомірного доступу до інформації.

Важливим напрямком інформаційно-аналітичного забезпечення стало застосування **OSINT**(Open Source Intelligence).

Технології OSINT дозволяють використовувати відкриті джерела інформації, які доступні без спеціальних дозволів. Це можуть бути медіа, соціальні мережі, державні реєстри, комерційні бази даних, наукові публікації та інші джерела. В умовах швидкого розвитку технологій, таких як Інтернет речей (IoT), ШІ та великі дані, інформація, яка раніше була б недоступною або важко досяжною, сьогодні може бути ефективно зібрана і проаналізована. Одним з основних застосувань OSINT є моніторинг інформаційних потоків у реальному часі для виявлення потенційних загроз. За допомогою інструментів OSINT можна оперативно оцінювати стан безпеки на різних етапах: від попередження загроз до оцінки наслідків від їх реалізації.

Технології OSINT охоплюють велику кількість різноманітних інструментів (Maltego, IBM i2, Analyst's Notebook, DataMiner, Nmap, Recon-ng тощо) та методик, що дозволяють отримувати інформацію з різних відкритих джерел. Деякі з цих інструментів відразу вбудовують в дистрибутив Kali Linux.

Основними аспектами застосування OSINT є [22]:

1. *Аналіз соціальних мереж*: соціальні мережі, такі як Facebook, Twitter (X), Instagram, є одним з найбільших джерел інформації, де можна виявляти різноманітні загрози – від інформаційних атак до актів насильства чи дестабілізації суспільства. Аналіз цих платформ за допомогою автоматизованих систем дозволяє швидко виявляти загрози та реагувати на них.

2. *Моніторинг медіа*: новинні сайти та інші медіа платформи містять велику кількість корисної інформації для оцінки політичної та соціальної ситуації в країні.

3. *Використання геоінформаційних систем*: застосування геопросторових даних, таких як карти, GPS-трекінг, є важливим для оцінки та прогнозування ситуацій на полі бою або для моніторингу інфраструктури.

4. *Аналіз відео та зображень*: завдяки розвитку технологій обробки зображень можна автоматично аналізувати відео та фотографії для виявлення можливих загроз, таких як зміни на території, загрози в інфраструктурі чи масові протести.

Останнім часом набула широкого розповсюдження практика використання мов програмування, зокрема, мови **Python** для інформаційно-аналітичного забезпечення правоохоронної діяльності. Використання мови Python надає широкі можливості для обробки даних, машинного навчання та автоматизації процесів, що допомагає у розслідуваннях, профілактиці злочинів та управлінні базами даних. Зокрема, Python використовується для аналізу великих обсягів даних з різних джерел, розробки моделей для виявлення підозрілих патернів, автоматизації рутинних завдань та створення аналітичних інструментів для ефективнішого прийняття рішень.

Конкретні сфери застосування Python в інформаційно-аналітичному забезпеченні правоохоронної діяльності:

- *Аналіз даних*: Python використовується для обробки та аналізу великих наборів даних, таких як кримінальні хроніки, бази даних свідків, записи камер відеоспостереження та дані з соціальних мереж для виявлення зв'язків та тенденцій.
- *Машинне навчання*: бібліотеки, такі як Scikit-learn, TensorFlow та PyTorch, дозволяють створювати моделі для прогнозування злочинності, ідентифікації шахрайства, виявлення підозрілої поведінки або аналізу відбитків пальців.
- *Автоматизація та оптимізація*: Python може автоматизувати рутинні завдання, наприклад, сортування документів, створення звітів або управління БД, що дозволяє працівникам зосередитися на більш складних завданнях.
- *Створення аналітичних інструментів*: Python використовується для розробки спеціалізованих програмних продуктів, які допомагають у розслідуваннях, візуалізують дані у вигляді карт, графіків та діаграм, або створюють ефективні системи пошуку та фільтрації інформації.
- *Інформаційна безпека (далі – ІБ)*: за допомогою Python можна розробляти інструменти для захисту інформації, виявлення кіберзагроз та аналізу мережевої активності, забезпечуючи, таким чином, інформаційну безпеку правоохоронних органів.

Переваги використання Python:

- *Простота та універсальність*: Python є відносно простим для вивчення та використання, що робить його доступним для багатьох фахівців. Він також є універсальним і може бути інтегрований з іншими системами та мовами програмування.
- *Велика екосистема*: існує велика кількість бібліотек та фреймворків, які спеціально розроблені для аналізу даних, машинного навчання та роботи з інформацією, що значно спрощує розробку.
- *Висока швидкість розробки*: завдяки простим синтаксистам та великій кількості готових рішень, розробка та впровадження програмних рішень за допомогою Python відбувається швидше.

1.4. Захист інформації та кібербезпеки на об'єктах інформаційної діяльності правоохоронних органів

1.4.1. Теоретичні основи інформаційної безпеки

Широке впровадження комп'ютерів в усі види діяльності людини, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу призвели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності.

Початковий етап розвитку ІБ міцно пов'язаний із *криптографією*. Головні умови безпеки інформації – її доступність і цілісність. Інакше кажучи, користувач може будь-коли запросити необхідний йому набір сервісних послуг,

а система безпеки повинна гарантувати при цьому його правильну роботу. Будь-який файл або ресурс системи, при дотриманні прав доступу, повинен бути доступний користувачеві в будь-який час. Якщо якийсь ресурс недоступний, то він некорисний. Інше завдання захисту – забезпечити незмінність інформації під час її зберігання або передавання. Це так звана умова цілісності [20].

Виконання процедур шифрування й дешифрування у будь-якій ІС сповільнює передачу даних і зменшує їхню доступність, тому що користувач буде занадто довго чекати свої «надійно захищені» дані, а це неприпустимо в деяких сучасних ІС. Тому система безпеки повинна, в першу чергу, гарантувати доступність і цілісність інформації, а потім уже її конфіденційність.

Принцип сучасного захисту інформації *можна виразити так – пошук оптимального співвідношення між доступністю й безпекою.*

Значення інформації зростає в міру зникнення національних кордонів між державами, подолання наслідків інформаційної ізоляції пострадянського суспільства. Водночас, стрімкий розвиток інформаційних технологій і збільшення обсягів інформації призвели до проблеми інформаційного перенасичення, надмірної кількості недостовірної та шкідливої інформації. З початком гострої фази Україно-російської війни, значно зросла загроза національній безпеці держави через інформаційне шпигунство, інформаційну агресію іноземних держав тощо.

Об'єктом ІБ є інформація, важлива для функціонування держави, демократичного розвитку суспільства, інформаційні стосунки між особою, державою та суспільством, інформаційні права людини як невід'ємна складова загальнолюдських прав [20].

Для забезпечення захисту персональних даних та конфіденційної інформації необхідно створення ***комплексної системи захисту інформації*** (далі – КСЗІ), яка являє собою сукупність організаційних, інженерно-технічних, програмно-апаратних та криптографічних заходів і засобів, що спільно забезпечують захист інформації від розголошення, витоку, несанкціонованого доступу та модифікації. КСЗІ створюється для захисту інформації, що обробляється в автоматизованих та інформаційно-комунікаційних системах (далі – ІКС), гарантуючи її конфіденційність, цілісність та доступність.

Основні складові КСЗІ наведені на рис. 1 [29]. Головне завдання КСЗІ полягає в блокуванні технічних каналів витоку інформації та ліквідації наслідків реалізації загроз інформації. Загрози інформації складаються з багатьох факторів, тому завдання захисту потребує комплексного підходу з використанням новітніх технічних засобів і наукових розробок. Вирішення завдань включають в себе аналіз об'єкта захисту, розробку системи виявлення каналів витоку інформації та економічне обґрунтування необхідності використання системи захисту інформації.

КСЗІ являє собою діючі у єдиній сукупності законодавчі, організаційні, технічні, криптографічні та інші заходи і засоби, які забезпечують захист інформації від усіх визначених загроз і можливих каналів її витоку, і, зокрема, каналів електромагнітного випромінювання.

Рис. 1.1. Основні складові КСЗІ

КСЗІ створюється поєднанням застосування технічних, фізичних та організаційних заходів. Проектування КСЗІ відбувалось на принципах побудови раціональної та ефективної системи захисту. Структура засобів КСЗІ зображена на рис. 1.2 [20].

Організаційно-правовими заходами реалізується комплекс відповідній нормативно-правовій базі держави адміністративних і обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту шляхом аналізу загроз, регламентації діяльності персоналу і визначення порядку функціонування засобів забезпечення інформаційної діяльності і засобів технічного захисту інформації (далі – ТЗІ), а також шляхом створення служб, відповідальних за їх реалізацію.

Основним завданням *технічних заходів* є забезпечення фізичної інформаційної безпеки. Фізичні заходи захисту інформації створюють пристрої та споруди, проводять заходи, що утруднюють або унеможливлюють проникнення потенційних порушників у місця, де можна мати доступ до системи управління та інформації, що захищається. Пропонується застосувати фізичну ізоляцію споруди, де встановлена апаратура, від інших будівель зокрема – огородження й систематичний контроль території, організація контрольно-пропускних пунктів, обладнання вхідних дверей спеціальними замками, організація системи охоронної сигналізації.

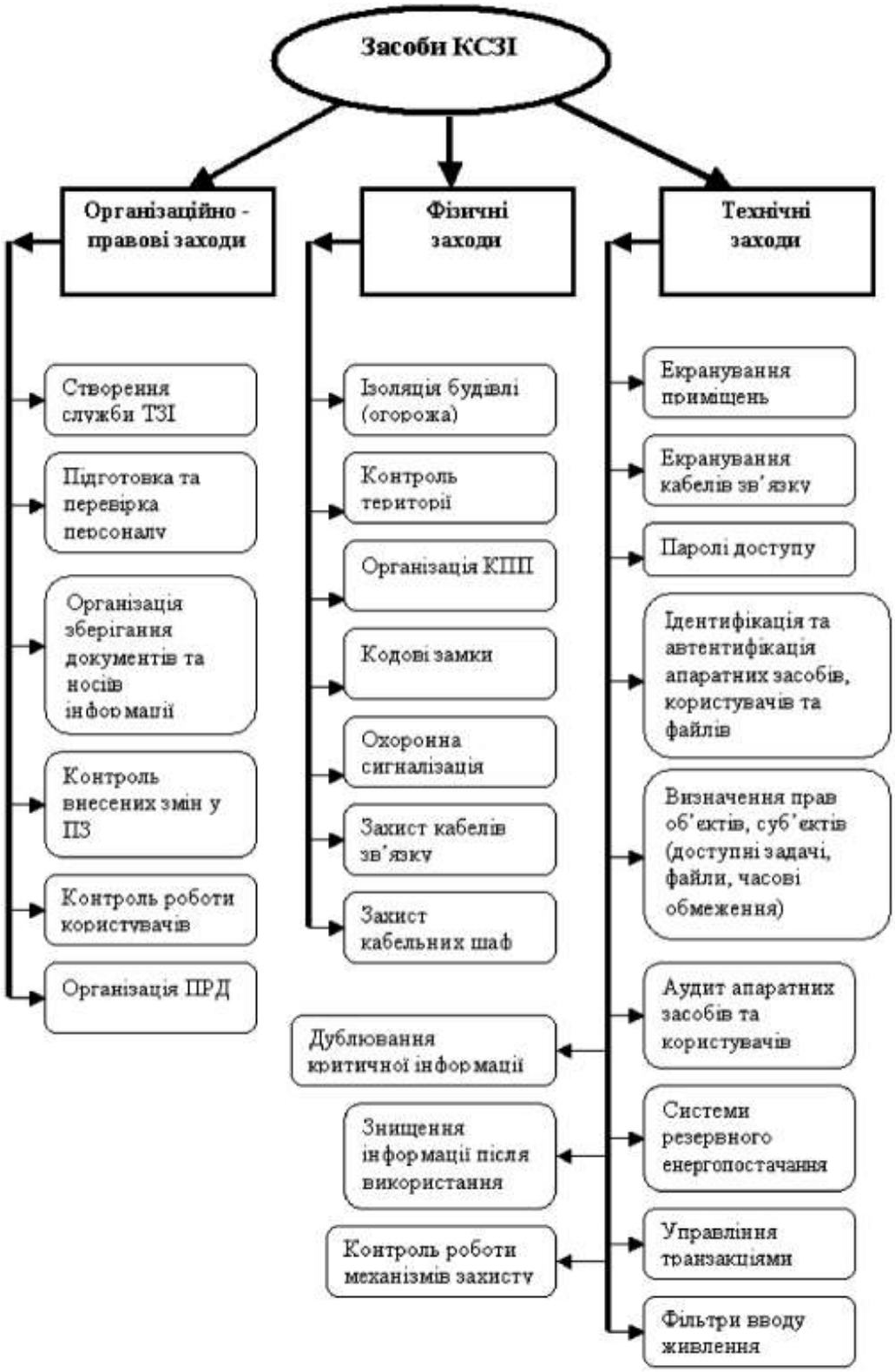


Рис. 1.2. Структура засобів КСЗІ

Застосовані ізоляція будинку, контроль території, кодові замки, контрольно-пропускний пункт (КПП), охоронна сигналізація. Від витоку інформації по каналах побічних електромагнітних випромінювань та наводок (ПЕОМ) пропонується екранування приміщень та кабелів зв'язку, по кабелях електроживлення передбачається установка фільтрів.

1.4.2. 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 Законі Україні «Про Національну безпеку України» [6], 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» [8] 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 (ІКС). Кіберпростір можна розглядати: а) як локальне середовище, у випадку функціонування засобу комп'ютерної техніки, який не під'єднано до мережі; б) як розосереджене середовище, яке виникає в разі підключення засобу комп'ютерної техніки до локальної або глобальної мережі передачі даних.

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» [8]: «***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. Причому 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 [9], 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: 1) *конфіденційності* – забезпечення доступу до інформації тільки уповноваженим на це користувачам; 2) *цілісності* – гарантування точності та повноти інформації; 3) *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 [26, с. 173]: 1) дій авторизованих користувачів; 2) дій «хакерів»; 3) дій шкідливого програмного забезпечення (далі – ШПЗ); 4) дій «спаму»; 5) дій «фішингу»; 6) дій «природних загроз» тощо.

Розглянемо їх більш детально.

1. 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.

2. 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.

3. 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, що 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. 1.3) [26, с. 174]. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу.

Рис. 1.3. 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 комп'ютери, наприклад, електронною поштою (рис. 1.4).

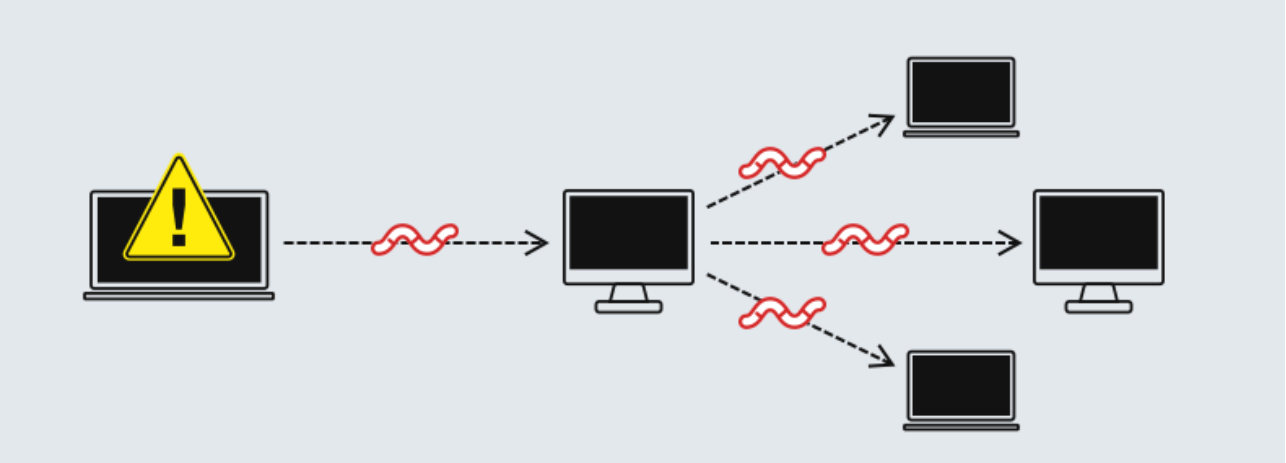


Рис. 1.4. Комп'ютерний хробак

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, комп'ютерних ігор 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 посилання на підроблений сайт). Троянська програма також може нести вірусне тіло – тоді запустив троянця комп'ютер перетворюється в осередок розповсюдження «зарази».

Рутκіт (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 переустановлення 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 (далі – 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.

4. ***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 ПЗ, що призведе до зараження комп'ютера, 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 найчастіше надсилаюся з добрими намірами.

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. 1.5). 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. 1.5). 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 навіть здогадуватися.

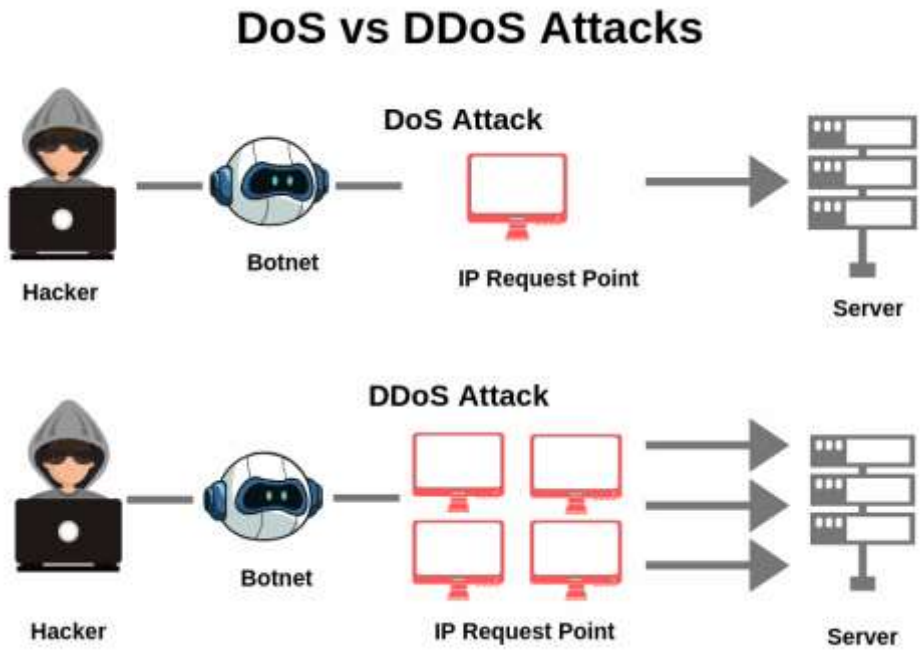


Рис. 1.5. DoS-атака та DDoS-атака

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.

5. ***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, логінів, 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.

6. ***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 (ІКС) 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» [8] 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.

Питання для самоконтролю

1. Мета, завдання та основні поняття навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності».
2. Поняття інформаційно-аналітичне забезпечення правоохоронної діяльності, основні її складові та тенденції розвитку.
3. Основні поняття про інформаційну діяльність окремих підрозділів правоохоронних органів.
4. Інструментарій аналізу даних і підтримки прийняття рішень в правоохоронній діяльності.
5. Загальна характеристика системи IBM i2.
6. Поняття технології інформаційно-аналітичного забезпечення OSINT.
7. Сфери застосування та переваги використання мови Python в інформаційно-аналітичному забезпеченні правоохоронної діяльності.
8. Поняття інформації та інформаційних технологій.
9. Поняття інформаційної безпеки та принцип сучасного захисту інформації.
10. Основні складові комплексної системи захисту інформації?
11. Структура засобів комплексної системи захисту інформації?
12. Поняття Національної безпеки держави.
13. Поняття кіберпростору.
14. Поняття кібербезпеки.
15. Основні загрози кібербезпеці.
16. Загрози кібербезпеці діями авторизованих користувачів.
17. Загрози кібербезпеці діями хакерів.
18. Поняття шкідливого програмного забезпечення.
19. Поняття фішингу.
20. Поняття спаму.
21. Поняття кібератаки.
22. Природні (об’єктивні) загрози кібербезпеці.

Практичні завдання до розділу І

Мета: отримання здобувачами ступеня вищої освіти магістра теоретичних знань, навичок та умінь щодо пошуку необхідної інформації в Інтернет, обробки статистичної інформації засобами Excel та захисту інформації за допомогою програмного продукту VeraCrypt.

Завдання 1.

1. Створити засобами редактора Word документ під назвою «Перелік інформаційних систем». Створити у документі відповідним чином відформатовану таблицю, наведену нижче.
2. В клітинки, залиті сірим, занесіть відповідну інформацію, знайдену в мережі Інтернет.
3. В документі «Перелік інформаційних систем» створити верхній (містить Ваше прізвище і дату) та нижній (містить номер групи) колонтитули.

Назва системи (підсистеми)	**Яким нормативним документом затверджена (назва, номер, дата)**
Єдина інформаційна система МВС	
Інформаційно-комунікаційна система «Інформаційний портал Національної поліції України»	
Інформаційна підсистема «Єдиний облік» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»	
Інформаційна підсистема «Гарпун» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»	
Інформаційна підсистема «Атріум» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»	
Інформаційна підсистема «Custody Records» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»	
Інформаційна підсистема «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»	

Завдання 2.

1. Створити в Excel таблицю з назвою «Статистика», на власний розсуд заповнити її вихідними даними, підрахувати суму та середнє значення (використавши відповідні формули або функції Excel), побудувати на основі даних двох нижніх рядків таблиці стовпчикову діаграму.

2. Заповнену даними таблицю та діаграму скопіювати та вставити в документ Word «Перелік інформаційних систем».

Назва району	Адмін. правопоруш.	Крадіжка	Угон АМТ	Розбійні напади	ДТП
Шевченківський					
Солом'янський					
Дарницький					
Святошинський					
Всього по 4 районам					
Середній показник по 4 районам					

Завдання 3

Підписати створений документ QR кодом, що містить Ваше прізвище латинськими літерами та захистити файл Word «Перелік інформаційних систем» паролем.

Завдання 4.

За допомогою програми VeraCrypt (у вільному доступі) створити файловий контейнер (віртуальний диск), у який помістити папку зі своїм файлом, розмонтувати контейнер, вийти з програми.

РОЗДІЛ ІІ
ОСНОВИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-ПОШУКОВИХ СИСТЕМ ТА МЕРЕЖІ ІНТЕРНЕТ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

2.1. Синтаксичні особливості пошукових машин сучасних інформаційно-пошукових систем

Синтаксичні особливості сучасних пошукових систем полягають у використанні спеціальних операторів для уточнення запитів, таких як лапки ("") для точного збігу, знак мінус (-) для виключення слів, site: для пошуку на конкретному сайті та filetype: для пошуку певних типів файлів. Системи пошуку також використовують синтаксис природної мови для розуміння більш складних запитань та контексту, а також автоматично розпізнають синоніми та різні форми слів.

***Основні синтаксичні особливості*:**

- Точний збіг: використання лапок ("") для пошуку точної фрази, наприклад, "синтаксичні особливості пошукових систем".
- Виключення слів: використання знаку мінус (-) перед словом, яке потрібно виключити з результатів, наприклад: пошукові машини -гугл.
- Пошук на конкретному сайті: використання оператора site: для обмеження пошуку певним доменом, наприклад, синтаксис: site:wikipedia.org.
- Пошук певних типів файлів: використання оператора filetype: для пошуку файлів певного формату (зокрема, pdf, docx), наприклад: звіт filetype:pdf.
- Об'єднання термінів: використання операторів AND (зазвичай неявно, якщо не вказано інакше) для пошуку всіх термінів та OR для пошуку хоча б одного з них, наприклад: синтаксичні OR оператори.
- Пошук за частиною слова (фрагментація): багато пошукових систем автоматично шукають варіації слова, але іноді можна використовувати символ * як підстановочний знак.
- Пошук у заголовках, тексті, посиланнях: деякі системи дозволяють вказувати, де саме шукати слово, наприклад: inurl:, intitle:, intext: .

2.1.1. Синтаксичні особливості пошукової машини ЄДРСР

1. Пошук по точній фразі

Зазначається, що він здійснюється за допомогою подвійних лапок (""). Якщо Ви шукаєте рішення з якоїсь точною фразою або словом, Вам потрібно взяти його в лапки. У такому випадку Єдиний державний реєстр судових рішень (далі – ЄДРСР) покаже документи, що містять пошуковий запит в тому вигляді, в якому Ви його написали. Приклад: «відновлення становища, яке існувало до порушення».

2. Пошук, якщо точний номер справи невідомий

Якщо Ви не знаєте точного номера справи, то замість одного невідомого символу в запиті ЄДРСР можна написати знак питання (?). Приклад: рішення № 594/5?8/20.

3. Пошук по основній частині пошукового слова

Здійснюється за допомогою зірочки (*). Вона замінює один або кілька символів. При цьому треба пам'ятати, що перед зірочкою повинно бути не менше трьох символів. В іншому випадку пошук в ЄДРСР за вказаними Вами параметрами виконаний не буде. Наприклад, якщо потрібно знайти рішення щодо будівельної компанії, то в поле контекстного пошуку можна ввести корінь основного слова, а після нього поставити зірочку. Приклад: будівельн*

4. Пошук одного з декількох пошукових слів

Здійснюється за допомогою логічного оператора OR, який обов'язково повинен бути зазначений великими літерами. В ЄДРСР будуть сформовані документи, які містять одне з написаних Вами слів або словосполучень. Приклад: рішення OR постанова.

5. Пошук за декількома пошуковими запитами

Зокрема, за замовчуванням пробіл між пошуковими запитами означає, що пошук буде здійснюватися одночасно по всім перерахованим словам. Однак якщо пошук в ЄДРСР планується робити не за окремими словами, а по пошуковим фразам, то більш доцільним є використання такого логічного оператора, як AND. Він, як і будь-який інший логічний оператор, повинен бути зазначений великими літерами. У такому випадку за результатами пошуку буде сформований список документів, які одночасно включають обидві пошукові фрази. Приклад: визнання права власності AND нерухоме майно.

6. Пошук з виключенням окремих слів

Для виключення з результатів пошуку окремих значень між пошуковими запитами потрібно поставити логічний оператор NOT. У такому разі всі слова, які були вказані перед логічним оператором, будуть враховані, а все, що після, ні. Прописується він великими літерами і може бути використаний в ЄДРСР тільки за наявності не менше двох пошукових слів. Приклад: нерухоме майно NOT земельна ділянка.

7. Пошук з обов'язковим включенням потрібного слова

Якщо хочете, щоб в ЄДРСР знайдені Вами документи обов'язково включали в себе певне значення, то перед пошуковим словом потрібно поставити знак + (плюс). Приклад: визнання права власності +автомобіль.

8. Пошук з виключенням певного слова

Для того, щоб результат пошуку в ЄДРСР не містив певного значення, перед таким пошуковим словом потрібно поставити знак - (мінус). Приклад: накладення арешту -рухоме майно.

9. Комбінований пошук

Передбачає одночасне використання різних способів пошуку і здійснюється за допомогою дужок. При цьому використання дужок на початку пошукового запиту в ЄДРСР не дозволяється. Приклад: визнання права власності AND (нерухоме майно OR нерухомість).

2.1.2. Синтаксичні особливості пошукової машини ІПС Google

Успіх пошуку необхідних інформаційних ресурсів в Інтернет в значній степені залежить від правильності написання запиту. Всі інформаційно-пошукові системи (далі – ІПС) мають власні мови запитів. Як правильно зробити запит, розглянемо на прикладі ІПС Google [30].

Інтерфейс Google містить досить складну мову запитів, яка дозволяє обмежити пошук окремими доменами, мовами, типами файлів і тому подібне. Пошукова машина Google, зазвичай, ігнорує пунктуацію, яка не є частиною оператора пошуку. Не слід ставити пробіли між символом або словом та пошуковим оператором. Пошук *site:nytimes.com* буде працювати, але *site: nytimes.com* не буде.

До речі, Google дозволяє вводити в рядок запиту не більше 32 слів.

Використання деяких операторів мови пошуку дозволяє зробити процес пошуку необхідної інформації більш гнучким і точним. Розглянемо деякі з них:

***Логічне "І" (AND)*:**

За замовчуванням при написанні слів запиту через space (пробіл) Google шукає документи, які одночасно містять всі слова запиту. Це і відповідає оператору AND. Тобто пробіл і є оператором AND.

Наприклад:

Кішки собаки папуги зебри

Кішки AND собаки AND папуги AND зебри

(обидва запити однакові).

***Логічне "АБО" (OR)*:**

Пишуть за допомогою оператора OR. Оператор OR повинен бути написаним великими літерами. Відносно нещодавно з'явилась можливість написання логічного "АБО" у вигляді вертикальної риски (|). Використовується для пошуку з декількома варіантами необхідної інформації.

Наприклад:

тексти наукові OR публіцистичні

тексти наукові | публіцистичні

(обидва запити однакові).

Необхідно запам'ятати, що запити в Google не чутливі до регістру! Тобто запити *Острів Гренландія* і *острів гренландія* будуть абсолютно однаковими.

***Оператор "Плюс" (+)*:**

Трапляються ситуації, коли треба зробити наголос на одне або декілька слів в пошуковому запиті (показати, що ці слова найбільш важливі). Тоді перед цими словами ставлять оператор "Плюс" (+).

Наприклад:

Газета +Голос України

Рівняння Бернуллі +математика

***Виключення слів із запиту. Логічне «НЕ» (-)*:**

Як відомо, інформаційне сміття часто зустрічається при складанні запиту. Щоб його видалити, стандартно використовуються оператори виключення – логічне «НЕ». У Google такий оператор представлений знаком «мінус». Використовуючи цей оператор, можна виключати з результатів пошуку ті сторінки, які містять в тексті певні слова. Використовується, як і оператор "+", перед словом (або словами), що виключається.

Наприклад:

Мертві душі –роман

UserandLinux часопис +грудень –листопад –жовтень -вересень

***Пошук точної фрази ("")*:**

Шукати точно співпадаючу фразу на практиці потрібно або для пошуку певного твору за відомою цитатою, або для пошуку певних продуктів чи компаній, в яких назву або частину опису складає фіксоване словосполучення, що стабільно повторюється. Для того, щоб вдало виконати таке завдання за допомогою Google, потрібно взяти точно співпадаючу частину запиту у лапки (мається на увазі розділовий знак – подвійні лапки).

Наприклад:

Драма-феєрія "Лісова пісня"

"Ти признайся мені, Звідки в тебе ті чари"

***Будь яке слово (*)*:**

Іноді потрібно шукати інформацію за допомогою фіксованого словосполучення слів (береться в лапки), в якому невідомі одне або декілька слів. Для такої мети замість невідомих слів використовується оператор "*". Тобто "*" – це будь-яке слово або група слів.

Наприклад:

"Національний академічний театр опери та *"

"Леонардо * Вінчі"

***Оператор cache*:**

Пошукова машина зберігає версію тексту, яка проіндексована пошуковим павуком, в спеціальному інформаційному сховищі Google, званому кешем. Кешовану версію сторінки можна витягнути, якщо оригінальна сторінка недоступна (наприклад, не працює сервер, на якому вона зберігається). Кешована сторінка показується в тому вигляді, в якому вона зберігається в базі даних пошукової машини і супроводжується написом нагорі сторінки про те, що це сторінка з кеша. Там же міститься інформація про час створення кешованої версії. На сторінці з кеша ключові слова запиту підсвічуються, причому кожне слово для зручності користувача підсвічується своїм кольором. Можна створити запит, який відразу видаватиме кешовану версію сторінки з певною адресою: cache:адреса_сторінки, де замість "адреса_сторінки" – адреса збереженої в кеші сторінки.

Якщо потрібно знайти в кеш-сторінці певну інформацію, треба після адреси сторінки через пробіл написати запит цієї інформації.

Наприклад:

cache:www.navs.edu.ua

Треба пам'ятати, що пробілу між ":" і адресою сторінки бути не повинно!

***Оператор filetype*:**

Як відомо, Google індексує не тільки html сторінки. Якщо, наприклад, знадобилося знайти яку-небудь інформацію у відмінному від html типі файлу, можна скористатися оператором filetype, який дозволяє шукати інформацію в певному типі файлів (html, pdf, doc, rtf...).

Наприклад:

Специфікація html filetype:pdf

Твори filetype:rtf

***Оператор site*:**

Цей оператор обмежує пошук конкретним доменом або сайтом. Тобто, якщо зробити запит: *розшук осіб site:mvs.gov.ua*, то результати будуть отримані із сторінок, що містять слова "розшук" і "осіб" саме на сайті "mvs.gov.ua ", а не в інших сайтах Інтернету.

Наприклад:

Кібервійни site:book.ua

Афоризми відомих українців site:knigoland.com.ua

***Оператор link*:**

Цей оператор дозволяє побачити адреси всіх сайтів, які посилаються на сторінку, щодо якої зроблено запит. Так, запит link:www.google.com видає сторінки, в яких є посилання на google.com.

Наприклад:

link:www.comfy.ua

Ноутбуки link:www.moyo.ua

***Оператор allintitle*:**

Якщо запит почати з оператора allintitle, що перекладається як "все в заголовку", то Google видає тексти, в яких всі слова запиту містяться в заголовках (всередині тегу TITLE в HTML).

Наприклад:

allintitle:Безкоштовний софт

allintitle:Скачати книги

***Оператор intitle*:**

Показує сторінки, в яких тільки те слово, яке стоїть безпосередньо після оператора intitle, міститься в заголовку, а решта всіх слів запиту може бути в будь-якому місці тексту.

Якщо поставити оператор intitle перед кожним словом запиту, це буде еквівалентно використанню оператора allintitle.

Наприклад:

Програми intitle:Скачати

intitle:Безкоштовно intitle:скачати софтвер

***Оператор allinurl*:**

Якщо запит починається з оператора allinurl, то пошук обмежений тими документами, в яких всі слова запиту містяться в адресі сторінки, тобто в url.

Наприклад:

allinurl:ukr програми

allinurl:books statistika

***Оператор inurl*:**

Слово, яке розташовано безпосередньо після оператору inurl (без пробілу між ними), буде знайдено тільки в адресі сторінки Інтернету, а решта слів – в будь-якому місці такої сторінки.

Наприклад:

inurl:books скачати

inurl:ukr excel

***Оператор related*:**

Цей оператор описує сторінки, які "схожі" на якусь конкретну сторінку. Так, запит related:www.google.com видає сторінки з схожою з Google тематикою.

Наприклад:

related:epicentrk.ua

related:www.foxtrot.com.ua

***Оператор define*:**

Цей оператор виконує роль своєрідного тлумачного словника, що дозволяє швидко отримати визначення того слова, яке введене після оператора.

Наприклад:

define:юрист

define:кібербезпека

***Оператор пошуку синонімів (~)*:**

Якщо ви хочете знайти тексти, що містять не тільки Ваші ключові слова, але і їх синоніми, то можна скористатися оператором "~" перед словом, до якого необхідно знайти синоніми.

Наприклад:

Види ~діаграм

~Об’єктне орієнтування

***Оператор діапазону (..)*:**

Для тих, кому доводиться працювати з цифрами, Google дав можливість шукати діапазони між числами. Для того, щоб знайти всі сторінки, що містять числа в якомусь діапазоні «від, - до», треба між цими крайніми значеннями поставити дві крапки (..), тобто, оператор діапазону.

Наприклад:

Купити книгу $100..$150

Чисельність населення 1913..1935

Оператор регіону (:):

Дозволяє шукати потрібні сторінки в певному регіоні (домені).

Наприклад:

“чисельність населення” +:ua

Пошук в соціальних мережах (@):

Введіть перед словом символ @

Наприклад: @Facebook

Пошук цін ($):

Введіть перед вартістю символ $.

Наприклад: смартфон $400

Пошук по хештегам (#):

Хештеги використовуються в соціальних мережах. Для пошуку певного хештегу введіть перед словом символ #.

Наприклад: #інформаційне право

2.2. Основні інструменти OSINT для пошуку та моніторингу потрібної інформації

OSINT (open source intelligence – розвідка відкритих баз даних) в цілому можна визначити як розвідку інформації, отриманої із загальнодоступних джерел, яка не потребує таємних методів збору. Термін «OSINT» є відносно уніфікованим у міжнародній спільноті, який розуміється всіма однаково [27].

OSINT – унікальна технологія, що дозволяє збирати, аналізувати інформацію з усього Інтернет-простору. За її допомогою можна дізнаватися інформацію про компанії, людей за різними критеріями, такими як контактні дані, місце проживання, найменування організації, ім’я, посада та ін. Незамінні Open Source Intelligence Techniques інструменти у сфері кібербезпеки – пентестери або кіберзлочинці з публічних даних складають портрет потенційної жертви.

Основними джерелами розвідки є Інтернет (соцмережі, блоги, відеохостинги, форуми), журнали, газети, ТБ, радіо, публічні матеріали держструктур, загальнодоступні спостереження, звіти, статті, доповіді, конференції.

OSINT відзначалася ефективністю ще з початку свого існування. У 1941-1942 роках суть технології полягала у вирізанні фотографій парадів із німецьких друкованих видань. Потім через збільшувальне скло фахівці рахували кількість кулеметів на фото, аналізували розповіді місцевих мешканців. Пізніше змогли визначати ситуацію у вищих ешелонах влади СРСР щодо того, які особи перебували на трибуні Мавзолею. У наш час принципи роботи залишилися ті ж, але змінилися інструменти, засоби та масштаби інформації [32].

В даному розділі розглядаються тільки open source інструменти пошуку та моніторингу інформації з відкритих джерел.

Залежно від запиту можна використовувати мануальний (ручний) або автоматизований OSINT:

1) *мануальний пошук* інформації актуальний, коли потрібно проаналізувати всього кілька джерел і немає сенсу використовувати програми або виконати пошук на дуже специфічних сайтах, які не аналізуються доступними інструментами;

2) при *автоматизованому пошуку* між Вами та процесом пошуку є посередник – Ваш OSINT фреймворк (OSINT Framework: https://osintframework.com/), який являє собою лінки на різноманіття інструментів для різних задач, серед яких пошук і аналіз e-mail, пошук даних в соціальних мережах або даркнеті. Вони згруповані за категоріями в інтерактивній карті (рис. 2.1). Кликнувши на той чи інший клас, можна вийти на підклас, а в ньому – на конкретне джерело інформації. Саме OSINT фреймворк виконує пошук по сотням різних джерел, надаючи отриману інформацію. Все, що потрібно зробити користувачу – проаналізувати та структурувати її, а також зробити висновки (хоча зараз цю функцію поступово беруть на себе програми).

Всі операції можна виконувати і за допомогою пошукової машини Google, але інструменти для OSINT набагато зручніші.

Основними інструментами OSINT пошуку за відкритими джерелами є інструменти для:

- збору інформації;
- аналізу та візуалізації;
- моніторингу появи нової інформації де-небудь (корисно, якщо Ви використовуєте соцмережі для спостереження, а об'єкт Вашого спостереження активно їх веде);
- аналіз сайтів та пошук вразливостей на серверах.

Пошук інформації засобами OSINT можна здійснювати щодо будь-якого об'єкту спостереження. Початкові дані для ідентифікації особи можуть бути абсолютно різні, починаючи з фото машини, закінчуючи якимись особистими даними. Фактично, якщо Ви знаєте реальне ім'я шуканої особи, Ви запросто її знайдете в соцмережах (за дуже рідкісним винятком), а потім Ви дізнаєтеся все про те, з ким Ваш об'єкт спостереження спілкується, де живе і т.д. Навіть якщо у профілі у мети немає жодної фотографії, але є хоч один друг, ви все одно зможете дізнатися як мінімум місце проживання, а за певних вдалих умов – все, з точністю до будинку та поверху.

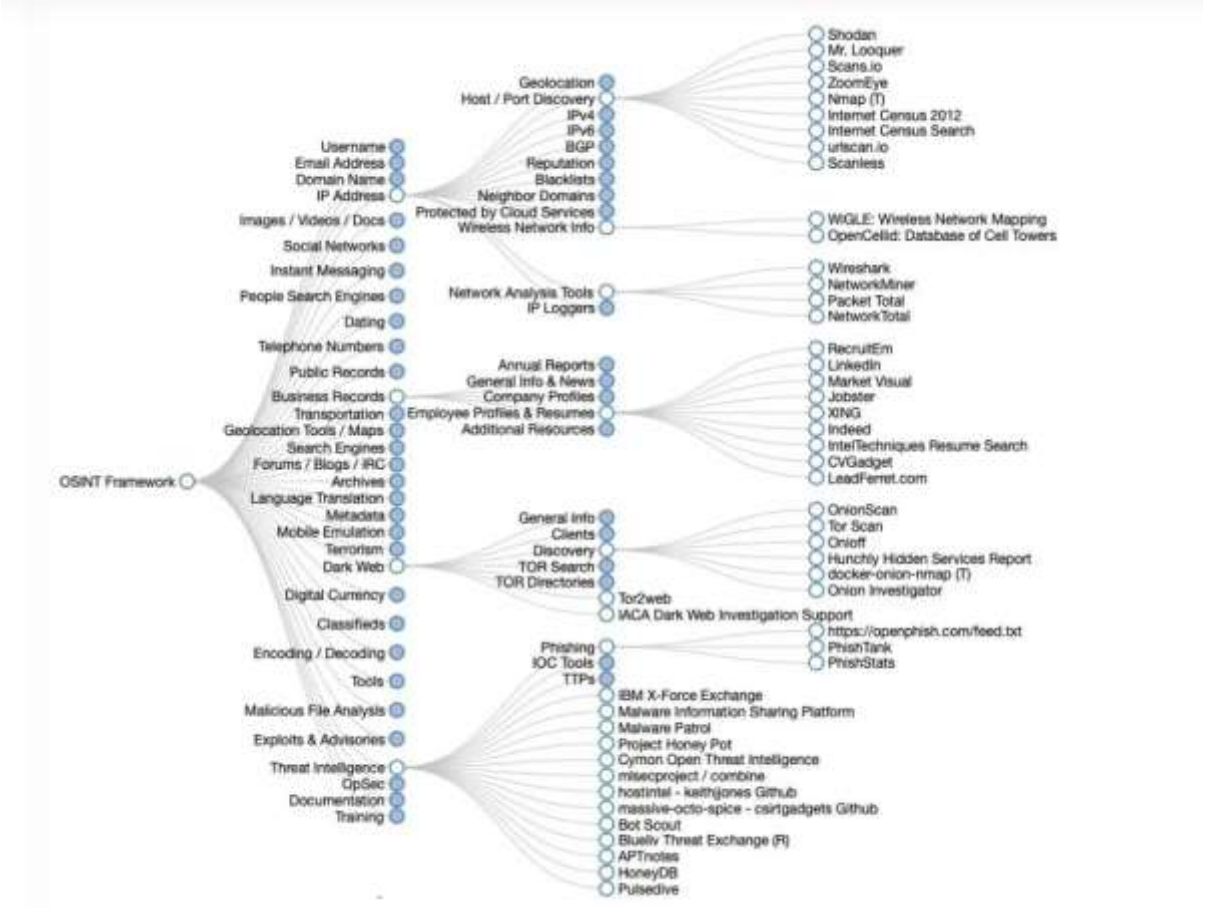


Рис. 2.1. Інтерактивна карта інструментів OSINT

Після того, як Вам стане відомий *nickname* особи спостереження хоч в одній соціальній мережі, Ви зможете спробувати знайти цю ж людину і в інших соцмережах, оскільки люди здебільшого схильні використовувати подібні *nickname* на різних сервісах.

Найбільш поширені наступні інструменти пошуку по імені та *nickname*:

• Maryam (https://github.com/saeeddhqan/Maryam) – один з найбільш функціональних інструментів пошуку. Він непогано підійде і для пошуку реального імені і для пошуку по ніку. Доступний на github.

• Snoop (https://github.com/snooppr/snoop) – це один з найшвидших і найпотужніших інструментів для пошуку за ім'ям. Він використовує близько 500 джерел збору інформації. Інструмент із відкритим вихідним кодом, проте є й платна версія, вона просто використовує більше джерел для збирання інформації.

• Alfred (https://github.com/Alfredredbird/alfred) – утиліта для збору інформації та ідентифікації облікових записів у соціальних мережах.

Пошук за зображенням дозволяє знайти людину, навіть якщо поки не знаємо її імені, але у нас є хоч одне її фото. Інструмент, яким це можна робити: search4face.com (https://search4faces.com/en/). Відносно швидко та зручно шукає людей по фото (переважно з аватарок) у різних соціальних мережах.

Також важливий пошук з визначенням місцевості, тобто, коли ми маємо кілька фотографій і нам треба дізнатися, де це знято. Тут вибір інструментів дуже великий, за фактом можна використовувати навіть банальний Google Maps, але є і зручніші інструменти:

• 2gis (https://2gis.ru/) – добре підходять для пошуку малого бізнесу, так як там відзначені навіть межі приміщень усередині будівлі, де сидить компанія;

• DualMaps (https://www.dualmaps.com/) – якщо коротко: це просто Google Maps із двох різних ракурсів та Google Street Viewer. Це може бути корисним, наприклад, якщо немає можливості використовувати другий монітор, а перемикатися між вікнами незручно;

• demo.f4map (https://demo.f4map.com/#camera.theta=0.9) – добре деталізована 3D карта. Може бути корисною, якщо треба «заглянути» в якесь подвір'я або подивитися на місто в 3D. До речі, в деяких випадках – більш детальна карта, ніж навіть Google Earth.

Щодо пошуку по Email, тут можливо застосування наступних інструментів:

• haveibeenpwned.com (https://haveibeenpwned.com/) – перевірка на наявність Email у зламаних та злитих в Інтернет базах;

• Ghunt (https://github.com/mxrch/GHunt) – пошук інформації про власника облікового запису Google.

Крім цього, у того ж Maryam (див. вище) є деякі можливості пошуку по Email.

Для пошуку за номером телефону доцільно скористатися інструментом PhoneInfoga (https://github.com/sundowndev/phoneinfoga).

Після збору інформації її треба правильно структурувати та проаналізувати. Для цього можна використовувати декілька інструментів: 1) Obsidian (https://obsidian.md/). Він непогано підходить для побудови графіків та представлення якихось знань у вигляді графів; 2) ще одна програма, аналогічна попередній за своїм функціоналом – TheBrain (https://www.thebrain.com/).

Аналіз та моніторинг соціальних мереж може бути корисним, наприклад, якщо Вам потрібно дізнатися краще коло спілкування та інтереси будь-якої особи. Тут нам можуть допомогти звичайні і прості інструменти, які шукають згадки щодо певної людини або будь-якої теми в соціальних мережах:

• Social Searcher (https://www.social-searcher.com/) – безкоштовний інструмент моніторингу соціальних мереж. Фактично це спеціальна пошукова система, яка шукає згадки про те, що їй скажуть.

• Google Alerts (https://www.google.com/alerts?hl=en) – сповіщає про появу в Інтернеті вказаної інформації. Цей інструмент можна застосувати як на себе (моніторити інформацію про себе), так і на об'єкт ваших досліджень.

Одними з ключових методів у OSINT є контент-аналіз матеріалів та статистичний аналіз джерел даних, які використовуються для систематизації та аналізу текстових, аудіо та відео матеріалів, знайдених у соціальних мережах, ЗМІ, форумах та інших відкритих джерелах. Приклад використання контент-аналізу та статистики для вивчення динаміки інформаційної агресії росії проти України наведено в [23].

2.3. Веб-скрепінг інформації з мережі Інтернет засобами Python

Веб-скрепінг за допомогою Python – це процес автоматичного збору даних з вебсайтів шляхом створення програм (скреперів), які витягують інформацію з HTML-коду сторінок. Цей процес може бути виконаний автоматично без необхідності вручну відвідувати кожний вебсайт та складати дані вручну. Web scraper може бути корисним для збору даних про ціни на товари, інформацію про нерухомість, контактну інформацію компаній та інше.

Для розробки web scraper, Ви можете використовувати будь-яку мову програмування. Проте, Python є однією з найпопулярніших мов програмування для розробки web scraper. Це через те, що Python має вбудовані бібліотеки, які дозволяють легко отримувати дані з вебсторінок. Для розробки web scraper потрібно мати базові знання з Python, HTML та CSS.

Основні кроки включають використання бібліотек, таких як **Requests**, для виконання HTTP-запитів та отримання HTML-коду сторінки, а також **BeautifulSoup** або **Scrapy** для парсингу (розбору) цього коду та вилучення потрібних даних у структурований формат.

Основні інструменти та кроки

1. **Requests:**

- Ця бібліотека використовується для надсилання HTTP-запитів до вебсайтів, зазвичай із запитом GET для отримання вмісту сторінки.
- Вона спрощує процес взаємодії з сервером порівняно зі стандартними засобами Python, як-от urllib.

2. **BeautifulSoup:**

- Бібліотека для парсингу HTML та XML документів.
- Це простий і легкий інструмент для витягання даних, який добре підходить для невеликих або простих завдань скрепінгу.
- Після отримання HTML-коду за допомогою Requests, Ви передаєте його до BeautifulSoup, щоб легко знаходити та вибирати потрібні елементи (наприклад, за тегами, класами чи атрибутами).

3. **Scrapy:**

- Це потужний фреймворк для збирання даних з вебсайтів.
- Він надає готову структуру для складніших проєктів скрепінгу, включаючи обробку запитів, обробку відповідей, зв'язування даних та їх збереження.
- Scrapy дозволяє створювати більш складні та продуктивні скрепери для обробки великих обсягів даних.

Загальний процес веб-скрепінгу

1. **Визначення цільових сторінок**: виберіть вебсайти та конкретні сторінки, з яких Ви хочете отримати дані.
2. **Отримання HTML-коду**: використовуйте бібліотеку Requests для надсилання GET-запиту на URL сторінки.
3. **Парсинг HTML**: передайте отриманий HTML-код до BeautifulSoup або іншого парсера для розбору структури.

4. **Вилучення даних**: за допомогою методів BeautifulSoup (або аналогічних у Scrapy) знайдіть та витягніть потрібну інформацію з елементів HTML (текст, посилання, атрибути).

5. **Збереження даних**: збережіть витягнуті дані у зручному форматі, наприклад, у CSV-файл, базу даних або JSON.

Важливе зауваження

Перед веб-скрепінгом завжди перевіряйте файл robots.txt вебсайту, щоб переконатися, що Ви не порушуєте його правил щодо автоматизованого доступу, та ознайомтеся з умовами використання сервісу.

2.4. Аналіз отриманих даних засобами електронних таблиць

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, що 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*:**

– **MODE.SNGL** – обчислює значення моди M_0 – значення ознаки, яка найчастіше трапляється в даній сукупності.

– **MEDIAN** – обчислює значення медіани M_e – значення ознаки, яка ділить розподіл (площу під кривою розподілу) на дві рівні частини.

– **AVERAGE** повертає середнє арифметичне своїх аргументів.

Синтаксис **AVERAGE**(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 **VAR.P** 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 **VAR.S** .

Рівняння для **VAR.P** має наступний вигляд:

$$\overline{D}_x = \frac{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2}{n^2}.$$

– **VAR.S** оцінює дисперсію за вибіркою

$$D_x = \frac{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2}{n\cdot(n-1)}.$$

– **STDEV.P** повертає значення стандартного відхилення для генеральної сукупності $\sigma_x = \sqrt{\frac{n\sum x_i^2 - \left(\sum x_i\right)^2}{n^2}}$.

– **STDEV.S** 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 **NORM.ST.DIST** повертає стандартний нормальний інтегрований розподіл, середнє значення якого дорівнює нулю і стандартне відхилення дорівнює одиниці.

Функція має синтаксис **NORM.ST.DIST(z;сукупне)**, де **z** – значення, для якого будуємо розподіл; **сукупне** – обов'язковий аргумент, може мати значення **TRUE** або **FALSE**. Це логічне значення визначає форму функції. Якщо аргумент «сукупне» має значення TRUE, то NORM.S.DIST повертає *інтегральну функцію розподілу*. Якщо значення хибне, повертається щільність *функції ймовірності*.

Рівняння щільності стандартного нормального розподілу має наступний вигляд: $f(z;0,1) = \frac{1}{\sqrt{2\pi}} e^{-\frac{z^2}{2}}$.

– Функція **NORM.DIST** повертає нормальну функцію розподілу для вказаного середнього і стандартного відхилення.

Функція має синтаксис **NORM.DIST(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 **NORM.DIST** 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)= **NORM.ST.DIST**(z) – 0,5.

– **SKEW** повертає асиметрію розподілу. Асиметрія характеризує ступінь несиметричності розподілу відносно його середнього.

$$A_s=\frac{n}{(n-1)\cdot(n-2)}\cdot\sum\left(\frac{x_i-M_x}{\sigma_x}\right)^3.$$

– **KURT** повертає ексцес розподілу, що характеризує гостровершинність (+) чи плосковершинність (-) кривої розподілу.

$$E_x=\frac{n(n+1))}{(n-1)(n-2)(n-3)}\sum\left(\frac{x_i-M_x}{\sigma_x}\right)^4-\frac{3(n-1)^2}{(n-2)(n-3)}.$$

– **BINOM.DIST** – повертає окреме значення біноміального розподілу. Функція **BINOM.DIST** 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, **BINOM.DIST** може обрахувати ймовірність того, що двоє з трьох наступних новонароджених будуть хлопчики.

Синтаксис:

BINOM.DIST(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 TRUE, то функція **BINOM.DIST** повертає інтегральну функцію розподілу, а саме ймовірність того, що кількість успішних випробувань не менш ніж значення аргументу кількість_успіхів; якщо цей аргумент має значення FALSE, то повертається функція розподілу, а саме ймовірність того, що кількість успішних випробувань точно дорівнює значенню аргументу кількість_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 **COMBIN**(n;m).

Інтегральний біноміальний розподіл має вигляд:

$$B(m;n,p) = \sum_{x=0}^{m} b(x;n,p)\,.$$

– **CONFIDENCE.NORM** – 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: **CONFIDENCE.NORM(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 «Data Analysis»: 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 **Data Analysis**, 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.

Anova (Дисперсійний аналіз). Існує декілька типів дисперсійного аналізу. Потрібний варіант вибирається з урахуванням числа факторів та наявних виборок з генеральної сукупності.

Anova:Single Factor (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).

Anova:Two-Factor With Replication (Двофакторний дисперсійний аналіз з повтореннями). Являє собою більш складний варіант однофакторного аналізу з кількома вибірками для кожної групи даних.

Anova:Two-Factor Without Replication (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.

Correlation (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:

$$\rho_{x,y} = \frac{\operatorname{cov}(X,Y)}{\sigma_X \cdot \sigma_Y}, \text{ де:}$$

$$\sigma_X = \frac{1}{n}\sum (X_j - \mu_X)^2,\ \sigma_Y = \frac{1}{n}\sum (Y_j - \mu_Y)^2.$$

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 **CORREL**.

Covariance (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:

$$\operatorname{cov}(X,Y) = \frac{1}{n}\sum (x_j - \mu_x)(y_j - \mu_y).$$

Descriptive Statistics (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.

F-Test Two-Sample for Variances (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-Test (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-Test (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.

Histogram (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.

Moving Average (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.

Rundom Number Generation (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.

Rank and Percentile (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.

Regresion (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.

Sampling (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 2.4 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 ІІ

Практичне заняття 2.1. Прогнозування засобами MS Excel

Мета заняття: навчитись здобувачам магістратури прогнозувати перебіг подій засобами програми MS Excel.

Завдання:

1. Створити в папці за допомогою програми Excel файл з назвою **Ваше прізвище_П.з. 2.1.**
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:

РОЗПОДІЛ
надзвичайних подій за наслідками серед особового складу НПУ

№ з/п	*Період*	*Наслідки надзвичайних подій:*		*Всього надзвичайних подій*	*Рівень надзвичайних подій*
		фізичних ушкоджень	*загиблих*		
1	*2*	*3*	*4*	*5*	*6*
1.	Січень	124	14		
2.	Лютий	80	26		
3.	Березень	72	18		
4.	Квітень	117	9		
5.	Травень	95	24		
6.	Червень	102	14		
7.	Липень	90	9		
8.	Серпень	48	12		
9.	Вересень	66	17		
10.	Жовтень	75	7		
	Всього (1-10):				
	Середнє (1-10):				
Прогноз на наступний період					
11.	Листопад				
12.	Грудень				
	Всього (1-12):				
	Середнє (1-12):				

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 «x» 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):».

o Для рядка «Всього (1-12):» встановити 0 десяткових розрядів у числах.

o Для рядка «Середнє (1-10):» встановити 1 десятковий розряд у числах.

o 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, але < 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 2.2. Використання інструментів OSINT

Мета заняття: ознайомитись з практичним застосуванням деяких загальнодоступних інструментів OSINT

Методичні рекомендації:

• Спробуйте провести своє розслідування. Ви можете спробувати з'ясувати інформацію про одного зі своїх знайомих і т.д. Це буде хорошим тренуванням, оскільки фактично буде справжньою справою.

• Codeby.games (https://codeby.games/) – непоганий сервіс, де, крім інших завдань, є і категорія OSINT. Є найрізноманітніші, як складні, і прості завдання.

• Osint Tasks Bot (https://t.me/osinttasksbot) – бот у телеграм, який видає та перевіряє завдання по OSINT, в основному – пошук по картах та на місцевості (працює дещо костально, але в ньому є моє улюблене – завдання на пошук по місцевості).

Завдання:

• За допомогою сервісу https://whoer.net визначте IP-адресу Вашого персонального комп'ютера та проаналізуйте загрози анонімності роботи в Інтернет.

• Перевірте наявність активованої функції WebRTC у Вашого браузера на сайті https://whoer.net або https://ipleak.net/. Які вимкнути функцію WebRTC у вашому браузері?

• Проаналізуйте відбиток Вашого браузера (browser fingerprint) на сайті https://panopticlick.eff.org

• Проведіть комплексну перевірку Вашого браузера на витоки на сайті https://browserleaks.com

• Знайдіть адресу інтернет-провайдера, на сервері якого знаходиться сайт https://2ip.ua

• Володіння якими сайтами пов'язано з власником email-адреси: urquhart@msu.edu?

• З'ясуйте, які сайти пов'язані з особою Anna Roussos

• Де знаходиться сервер IP-адреси 91.198.149.28 (країна, місто, адреса, телефони)?

• Які сайти знаходяться на даному сервері (IP-адресі)?

• Знайдіть дату реєстрації сайту antimaydan.info

• Підготуйте зашифроване повідомлення з прикріпленим будь-яким файлом на сервісі https://secserv.me/. Додайте до нього фейкове повідомлення. Змоделюйте отримання підготовленого повідомлення. Переконайтеся, що після переходу за надісланим посиланням повідомлення на сервері знищується.

• Знайдіть відповідну опцію інтернет-браузера та видаліть історію та файли кукі (Cookie).

Практичне заняття 2.3. Веб-скрепінг інформації з сайту

Мета заняття: отримати початкові навички пошуку інформації шляхом веб-скрепінгу.

Завдання: Виконати нижченаведений алгоритм веб-скрепінгу.

Алгоритм узято з джерела [31]. Він складається з наступних кроків:

1. Встановіть бібліотеку BeautifulSoup та Requests за допомогою наступного коду:

```
pip install beautifulsoup4
pip install requests
```

2. Підключіть бібліотеку BeautifulSoup та Requests до свого коду:

```
from bs4 import BeautifulSoup
import requests
```

3. Відкрийте сторінку вебсайту, з якої ви хочете отримати дані, використовуючи бібліотеку Requests:

```
url = 'https://example.com'
response = requests.get(url)
```

4. Перевірте, чи успішно здійснено запит до вебсайту:

```
if response.status_code == 200:
    print('Success!')
else:
    print('An error has occurred')
```

5. Використовуйте бібліотеку BeautifulSoup для отримання даних з вебсторінки:

```
soup = BeautifulSoup(response.content, 'html.parser')
```

Використовуйте методи бібліотеки BeautifulSoup, щоб отримати потрібні дані:

```
# Отримання заголовка сторінки
title = soup.title.text
# Отримання списку всіх посилань на сторінці
links = []
for link in soup.find_all('a'):
    links.append(link.get('href'))
# Отримання тексту з HTML тегу
paragraph = soup.find('p').text
# Отримання таблиці з HTML сторінки
table = soup.find('table')
rows = table.find_all('tr')
for row in rows:
    cells = row.find_all('td')
    for cell in cells:
        print(cell.text)
```

6. Збережіть отримані дані у відповідному форматі, наприклад, у файлі CSV:

```
import csv
# Запис даних у файл CSV
```

```
with open('data.csv', mode='w') as file:
    writer = csv.writer(file)
    writer.writerow(['Title', 'Link', 'Paragraph'])
    writer.writerow([title, links, paragraph])
```

Запустіть свій код та перевірте, чи успішно він отримує та зберігає дані з вебсайту.

Практичне заняття 2.4. Аналітичні дослідження залежності показників злочинності від певних факторів

Мета заняття: навчитись здобувачам проводити аналіз кореляційного зв'язку між двома вимірюваними змінними засобами програми MS Excel (на прикладі статистичних об'єктів «*Рівень тяжких та особливо тяжких злочинів*» та «*Зареєстрована кількість хворих на нарко-токсикоманію*»).

ТЕОРЕТИЧНІ ВІДОМОСТІ:

Дві випадкові величини X та Y можуть бути:

1) незалежними;
2) пов'язані функціональною залежністю, що реалізується рідко;
3) пов'язані залежністю іншого роду, що називається статистичною.

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*.

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** (r), який набуває значень від -1 до $+1$ включно. При цьому:

а) якщо $r > 0$, то зв'язок між X та Y є додатним, і вони зменшуються або збільшуються одночасно;

б) якщо $r < 0$, то зв'язок між X та Y є від'ємним – із збільшенням однієї з них друга зменшується або навпаки;

в) якщо $r = 0$, то випадкові величини X і Y – некорельовані.

Кореляція	Негативна	Позитивна
Відсутня	−0.09 до 0.0	0.0 до 0.09
Низька	−0.3 до −0.1	0.1 до 0.3
Середня	−0.5 до −0.3	0.3 до 0.5
Висока	−1.0 до −0.5	0.5 до 1.0

На відміну від кореляційного аналізу, який досліджує наявність і характер зв'язків між випадковими величинами X та Y – ознаками генеральної сукупності, ***регресійний аналіз*** встановлює аналітичну форму цієї залежності.

Коефіцієнт детермінації (позначається як $\mathbf{r^2}$) – статистичний показник, що використовується в статистичних моделях як міра залежності варіації залежної змінної від варіації незалежних змінних. Іншими словами, чисельно показує, яка частина варіації залежної змінної пояснена моделлю. Вказує, наскільки отримані спостереження підтверджують модель.

В умовах класичної лінійної множинної регресії, коефіцієнт приймає значення від 0 до 1. Вважається, що чим ближче коефіцієнт до 1, тим кращою є модель.

ЗАВДАННЯ:

Необхідно проаналізувати залежність для статистичних об'єктів «*Рівень тяжких та особливо тяжких злочинів»* та «*Зареєстрована кількість хворих на нарко-токсикоманію*» відповідно до даних таблиці.

Порядок виконання:

1. Створити за допомогою програми Excel файл з назвою **Ваше прізвище_П.з. 2.4**.
2. Встановити **пароль** на файл.
3. Скопіювати таблицю 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.
4. 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).
5. Заповнити поля жовтого кольору для рядків 30 (Сума:), 31 (Середнє:) та 32 (Квадрат середнього:).
6. 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:

$\sum_{i=1}^{27} X_i Y_i$ знаходиться в комірці F30; $n = 27$;

$\bar{X}$ знаходиться в комірці B31; $\bar{Y}$ знаходиться в комірці C31;

$\sum_{i=1}^{27} X_i^{\,2}$ знаходиться в комірці D30; $\bar{X}^2$ знаходиться в комірці B32;

$\sum_{i=1}^{27} Y_i^2$ знаходиться в комірці E30; $\bar{Y}^2$ знаходиться в комірці C32;

знаходження квадратного кореня: (вираз)^(1/2)

Тобто, скелет формули наступний:

=(чисельник дробу)/(вираз у знаменнику під коренем)^(1/2)

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 середн.:					
Коефіцієнт кореляції Пірсона (r)					
Коефіцієнт детермінації ($\mathbf{r^2}$):					
Коефіцієнт кореляції згідно пакету «Аналіз даних» (r)					
РЕГРЕСІЙНИЙ АНАЛІЗ					
Лінії тренду:	**Рівняння лінії тренду (регресії)**			**К-т детермінації** (r^2)**:**	
експоненціальна:					
лінійна:					
логарифмична:					
поліноміальна:					
степенева:					
ВИСНОВКИ:					

7. У рядку 34 підрахувати коефіцієнт детермінації (**r^2**).

8. 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» -> «Надстройки» -> «Перейти» -> «Доступні надстройки» 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.

9. На аркуші, що містить таблицю з даними експериментів, виділити діапазон B2:C28. Побудувати діаграму Вставка -> Рекомендовані діаграми -> **Крапкова**, 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*».

10. 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. Після чого за допомогою клавіші **Delete** видаліть отриману лінію тренду.

11. Послідовно повторюйте пункт 10 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».

12. На підставі отриманих даних заповнити поле «Висновки» в рядку 43 щодо сили та напрямку залежності між означеними показниками, яка лінія тренду найкраще її описує.

Практичне заняття 2.5. Використання логічних операторів Google для пошуку необхідної інформації

Мета роботи: отримати навички щодо використання логічних операторів Google для пошуку необхідної інформації.

Підготовка до роботи:

1. Відкрийте програму Microsoft Word.
2. Збережіть документ з ім'ям ***Прізвище_П.з. 2.5***.
3. Встановить пароль на документ.

УВАГА! Завдання складається з двох частин (Частина 1 та Частина 2)

Частина 1

Створити наступну таблицю Word. У пошуковій системі Google знайти Web-документи, які містять указані в завданні ключові слова, використовуючи мову запитів цієї системи. До таблиці записати відповіді на наступні питання:

№ з/п	***Питання***	***Формулювання запиту***	***Кількість знайдених сторінок***
1.	Знайти сторінки, які містять одночасно слова **академія** та **Київ**		
2.	Знайти сторінки, які містять точну фразу **Національна академія внутрішніх справ**		
3.	Знайти сторінки, які містять хоча б одне із слів **академія** або **НАВС**		
4.	Знайти сторінки, які містять одночасно слова **НАВС** і **Київ**, при цьому слово **НАВС** найбільш важливе		
5.	Знайти сторінки, які містять слово **НАВС**, але не містять слово **Київ**		
6.	Знайти сторінки, які містять фіксоване словосполучення слів **Проректор НАВС Станіслав**		
7.	Знайти файли типу **pdf**, які містять слово **НАВС**		
8.	Знайти файли **презентацій** на тему **крадіжка**		
9.	Знайти визначення слова **юрист**		
10.	Знайти сторінки, які містять **кіберзлочини** за **2020-2025** роки		

Частина 2

Створити наступну таблицю Word:

№ питання	***Формулювання запиту***	***Відповідь***	***URL-адреси документа, в якому знайдено відповідь***
1.			
…			
10.			

У пошуковій системі Google знайти Web-сторінки, які містять указані в завданні ключові слова, використовуючи мову запитів цієї пошукової системи.

До таблиці записати відповіді на наступні питання:

Зразок заповнення:

1.	Голова ВРУ	**Стефанчук Руслан Олексійович**	https://uk.wikipedia.org/wiki/Список_голів_Верховної_Ради_України

ПИТАННЯ:

1. Як називалась перша механічна обчислювальна машина, проект якої розробив Блез Паскаль?

2. Хто є автором поетичного рядка «Ще вруняться горді славутові кручі…»?

3. За досягнення в яких сферах людської діяльності (навести назви) надається Нобелевська премія?

4. Скільки людей помирають щороку у світі через паління?

5. Коли були сонячні затемнення в Україні в 2022 році?

6. Який космічний сигнал зареєстрував радіотелескоп «Велике вухо»?

7. Офіційні мови ООН.

8. Яка дата створення Національної академії внутрішніх справ?

9. Які попередні назви мала Солом’янська площа в м. Києві?

10. Які були назви Національної академії внутрішніх справ за останні 30 років?

РОЗДІЛ ІІІ
ЗАГАЛЬНІ ПРИНЦИПИ ВИКОРИСТАННЯ ДЕРЖАВНИХ РЕЄСТРІВ ТА ВІДОМЧИХ ІНФОРМАЦІЙНИХ СИСТЕМ ПРИ ЗДІЙСНЕННІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ ПРАВООХОРОННИМИ ОРГАНАМИ

3.1. Єдина інформаційна система МВС

Єдина інформаційна система (далі – ЄІС) МВС – це інтегрована інформаційна система, що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супроводження їх діяльності і становить сукупність взаємозв'язаних функціональних підсистем, сервісів, програмно-інформаційних комплексів, програмно-технічних та технічних засобів електронної комунікації, які забезпечують логічне поєднання та інтеграцію електронних інформаційних ресурсів єдиної інформаційної системи МВС, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію шляхом використання функціональної підсистеми єдиної інформаційної системи МВС із спеціальними функціями [10].

Мета єдиної інформаційної системи МВС – призначена для автоматизації та технологічного забезпечення обміну даними між суб'єктами єдиної інформаційної системи МВС, зокрема в інтересах національної безпеки, захисту прав та законних інтересів громадян, суспільства і держави у сферах:

1) забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку;

2) захисту державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні;

3) цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності;

4) міграції (імміграції та еміграції), зокрема протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів.

***Завдання єдиної інформаційної системи МВС*:**

1) створення єдиного інформаційного простору системи МВС та центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України (далі – КМУ) через Міністра внутрішніх справ, шляхом логічного об'єднання їх електронних інформаційних ресурсів, оптимізація процесів спільного використання технічних та програмних ресурсів;

2) інформаційна підтримка діяльності суб'єктів єдиної інформаційної системи МВС під час виконання завдань та функцій, покладених на них законодавством, з метою підвищення її ефективності;

3) створення умов для електронної взаємодії суб'єктів єдиної інформаційної системи МВС з метою оперативного виконання завдань, зокрема в інтересах національної безпеки, покладених на них законодавством, зменшення часових та фінансових витрат на адміністративно-управлінські, інформаційно-пошукові, розрахункові та аналітичні роботи, формування звітності;

4) інтеграція електронних інформаційних ресурсів єдиної інформаційної системи МВС, реєстрація суб'єктів єдиної інформаційної системи МВС в єдиній інформаційній системі МВС та надання доступу до неї.

***Функціональні підсистеми (далі – ФП) ЄІС МВС*:**

1) національна система біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства;

2) інформаційний портал Національної поліції України;

3) Єдиний державний реєстр транспортних засобів;

4) Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху;

5) система фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі;

6) інтегрована міжвідомча ІКС щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон;

7) інформаційно-комунікаційна система прикордонного контролю "Гарт-1";
інформаційно-комунікаційна система 112;

8) Електронний реєстр геномної інформації людини;

9) Єдиний реєстр осіб, зниклих безвісти за особливих обставин;

10) Єдиний реєстр зброї;

11) Система управління силами та засобами цивільного захисту;

12) інші системи, реєстри та бази (банки) даних, створені суб'єктами єдиної інформаційної системи МВС в межах реалізації владних повноважень.

Інформаційні ресурси ЄІС МВС – це визначені групи взаємозв'язаних задокументованих одиниць інформації, які формуються і об'єднуються в автоматизованих інформаційних системах суб'єктів ЄІС МВС за певними ознаками, у тому числі зазначені в Переліку пріоритетних електронних інформаційних ресурсів суб'єктів єдиної інформаційної системи Міністерства внутрішніх справ, затвердженому постановою КМУ № 1024 від 14 листопада 2018 р. [10].

Перелік пріоритетних електронних інформаційних ресурсів суб'єктів ЄІС МВС

ВСЬОГО – **34**, з них:

1. Національна поліція – **18**
2. Державна прикордонна служба – **5**
3. МВС – **4**
4. Державна міграційна служба – **3**
5. Державна служба з надзвичайних ситуацій – **2**
6. Державна судова адміністрація – **1**
7. Офіс Генерального прокурора – **1**

Пріоритетними проєктами інформатизації системи МВС України на сьогодні є:

1. Безпечна країна.
2. Система 112.
3. Модернізація електронних інформаційних ресурсів у сфері безпеки дорожнього руху.
4. Єдиний реєстр зброї.
5. Реєстр відомостей про статус особи у кримінальному провадженні та судимості.
6. Єдиний сервіс ідентифікації фізичних осіб.
7. Єдина багатозонова система цифрового радіозв'язку.
8. Єдиний державний реєстр територіальних громад.
9. Система планування та управління об'єднаними силами із забезпечення громадської безпеки та ліквідації надзвичайних ситуацій.

***Структура ЄІС МВС*:**

1) центральна підсистема (далі – ЦП);
2) функціональні підсистеми;
3) функціональні підсистеми із спеціальними функціями;
4) електронних інформаційних ресурсів суб'єктів єдиної інформаційної системи МВС;
5) транспортної мережі передачі даних;
6) центрів обробки даних, електронних комунікаційних мереж суб'єктів єдиної інформаційної системи МВС;
7) комплексних систем захисту інформації підсистем єдиної інформаційної системи МВС з підтвердженою в установленому законодавством порядку відповідністю.

Власником і розпорядником ЄІС є держава в особі МВС.

Володільцем інформації в ЦП ЄІС є МВС.

Володільцями інформації у ФП ЄІС є відповідні суб'єкти ЄІС МВС, які забезпечують захист інформації.

Користувачі ЄІС МВС – це фізичні особи та уповноважені посадові особи суб'єктів ЄІС, яким надано відповідні права доступу до інформації.

МВС визначає структурний підрозділ апарату Міністерства, який забезпечує реалізацію пріоритетних напрямів інформатизації системи МВС та центральних органів виконавчої влади, діяльність яких спрямовується і координується КМУ через Міністра внутрішніх справ (служба єдиної інформаційної системи МВС).

Інформаційна служба: 1) Департамент інформатизації МВС України; 2) Департамент інформаційно-аналітичної підтримки Національної поліції.

Історія інформаційної служби

1. Республіканський науково-дослідний інформаційний центр (17 травня 1971 року).
2. Головне інформаційне бюро (ГІБ) (1993 р.).
3. Головний інформаційний центр (ГІЦ) (1997 р.).
4. Управління оперативної інформації (1999 р.).
5. Департамент інформаційних технологій (2002 р.).
6. Департамент інформаційно-аналітичного забезпечення (2010 р.).
7. Департамент інформаційних технологій (2012 р.).
8. Департамент інформатизації (2017 р.).

Розшукові обліки МВС України *(https://wanted.mvs.gov.ua/)* розташовані на вебпорталі МВС України (рис. 3.1.).

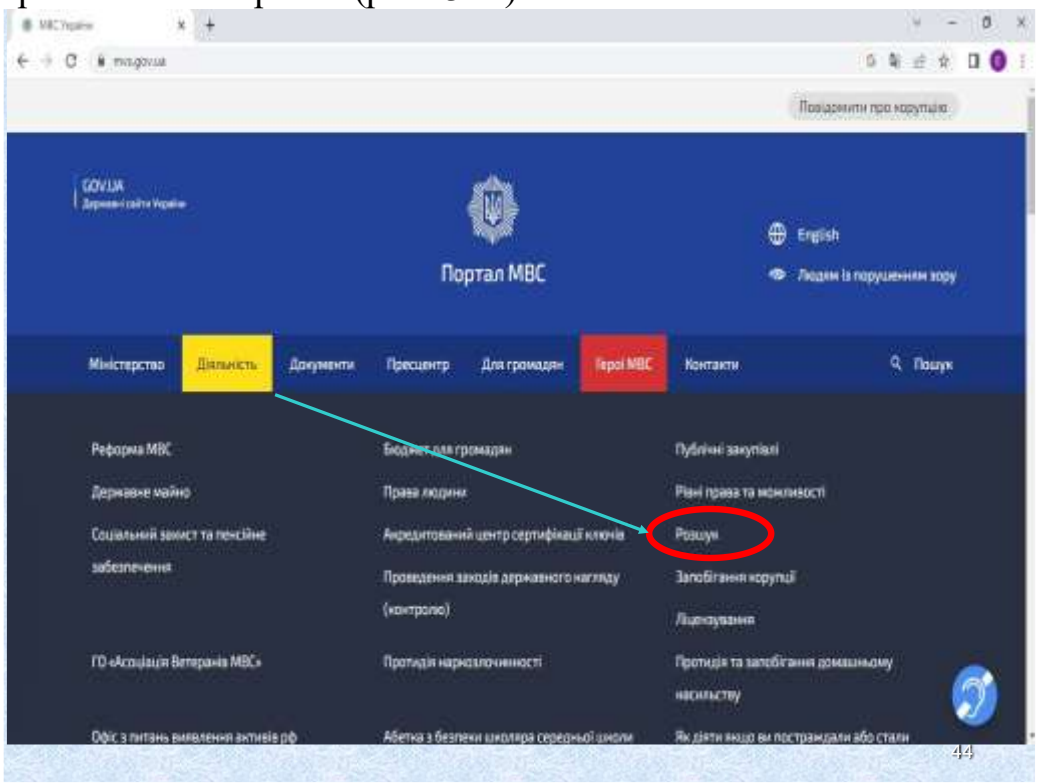


Рис. 3.1. Доступ до розшукових обліків МВС

Інформація в розшукових обліках складається з категорій (рис. 3.2.):

1. Пошук паспорта громадянина України серед викрадених та втрачених.
2. Особи, які переховуються від органів влади.
3. Зниклі громадяни та діти.
4. Особи, що не можуть надати про себе відомостей внаслідок хвороби або неповнолітнього віку.
5. Неопізнані трупи.
6. Мобільні телефони.
7. Транспортні засоби у розшуку.
8. Зброя у розшуку.
9. Культурні цінності.
10. Перевірка витягу з Єдиного реєстру осіб, зниклих безвісти за особливих обставин.

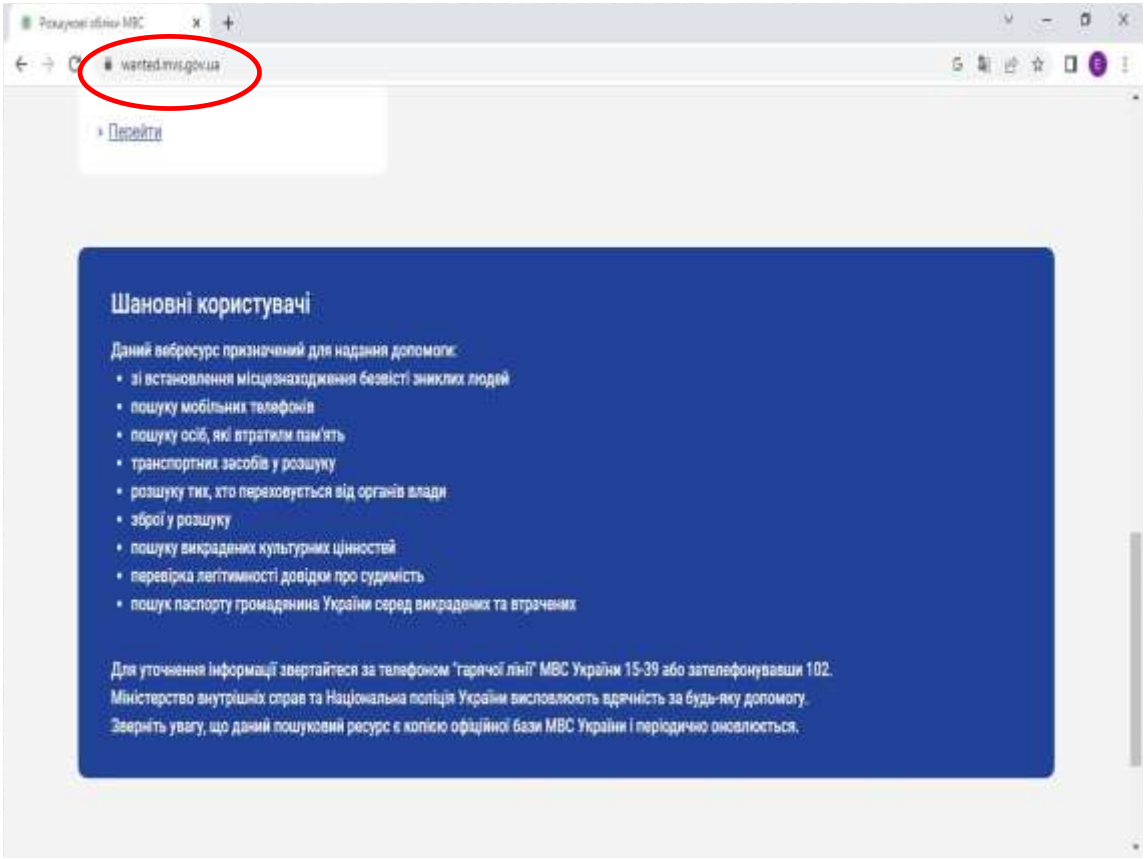


Рис. 3.2. Розшукові обліки на вебпорталі МВС

Примітка: раніше також був доступним на вебпорталі облік «Перевірка легітімності довідки про судимість».

3.2. Система інформаційного забезпечення Національної поліції

Система інформаційного забезпечення (далі – СІЗ) Національної поліції – це сукупність інформаційних підсистем певних обліків, побудованих з урахуванням дотримання таких вимог:

1) наявності нормативно-правової бази;

2) організаційно-кадрового забезпечення інформаційних підрозділів;

3) організації підготовки та перепідготовки кадрів;

4) наявності відповідних технічних, програмних та електронних комунікаційних технологій;

5) матеріально-технічного та фінансового забезпечення.

Мета СІЗ – всебічна інформаційна підтримка практичної діяльності органів Національної поліції у боротьбі зі злочинністю.

***Завдання СІЗ*:**

1. Забезпечення можливості оперативного отримання інформації у повному, систематизованому та зручному для користування вигляді.

2. Збір, обробка та узагальнення інформації для оцінки ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях управління.

3. Забезпечення усіх динамічної та ефективної інформаційної взаємодії органів НПУ, інших правоохоронних органів та державних установ.

4. Забезпечення захисту інформації.

***Принципи побудови інформаційних підсистем*:**

1. Функціонального призначення.
2. Нормативно-правової забезпеченості.
3. Фактичності даних.
4. Доцільності впровадження та експлуатації.
5. Нарощення та розвитку.

***Основні види обліків*:**

1. Оперативного призначення.
2. Експертно-криміналістичного призначення.
3. Статистичного та аналітичного призначення.
4. Адміністративного (управлінського) та загального призначення.

***Інформація оперативних обліків*:**

1. Облік осіб і їх характеристик.
2. Облік подій.
3. Облік предметів та речей.

***Інформація експертно-криміналістичного призначення*:**

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

***Приклади оперативно-пошукових обліків*:**

1) дактилоскопічні обліки;
2) 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 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.

***Національна поліція має доступ до баз (банків) даних*:**

1. Єдиної інформаційної системи Міністерства внутрішніх справ України.
2. Інших органів державної влади України.
3. Генерального секретаріату Інтерполу.
4. Інших інформаційних ресурсів.

3.2.1. 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» [7].

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

1) формує бази (банки) даних, що входять до єдиної інформаційної системи 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» [7].

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» [7]. Поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних» [5].

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 [7], фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій Міністерства внутрішніх справ України.

3.2.2. Відкриті бази даних на вебпорталі Національної поліції

На вебпорталі Національної поліції України наявні різні інформаційні системи, але доступ до більшості з них є обмеженим і надається лише авторизованим користувачам (посадовим особам поліції) після реєстрації. Це пов'язано з тим, що ці бази даних містять конфіденційну інформацію, яка належить до державних інформаційних ресурсів і не підлягає поширенню без законних підстав.

Деякі бази мають відкритий доступ для громадян (рис. 3.3).

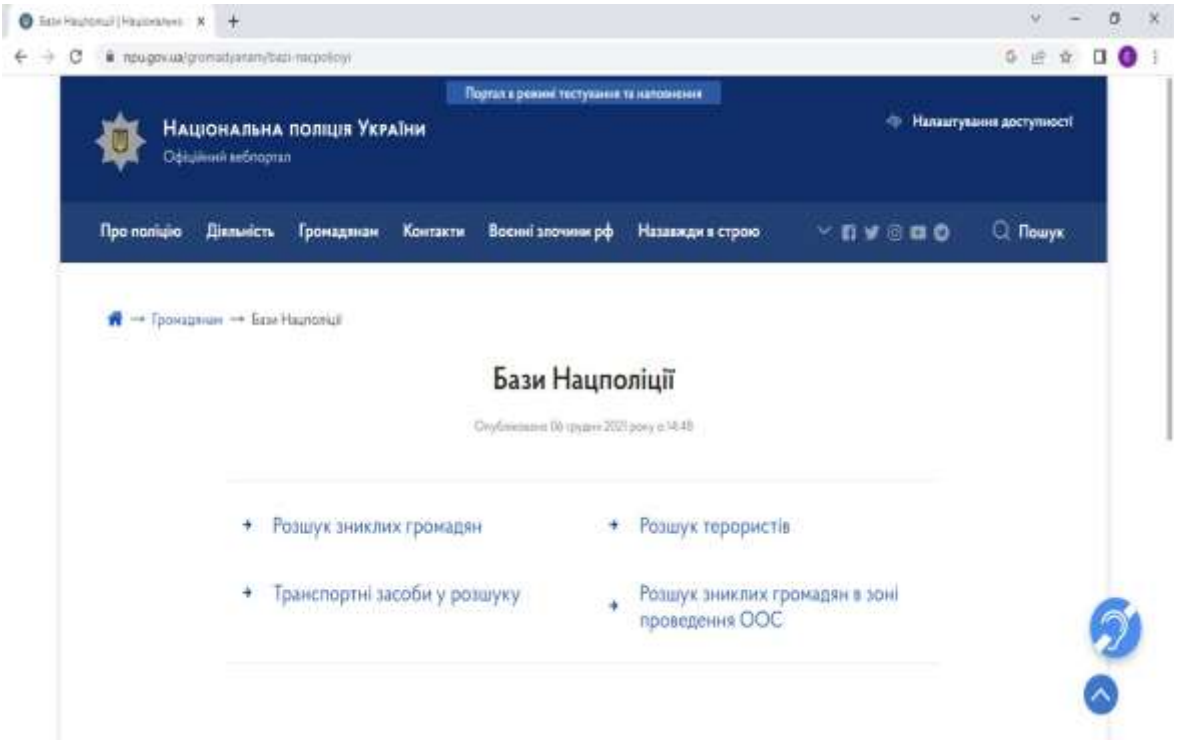


Рис. 3.3. Бази даних на вебпорталі Національної поліції України

3.3. Загальні характеристики інформаційно-комунікаційної системи ІПНП

Інформаційно-комунікаційна система «Інформаційний портал Національної поліції України» (далі – система ІПНП) – це сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності НПУ та її інформаційно-аналітичного забезпечення. Система ІПНП є складовою частиною єдиної інформаційної системи МВС України [13].

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. 3.4 відображена структура інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», на рис. 3.5 – взаємодія ІПНП з деякими Центральними органами виконавчої влади, на рис. 3.6 – взаємодія ІПНП з деякими державними електронними інформаційними ресурсами.

Рис. 3.4. Структура інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»

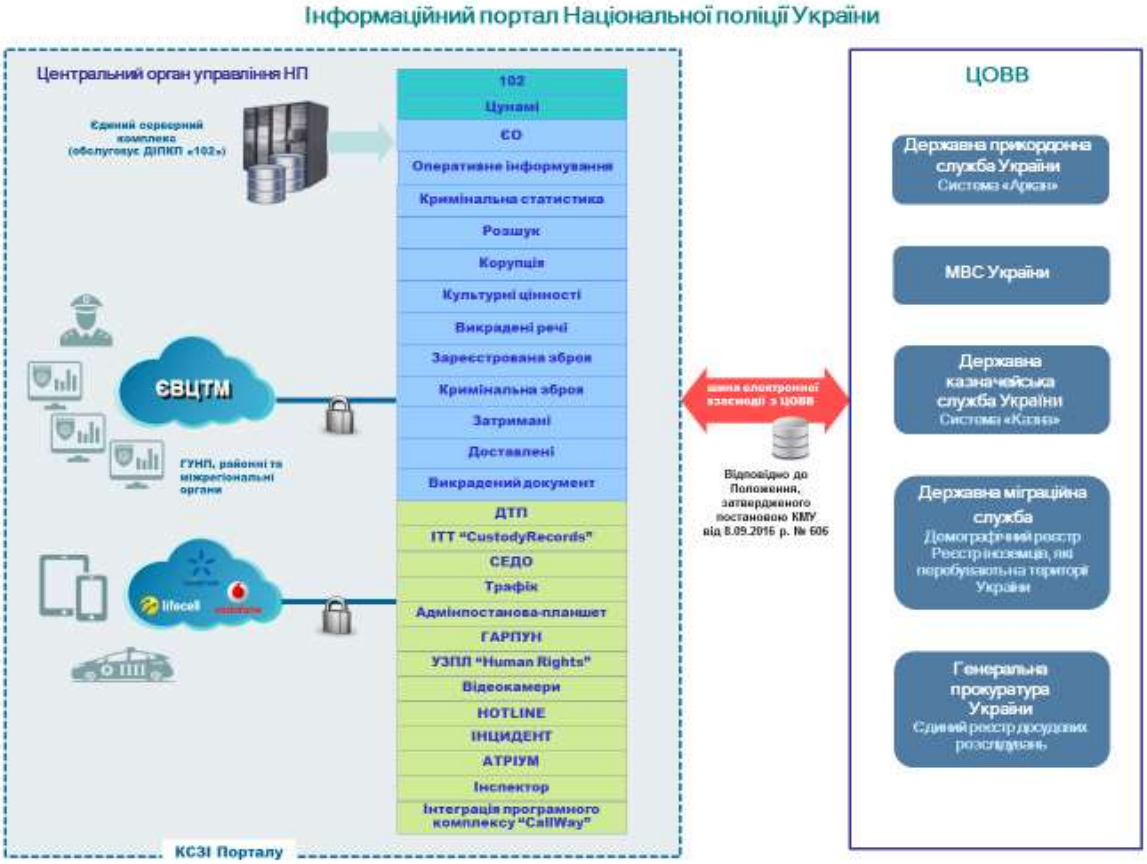


Рис. 3.5. Взаємодія ІПНП з деякими центральними органами виконавчої влади

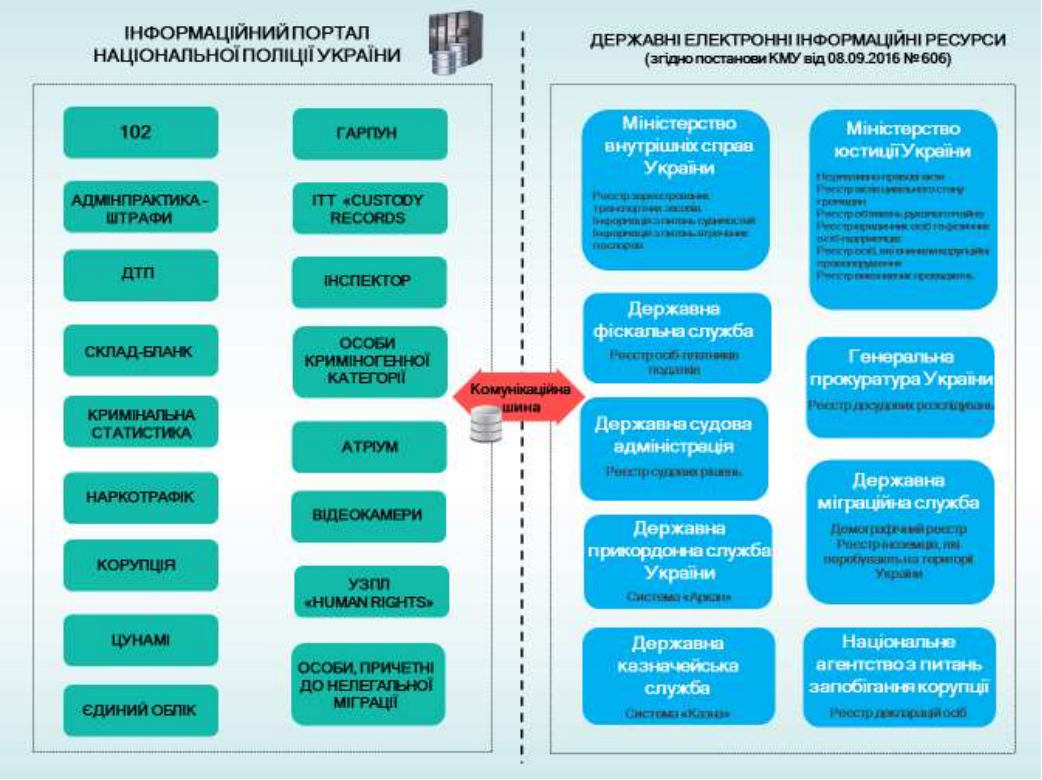


Рис. 3.6. Взаємодія ІПНП з деякими державними електронними інформаційними ресурсами

В межах інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» реалізовано доступ до електронних кабінетів окремих категорій працівників Національної поліції (рис. 3.7).

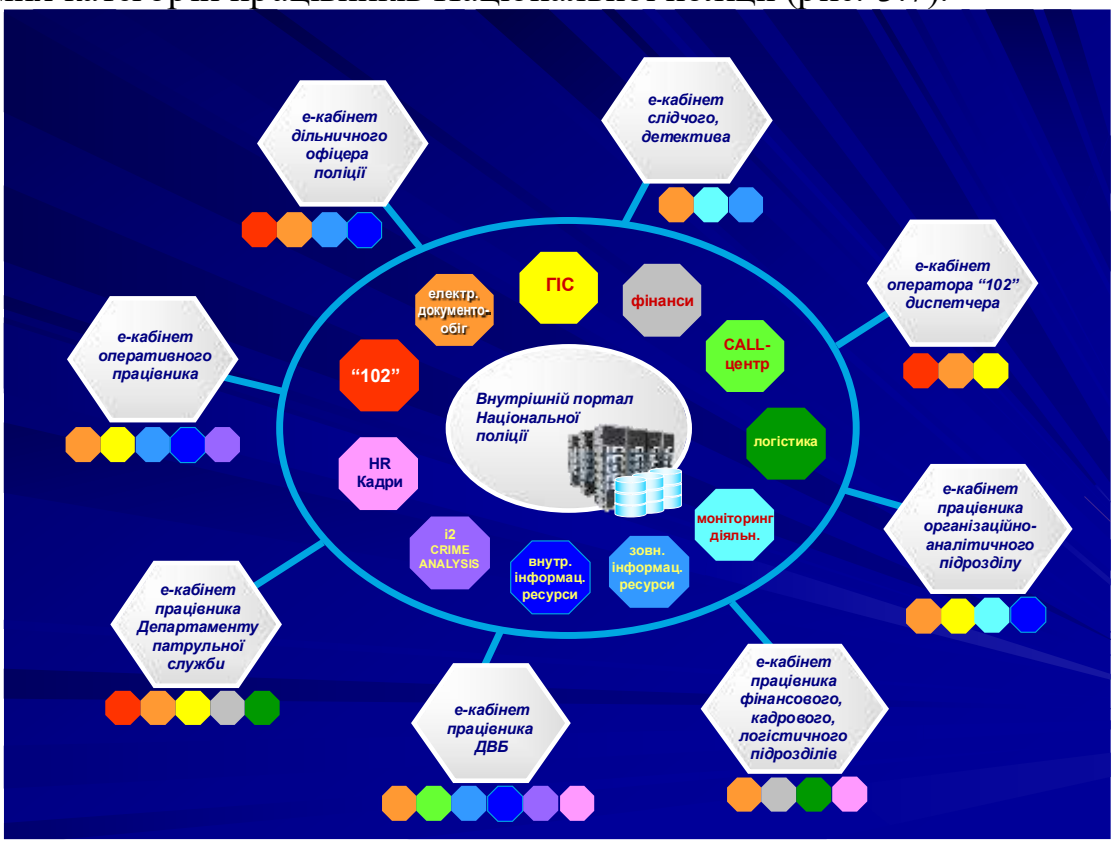


Рис. 3.7. Електронні кабінети окремих категорій працівників НПУ

Зокрема, функціональні можливості електронного кабінету дільничного офіцера поліції відображено на рис. 3.8.

Рис. 3.8. Функціональні можливості електронного кабінету дільничного офіцера поліції

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

Відповідно до законодавства 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» [12].

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. 3.9).

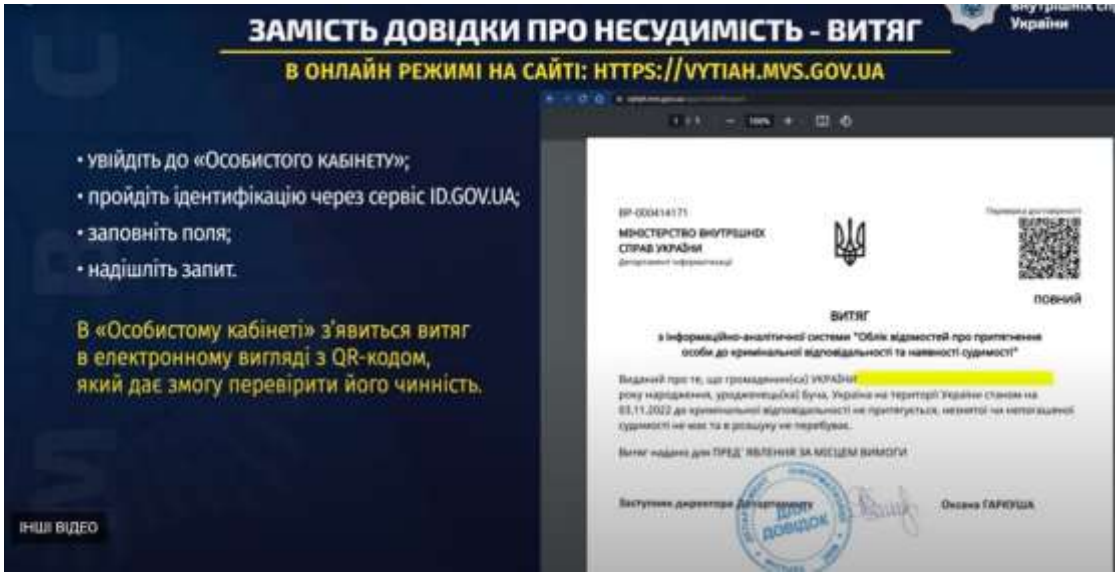


Рис. 3.9. Інформаційне повідомлення щодо порядку отримання витягу з ІАС

3.5. Реєстри вебпорталу Міністерства юстиції України

У правозастосовній діяльності можна також використовувати можливості низки реєстрів вебпорталу Міністерства юстиції України (рис. 3.10, 3.11).

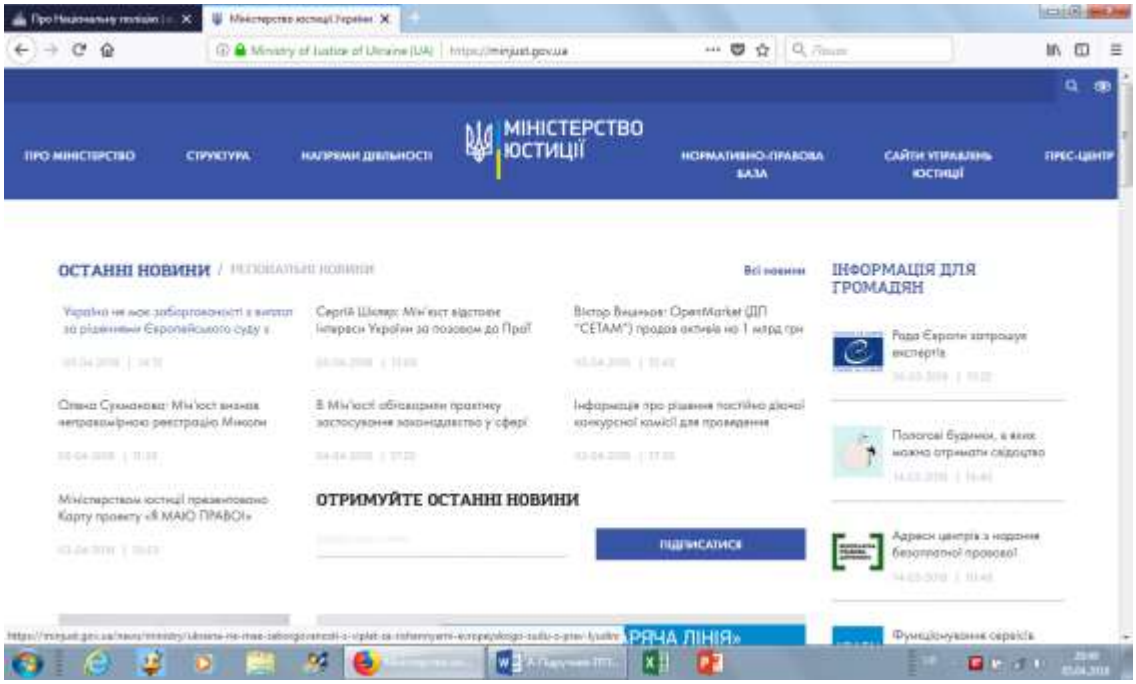


Рис. 3.10. Вебпортал Міністерства юстиції України (https://minjust.gov.ua/)

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».

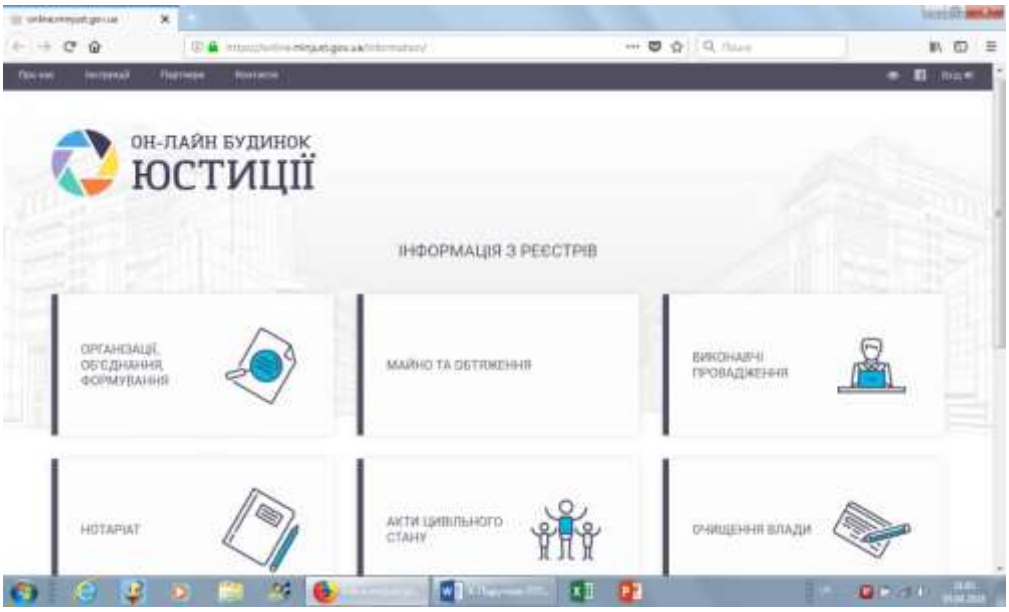


Рис. 3.11. Онлайн будинок юстиції

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

3.6. Єдиний державний реєстр судових рішень

Єдиний державний реєстр судових рішень – це автоматизована система збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень (рис. 3.12).

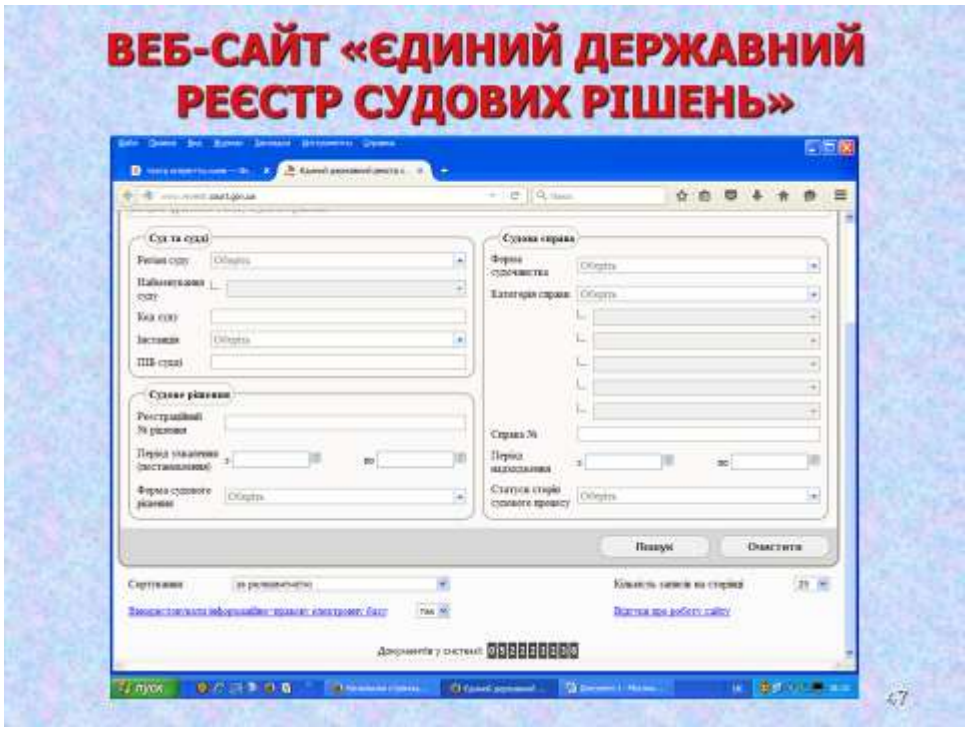


Рис. 3.12. Головна вебсторінка вебпоралу ЄДРСР (http://www.reyestr.court.gov.ua)

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 [4].

База даних ЄДРСР містить інформацію *довідкового характеру*, яка станом на 29.11.2025 містить 130 063 288 документів.

3.7. 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 Кримінального процесуального кодексу (далі – КПК) України [2] та законодавства, яким врегульовано питання захисту персональних даних та доступу до інформації з обмеженим доступом [14].

ЄРДР утворений та ведеться 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;

o 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.

3.8. 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 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 Головного управління НПУ в м. Києві дозволила оператору служби заповнювати на комп'ютері формалізовану інформаційну картку 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. 3.13). 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» ІКС ІПНП, 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 Головного управління НПУ 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.

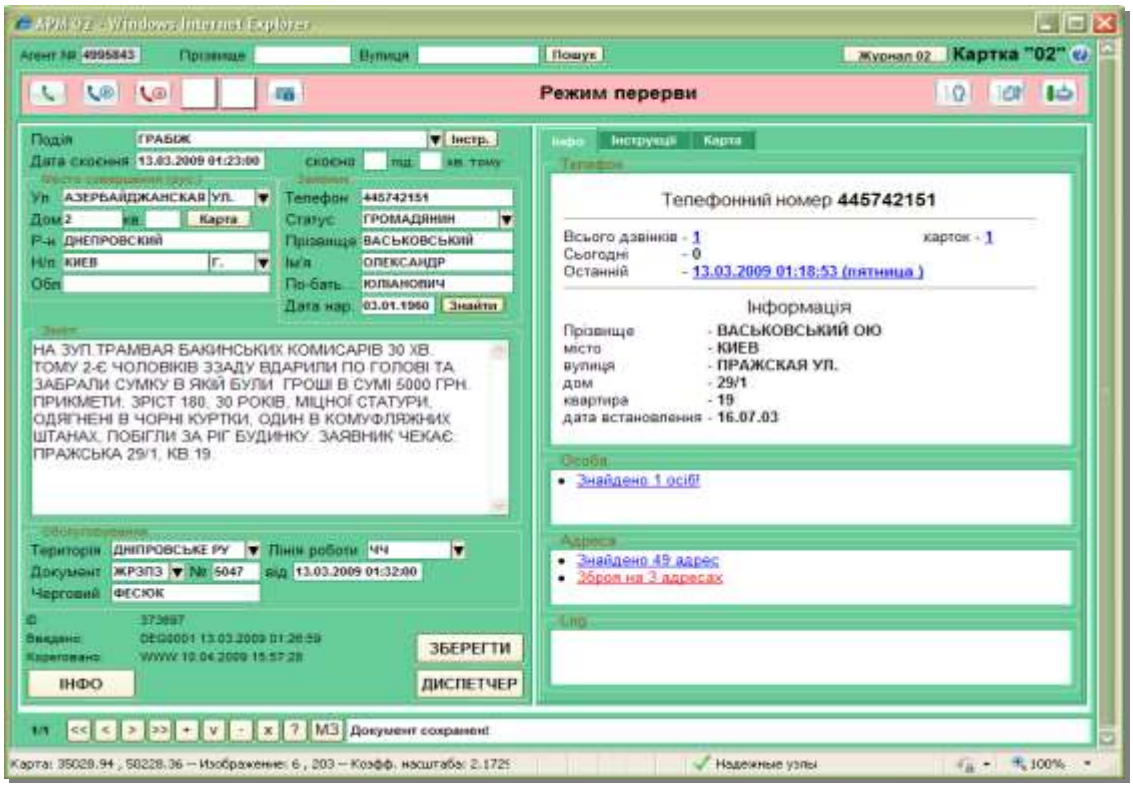


Рис. 3.13. Інформаційна картка «102»

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 диспетчерського центру (рис. 3.14).

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;

– 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.

Рис. 3.14. Диспетчерський центр управління

АРМ диспетчера ЧЧ Головного управління:

– відображає перелік подій, прийнятих оператором «102», які були вчинені в районі обслуговування (рис. 3.15);

– 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 ІПНП МВС України;

– надає повну інформацію на адресу з ІПНП МВС України;

– інформує про повторність надходження інформації про подію;

– відображає дислокацію та стан роботи патрульних нарядів (рис. 3.15);

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

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

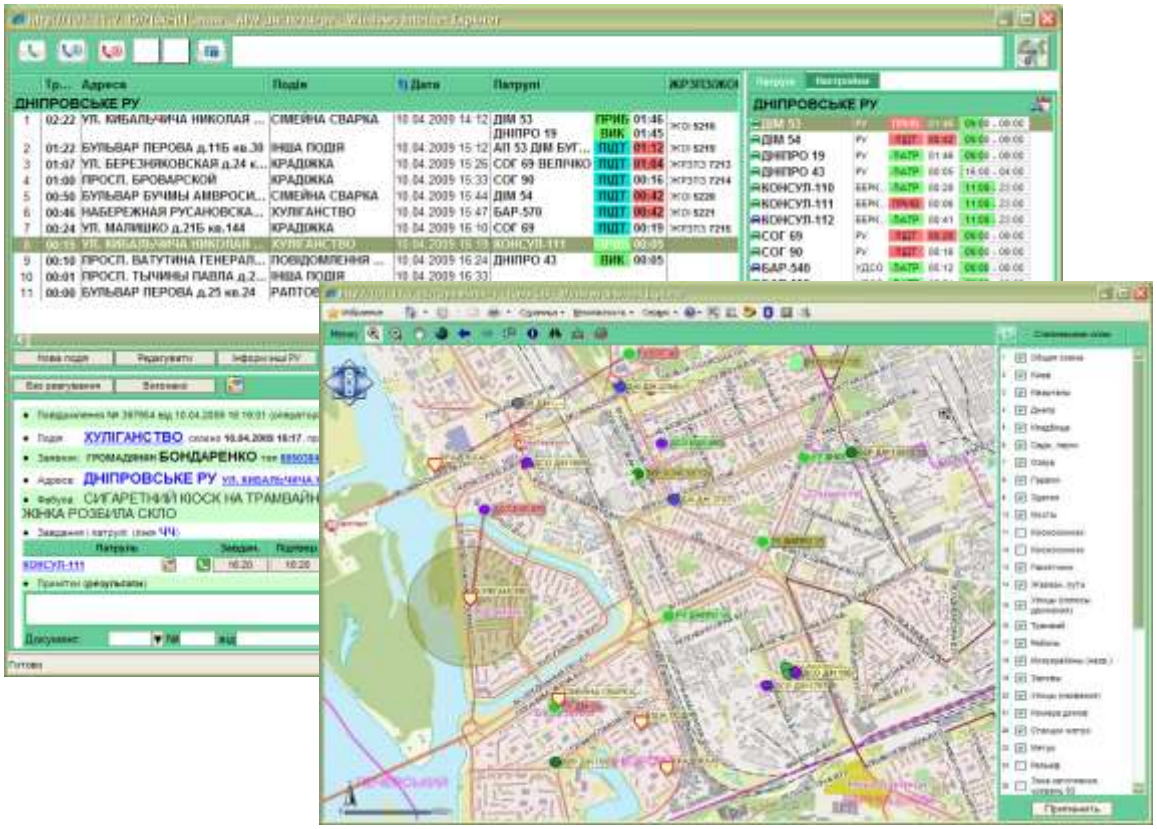


Рис. 3.15. Перелік подій, прийнятих оператором «102», дислокація та стан роботи патрульних нарядів на екранах комп'ютера АРМ диспетчера

3.9. 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 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, Міжнародної організації кримінальної поліції (далі – Інтерполу) та Європейського поліцейського офісу (далі – Європолу), а також реалізацію повноважень щодо здійснення представництва та забезпечення виконання зобов'язань України в Інтерполі та Європолі, повноважень Національної поліції України як Національного центрального бюро (далі – НЦБ) Інтерполу та Національного контактного пункту Європолу в Україні.

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 злочинності*, 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 даних «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 даних «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 даних «Криміналістика» містить відбитки пальців, профілювання ДНК і розпізнавання обличь 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 даних «*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 даних «*ДНК*» – містить профілі ДНК правопорушників, місць злочинів, зниклих безвісти та невпізнаних тіл (не зберігаються жодні номінальні дані, які пов'язують профіль ДНК з будь-якою особою).

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

4. Банк даних «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 даних «*Проїзні та ідентифікаційні документи (SLTD)*» – містить інформацію про проїзні документи та документи, що посвідчують особу, про які було повідомлено як про викрадені, втрачені, анульовані, недійсні або викрадені бланки.

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

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

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 даних «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 даних «*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 даних «*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. Вона покращує обмін інформацією та співпрацю між правоохоронними органами щодо тероризму та інших злочинів, пов'язаних із вогнепальною зброєю.

База даних «*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 даних «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 даних «*Морське піратство*». 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. 3.16. 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 ***ІКС системи Інтерполу I-24/7*** (Інтерпол 24 години на добу – 7 днів на тиждень).

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 I-24/7 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 I-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 I-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 I-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.

Питання для самоконтролю

1. Формування поліцією інформаційних ресурсів відповідно до норм Закону України «Про Національну поліцію».
2. Використання поліцією інформаційних ресурсів відповідно до норм Закону України «Про Національну поліцію».
3. Класифікація основних видів обліків Міністерства внутрішніх справ України та Національної поліції.
4. Основні правові інформаційно-пошукові системи.
5. Реєстри вебпорталу Міністерства юстиції України.
6. Поняття Єдиного державного реєстру судових рішень.
7. Загальна характеристика Єдиного реєстру досудових розслідувань.
8. Розшукові обліки на вебпорталі МВС України.
9. Поняття персонально-довідкового обліку МВС України.
10. Характеристика банків даних Генерального секретаріату Інтерполу.
11. Поняття інформаційно-комунікаційної системи Інтерполу I-24/7.
12. Загальна характеристика системи «ЦУНАМІ».
13. Характеристика Центру прийняття повідомлень – служби «102».
14. Характеристика Центра управління системи «ЦУНАМІ».
15. Поняття, основні завдання та структура інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України».
16. Перелік інформаційних підсистем ІКС ІПНП.

Практичні завдання до розділу ІІІ

Мета роботи: ознайомитись з можливостями пошуку необхідної інформації в Єдиному державному реєстрі судових рішень.

Крок 1. Створити новий документ Word виконавши команду Файл-Створити-Новий документ або необхідно виконати команду Ctrl + N. Встановіть альбомну орієнтацію аркушів новоствореного документа.

Крок 2. У створеному документі дати відповіді на наступні питання у таблиці (форма таблиці в кінці):

1. Скільки документів в ЄДРСР?
2. Що таке ЄДРСР?
3. Які до ЄДРСР вносяться судові рішення?
4. Які спеціальні знаки можна використовувати при пошуку документів?
5. Які логічні оператори можна використовувати при пошуку документів?
6. Знайти судову справу за номером № 760/11149/17.
   6.1. Які номери судових рішень?
   6.2. Які форми судових рішень?
   6.3. Яка дата набрання вироком законної сили?
   6.4. Яка назва суду?
   6.5. Яке прізвище судді?
   6.6. Яка фабула злочину?
   6.7. Який вирок суду?

7. Знайти судову справу за номером № 344/3768/21.
   7.1. Який злочин вчинений на яку посадову особу?
   7.2. Який мотив був у особи, що вчинила злочин?
   7.3. Який зміст повідомлення надсилала підозрювана особа?
8. Знайти судову справу за номером № 757/47534/21-к.
   8.1. Який номер кримінального провадження в ЄРДР?
   8.2. Яку суму застави ухвалив Печерський районний суд м. Києва?
   8.3. Яку суму застави ухвалив Київський апеляційний суд?
9. Знайти судове рішення за номером № 94982742.
   9.1. Які прізвища головуючого судді та секретаря судових засідань?
   9.2. З якою інформаційно-пошуковою системою пов'язані гіперпосилання?
   9.3. Який автомобіль у позивача і де він був припаркований?
10. Знайти судове рішення за номером № 100222521.
   10.1. Яка назва та адреса суду?
   10.2. Хто відповідачі за позовом Особи 1?
   10.3. Який п. 5 рішення суду?

Крок 3. Під таблицею вставте QR-код з Вашим прізвищем.

Крок 4. Встановити пароль на документ, виконавши команду Файл-Відомості-Захист документа-Зашифрувати та встановити пароль.

Крок 5. Зберегти документ як «Ваше Прізвище – П.з. 3.1» у папці «Тема 3», виконавши команду Файл-Зберегти як.

Приклад таблиці

№ запитання	*Формулювання запитання*	*Відповідь*	*URL-адреси документа, в якому знайдено відповідь*

СПИСОК ВИКОРИСТАНИХ І РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Нормативно-правові акти України

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР // Відомості Верховної Ради України. 1996. № 30. Ст. 141.

2. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI // Відомості Верховної Ради України. 2013. № 9-10, № 11-12, № 13. Ст.88.

3. Про Бюро економічної безпеки України : Закон України від 28 січ. 2021 р. № 1150-IX // Відомості Верховної Ради України. 2021. № 23. Ст. 197.

4. Про доступ до судових рішень : Закон України від 22 груд. 2005 р. № 3262-IV // Відомості Верховної Ради України. 2006. № 15. Ст. 128.

5. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481.

6. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII // Відомості Верховної Ради України. 2018. № 31. Ст. 241.

7. Про Національну поліцію : Закон України від 02 лип. 2015 р. № 580-VIII // Відомості Верховної Ради України. 2015. № 40-41. Ст. 379.

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. Ст. 403.

9. Про рішення Ради національної безпеки і оборони України від 14 вер ес. 2020 р. «Про Стратегію національної безпеки України» : Указ Президента України від 14 верес. 2020 р. № 392/2020.

10. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів : Постанова Кабінету Міністрів України від 14 листоп. 2018 р. № 1024.

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

12. Порядок доступу до відомостей інформаційно-аналітичної системи «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості : Наказ МВС України від 30 берез. 2022 р. № 207.

13. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : Наказ МВС України від 03 серп. 2017 р. № 676.

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

15. Про затвердження Положення про інформаційно-комунікаційну систему «Автоматизована аналітична платформа» єдиної інформаційної системи МВС : Наказ МВС України від 06 жовт. 2025 р. № 677.

Навчальна та наукова література

16. Білас Х.І., Поляк С.П. Інформаційні технології у психологічному забезпеченні правоохоронної діяльності. *Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України*: матеріали наук.-практ. конф. (Львів, 20 грудня 2024 р.) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2025. С.9-11.

17. Борецька С.М., Поляк С.П. Роль біометричної ідентифікації в інформаційно-аналітичному забезпеченні безпеки України. *Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України*: матеріали наук.-практ. конф. (Львів, 20 грудня 2024 р.) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2025. С.11-13.

18. Варенко В.М. Інформаційно-аналітична діяльність : навч. посіб. Київ : Університет «Україна», 2014. 417 с.

19. Войтюк О.Р., Магеровська Т.В. Аналіз даних та надання підтримки в процесі прийняття рішень у практичній діяльності Національної поліції України. *Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України*: матеріали наук.-практ. конф. (Львів, 20 грудня 2024 р.) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2025. С.15-17.

20. Вишня В.Б., Гавриш О.С., Рижков Е.В. Основи інформаційної безпеки : навч. посібник. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с. URL: https://er.dduvs.edu.ua/bitstream/123456789/4206/1/Основи%20інформаційної%20безпеки%20навчальний%20посібник%2006.2019%20%283%29.pdf

21. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 180 с. URL: https://er.dduvs.edu.ua/handle/123456789/15045

22. Калин С.П., Огірко О.І. Інструменти OSINT у сучасній освіті: перспективи та виклики. *Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України*: матеріали Науково-практичної конференції (Львів, 20 грудня 2024 р.) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2025. С.43-46.

23. Кудінов В.А., Корнейко О.В., Пакриш О.Є. Інформаційна агресія росії проти України: динаміка та вплив на цивільне населення. Юридичний науковий електронний журнал. 2025. № 8. С. 372-378. URL: https://doi.org/10.32782/2524-0374/2025-8/76 (дата звернення: 22.11.2025).

24. Латковський П.П. Інформаційно-аналітичне забезпечення правоохоронної діяльності. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. № 90. С.453-458. URL: https://doi.org/10.24144/2307-3322.2025.90.5.61

25. Обробка та аналіз за допомогою MS Excel та IBM i2 Analyst's Notebook інформації щодо одночасного перетину кордону декількома особами [Текст] : практ. посіб. / В. Школьніков та ін. Київ : Вид-во Нац. акад. внутр. справ, 2020. 144 с.

26. Сучасні інформаційні технології в юридичній діяльності [Текст] : навч. посіб. / О. В. Корнейко та ін. Київ : Нац. акад. внутр. справ, 2024. 205 с.

27. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Видавництво «Юридика», 2024. 180 с.

28. Шевчук В.М. Роль технології штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки та обороноздатності України. Юридичний електронний журнал. 2024. №6. С.356-361. URL: https://doi.org/10.32782/2524-0374/2024-6/88 (дата звернення: 22.11.2025).

29. Zemlyanko U.V., Zamula A.A., Tkach A.A. та ін. Principles and order of developing complex information security systems in information and telecommunication systems. *Applied Radio Electronics*. 2010. Vol. 9. № 3. P. 460-469.

Інтернет-ресурси

30. Іванина Р., Е. Клюєв. Як працює пошукова система Google: основні принципи. URL: https://elit-web.ua/ua/blog/kak-rabotaet-poiskovik-google (дата звернення: 22.11.2025)

31. Повний посібник з веб-скрепінгу. URL: https://www.rapidseedbox.com/uk/blog/web-scraping (дата звернення: 22.11.2025).

32. Топ-10 кращих інструментів OSINT для розвідки з відкритим вихідним кодом. URL: https://softlist.com.ua/ua/news/top-10-luchshykh-ynstrumentov-osint-dlia-razvedki-s-otkrytym-ishodnym-kodom (дата звернення: 22.11.2025)

33. Як захиститися від dos/ddos/… URL: https://habr.com/ru/companies/nixys/articles/665126/ (дата звернення: 22.11.2025)

Додаток 1

Витяг з Переліку наборів даних,
які підлягають оприлюдненню у формі відкритих даних[1]

Верховна Рада України
Інформація про пленарні засідання Верховної Ради України
Інформація про розгляд питань порядку денного Верховної Ради України
Інформація про законопроєкти, зареєстровані у Верховній Раді України Нормативно-правова база України (база даних “Законодавство України”)*
Інформація про народних депутатів України, їх активність*
Господарсько-фінансова діяльність Верховної Ради України
Адміністративно-територіальний устрій України
Інформація про присутність народних депутатів України на засіданнях профільних комітетів
Інформація про помічників-консультантів народних депутатів України
Стенограми та порядки денні пленарних засідань Верховної Ради України
Конституційний Суд України
Акти Конституційного Суду України за результатами конституційного провадження*
Перелік ухвал, прийнятих у справах, у яких конституційне провадження не завершилося
Акти Конституційного Суду України з організаційних питань
Порядки денні органів Конституційного Суду України
Інформація про конституційні подання, конституційні звернення, конституційні скарги, що надійшли до Конституційного Суду України, та стан їх розгляду
ДСА
Реквізити для сплати судового збору
Єдиний державний реєстр судових рішень*
Судова статистика (річні звіти про здійснення правосуддя місцевими та апеляційними судами)*
Перелік судів із зазначенням коду згідно з ЄДРПОУ, місцезнаходження та адрес електронної пошти
Інформація щодо стадій розгляду судових справ
Список судових справ, призначених до розгляду
Відомості про справи про банкрутство
Протоколи автоматизованого розподілу судових справ між суддями*
Звіти про автоматизований розподіл судових справ між суддями
Інформація про надходження судового збору

[1] Постанова КМУ від 21.10.2015 №835 "Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних"

Вища рада правосуддя
Рішення Вищої ради правосуддя, зокрема її органів (з фіксацією результатів відкритого поіменного голосування, крім випадків проведення голосування у спеціальному приміщенні (нарадчій кімнаті) на підставі Закону України "Про Вищу раду правосуддя"*
Проєкти порядків денних засідань Вищої ради правосуддя (та її дисциплінарних палат)*
Інформація про автоматизований розподіл справ (зокрема дисциплінарних скарг) між членами Вищої ради правосуддя та дисциплінарними інспекторами*
Інформація про притягнення суддів до дисциплінарної відповідальності*
Реєстр повідомлень суддів про втручання у здійснення правосуддя*
Інформація про склад Конкурсної комісії з добору кандидатів на посаду членів Вищої кваліфікаційної комісії суддів України
Інформація про склад Конкурсної комісії для проведення конкурсу на зайняття посади керівника служби дисциплінарних інспекторів Вищої ради правосуддя та його заступника, дисциплінарного інспектора Вищої ради правосуддя
Протоколи Конкурсної комісії з добору кандидатів на посаду членів Вищої кваліфікаційної комісії суддів України
Протоколи Конкурсної комісії для проведення конкурсу на зайняття посади керівника служби дисциплінарних інспекторів Вищої ради правосуддя та його заступника, дисциплінарного інспектора Вищої ради правосуддя
Проєкти порядків денних засідань Конкурсної комісії з добору кандидатів на посаду членів Вищої кваліфікаційної комісії суддів України
Проєкти порядків денних засідань Конкурсної комісії для проведення конкурсу на зайняття посади керівника служби дисциплінарних інспекторів Вищої ради правосуддя та його заступника, дисциплінарного інспектора Вищої ради правосуддя
Інформація про перебіг та результати конкурсу на зайняття посади члена Вищої кваліфікаційної комісії суддів України
Інформація про перебіг та результати конкурсів на зайняття посад керівника служби дисциплінарних інспекторів Вищої ради правосуддя, його заступника, дисциплінарних інспекторів Вищої ради правосуддя
Вища кваліфікаційна комісія суддів України
Рішення Вищої кваліфікаційної комісії суддів України*
Інформація про прогнозовану кількість вакантних посад суддів на поточний рік
Інформація про кількість посад суддів у судах, у тому числі вакантних
Інформація про результати кваліфікаційного іспиту в межах процедури добору кандидатів на посаду судді*
Рейтингові списки кандидатів на посаду судді (зокрема в рамках добору та конкурсів на зайняття вакантних посад)*
Список кандидатів, зарахованих до резерву на заміщення вакантних посад суддів*
Реєстр декларацій родинних зв'язків та доброчесності*

Перелік питань, що виносяться для розгляду на засіданні Вищої кваліфікаційної комісії суддів України*
Інформація про результати кваліфікаційного оцінювання суддів*
Список суддів*
Відомості щодо ефективності здійснення судочинства суддями*
Інформація про автоматизований розподіл справ (документів) між членами Вищої кваліфікаційної комісії суддів України
Рада суддів України
Рішення з'їзду суддів України
Рішення Ради суддів України
Порядки денні з'їзду суддів України
Порядки денні засідань Ради суддів України
Інформація про склад делегатів з'їздів суддів України
Інформація про склад Ради суддів України
Офіс Генерального прокурора
Звіт про роботу прокурора
Єдиний звіт про кримінальні правопорушення
Єдиний звіт про осіб, які вчинили кримінальні правопорушення
Звіт про кримінальні правопорушення, вчинені на підприємствах, в установах, організаціях за видами економічної діяльності
Національна рада з питань телебачення і радіомовлення
Реєстр суб'єктів у сфері медіа*
Мін'юст
Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань*
Єдиний реєстр нотаріусів*
Державний реєстр атестованих судових експертів
Інформація про дійсні чи недійсні бланки з Єдиного реєстру спеціальних бланків нотаріальних документів*
Повідомлення про електронні аукціони та інша інформація про реалізацію конфіскованого та арештованого майна та їх результати, про майно для безоплатної передачі*
Реєстр методик проведення судових експертиз
Єдиний реєстр боржників, відносно яких відкрито провадження у справі про банкрутство (неплатоспроможність)*
Єдиний реєстр арбітражних керуючих України
Єдиний державний реєстр нормативно-правових актів*
Словник адміністративно-територіального устрою України
Словник вулиць населених пунктів та вулиць іменованих об'єктів
Єдиний державний реєстр осіб, щодо яких застосовано положення Закону України "Про очищення влади"
Інформація з автоматизованої системи виконавчого провадження*
Єдиний реєстр боржників*

Дані центральної бази даних системи електронних аукціонів з реалізації арештованого майна
Єдиний реєстр приватних виконавців України
МВС
Місце розміщення стаціонарних технічних засобів (приладів контролю) системи фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі*
Перелік суб'єктів, які мають ліцензії на провадження охоронної діяльності
Перелік суб'єктів, які мають ліцензії на провадження діяльності з виробництва, ремонту, торгівлі вогнепальною зброєю невійськового призначення, боєприпасами до неї та спецзасобами
Міноборони
Інформація про втрати живої сили та техніки противника
Перелік операторів протимінної діяльності – суб'єктів господарювання і неприбуткових підприємств, установ та організацій, які мають право на провадження видів господарської діяльності у сфері протимінної діяльності та отримали сертифікат відповідності в установленому законодавством порядку
МОН
Державний реєстр наукових установ, яким надається підтримка держави
Реєстр технологій, створених чи придбаних за бюджетні кошти
Національний репозитарій академічних текстів
Реєстр наукових фахових видань України
Державний реєстр наукових об'єктів, що становлять національне надбання
Дані щодо фактичного прийому за спеціальностями у закладах вищої освіти
Дані щодо фактичного прийому за професіями у закладах професійної (професійно-технічної) освіти
Реєстр сертифікатів зовнішнього незалежного оцінювання (знеособлені дані)
Реєстр суб'єктів освітньої діяльності*
Перелік установ, які здійснювали передачу технологій
Реєстр документів про освіту (знеособлені дані)*
Реєстр студентських (учнівських) квитків (знеособлені дані) Знеособлені дані про педагогічних працівників закладів освіти
Дані про заяви вступників на вступ до закладів вищої освіти (знеособлені дані)
Звіт очної (денної) форми здобуття освіти закладу загальної середньої освіти (форма № ЗНЗ-1)
Зведений звіт очної (денної) форми здобуття освіти закладів загальної середньої освіти (форма № 76-РВК)

Мінцифри
Реєстр публічних електронних реєстрів
Реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів
Перелік офіційних вебсайтів органів державної влади*
Реєстр адміністративних послуг
Інформація про використання коштів, які надійшли на рахунок для забезпечення протидії інформаційним загрозам з боку держави-агресора
Адміністрація Держспецзв'язку
Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів, та інформації, вимога щодо захисту якої встановлена законом
Перелік суб'єктів господарювання, які мають ліцензії на провадження господарської діяльності з надання послуг у галузі технічного захисту інформації
Перелік суб'єктів господарювання, які мають ліцензію на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації
Перелік сертифікованих засобів криптографічного захисту інформації
Перелік технічних засобів, які можуть застосовуватися в електронних комунікаційних мережах загального користування
Перелік засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації
Національне агентство з питань запобігання корупції
Єдиний державний реєстр декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування*
Звіти політичних партій про майно, доходи, витрати і зобов'язання фінансового характеру
Антикорупційні програми міністерств, інших центральних органів виконавчої влади, а також інших державних органів та органів місцевого самоврядування, державних цільових фондів
Єдиний державний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення*
Результати повної перевірки декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування
Інформація про протоколи про адміністративні правопорушення, складення яких віднесено законом до повноважень Національного агентства з питань запобігання корупції
Приписи, внесені Національним агентством з питань запобігання корупції
Уповноважені підрозділи (уповноважені особи) з питань запобігання та виявлення корупції
Інформація про прийняті Національним агентством з питань запобігання корупції рішення за результатами перевірки організації роботи із запобігання і виявлення корупції в державних органах, органах влади Автономної

Республіки Крим, органах місцевого самоврядування, юридичних особах публічного права та юридичних особах, зазначених у частині другій статті 62 Закону України “Про запобігання корупції”
Результати аналізу законопроєктів, що можуть вплинути на державну антикорупційну політику чи на стан корупції в Україні
Результати антикорупційних експертиз проєктів нормативно-правових актів
АРМА
Єдиний державний реєстр активів, на які накладено арешт у кримінальному провадженні, крім даних, визначених абзацом дванадцятим частини першої статті 25 Закону України “Про Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів”
Національна поліція України
Інформація про осіб, які переховуються від правоохоронних органів*
Інформація про транспортні засоби, що перебувають у розшуку у зв’язку з їх незаконним заволодінням (включаючи ідентифікаційні номери транспортних засобів (VIN)
Дані з інформаційної підсистеми “Гарпун”*
Інформація про викрадену, втрачену зброю
Інформація про осіб, які не можуть надати про себе відомості внаслідок хвороби або неповнолітнього віку
Інформація про осіб, зниклих безвісти
Інформація про викрадені, втрачені мобільні телефони Місцезнаходження камер автоматичної фіксації швидкості руху*
Головний сервісний центр МВС
Реєстр суб’єктів проведення обов’язкового технічного контролю транспортних засобів
Інформація про заклади, що проводять підготовку, перепідготовку та підвищення кваліфікації водіїв транспортних засобів
Відомості про номерні знаки, доступні для видачі в результаті реєстрації транспортних засобів
Інформація про виявлені адміністративні правопорушення*
Карта маршрутів мобільних сервісних центрів і графік виїздів мобільних сервісних центрів
Інформація про зареєстровані транспортні засоби (включаючи ідентифікаційні номери транспортних засобів (VIN)*
Маршрути для перевірки навичок керування транспортними засобами
Дані обліку дорожньо-транспортних пригод (знеособлені дані)*
Адміністрація Держприкордонслужби
Перелік діючих пунктів пропуску через державний кордон та пунктів контролю
Інформація про перетин державного кордону України

ДСНС
Оперативна інформація про надзвичайні ситуації техногенного, природного та іншого характеру на території України
Реєстр декларацій відповідності матеріально-технічної бази суб'єктів господарювання вимогам законодавства з питань пожежної безпеки
Перелік підприємств, установ, організацій, які проводять навчання з питань пожежної безпеки
Реєстр атестованих аварійно-рятувальних служб
Адреси пунктів обігріву, розгорнутих на території України
Реєстр територій, забруднених/імовірно забруднених вибухонебезпечними предметами
Державний електронний реєстр об'єктів підвищеної небезпеки
Державний водний кадастр за розділом "Поверхневі води" у частині проведення постійних гідрометричних, гідрохімічних спостережень за кількісними та якісними характеристиками поверхневих вод
Кліматичний кадастр України
Узагальнена інформація про стан забруднення навколишнього природного середовища на території України за рік
ДМС
Дані про номер та/або серію документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус, які визнані недійсними, із зазначенням підстав визнання недійсності*
Відомості Єдиної інформаційно-аналітичної системи управління міграційними процесами
Відомості про результати моніторингу міграційних процесів
Держстат
Довідник розділів статистики
Метаописи державних статистичних спостережень
Звіти з якості
Офіційна державна статистична інформація, що поширюється відповідно до плану державних статистичних спостережень*
Статистичні класифікації, класифікатори, номенклатури, переліки кодів, довідники для проведення державних статистичних спостережень
Фінансова звітність підприємств, що складається та подається відповідно до Закону України "Про бухгалтерський облік та фінансову звітність в Україні"
Статистичні показники щодо циркулярної та низьковуглецевої економіки, що поширюються відповідно до плану державних статистичних спостережень
ДПС
Реєстр платників податку на додану вартість
Інформація про анулювання реєстрації платників податку на додану вартість
Державний реєстр реєстраторів розрахункових операцій
Реєстр великих платників податків
Реєстр платників податків – нерезидентів

Реєстр електронних форм податкових документів
Єдиний реєстр суб'єктів господарювання, які можуть здійснювати реалізацію безхазяйного майна та майна, що переходить у власність держави
Єдиний реєстр обладнання
Довідники податкових пільг, що є втратами доходів бюджету, та інших податкових пільг
Перелік типів об'єктів оподаткування
Інформація про обсяги відшкодування податку на додану вартість з державного бюджету в звітному році
Інформація про надходження податків і зборів
Інформація про нарахування податків і зборів
Інформація про суб'єктів господарювання, які мають податковий борг*
Інформація про надходження коштів єдиного внеску на загальнообов'язкове державне соціальне страхування
Показники контрольної роботи
Єдиний реєстр місць зберігання
Інформація про суми надміру сплачених грошових зобов'язань платників податків та суми платежів, які сплачені та будуть нараховані в наступних звітних періодах
Дані про податковий борг: загальна сума, сума і кількість розстрочок до року і більше року
Інформація про кількість і результати розгляду скарг за наслідками адміністративного оскарження
Інформація про щомісячні надходження податків і зборів (за видами згідно з кодом бюджетної класифікації у галузевому та регіональному розрізі)
Інформація про щомісячні відомості про надані відстрочення (розстрочення) сплати податкових зобов'язань, списання податкового боргу (за видами податків та зборів та за окремими платниками податків)
Інформація про квартальні відомості про втрати бюджету від надання податкових пільг (за видами податків та зборів)
Інформація про кількість проведених планових/позапланових перевірок та їх результати
Інформація про суми донарахувань за актами перевірок
Реєстр платників єдиного податку
Реєстр неприбуткових установ та організацій
Реєстр платників акцизного податку з реалізації пального та спирту етилового
Електронний реєстр суб'єктів господарювання, які використовують спирт етиловий для виробництва продукції хімічного і технічного призначення, парфумерно-косметичної продукції, оцту з харчової сировини
Кількість зареєстрованих підприємців - платників єдиного податку із розподілом за групами, тис. осіб
Інформація про сплату екологічного податку суб'єктами природних монополій та суб'єктами господарювання, які є платниками рентної плати за користування надрами

Фінансова звітність (звіт про фінансовий стан (баланс) та звіт про прибутки та збитки та інший сукупний дохід (звіт про фінансові результати), подані як додаток до звітної (звітної нової) податкової звітності за річний податковий (звітний) період відповідно до пункту 46.2 статті 46 Податкового кодексу України*
Реєстр заяв про розстрочення, відстрочення грошового зобов'язання чи податкового боргу
Перелік транспортних засобів, що переміщують пальне або спирт етиловий
Єдиний реєстр ліцензіатів та місць обігу пального
Інформація про платників, які мають борг (недоїмку) із сплати єдиного внеску на загальнообов'язкове державне соціальне страхування
Єдиний реєстр ліцензіатів з виробництва та обігу спирту етилового, спиртових дистилятів, алкогольних напоїв, тютюнових виробів, тютюнової сировини та рідин, що використовуються в електронних сигаретах
Держмитслужба
Перелік місць доставки
Відомчі класифікатори інформації з питань державної митної справи, які використовуються у процесі оформлення митних декларацій
Ставки ввізного та вивізного мита
Коди товарів згідно з УКТЗЕД, на переміщення яких через митний кордон України у відповідному напрямку встановлено заборону законом або міжнародним договором України, згода на обов'язковість якого надана Верховною Радою України, або відповідно до закону чи міжнародного договору України, згода на обов'язковість якого надана Верховною Радою України
Коди товарів згідно з УКТЗЕД, на переміщення яких через митний кордон України у відповідному напрямку встановлено обмеження
Реєстр підприємств, яким надано дозвіл на провадження митної брокерської діяльності
Реєстр підприємств, яким надано дозвіл на відкриття та експлуатацію митного складу
Реєстр підприємств, яким надано дозвіл на відкриття та експлуатацію складу тимчасового зберігання
Реєстр підприємств, яким надано дозвіл на відкриття та експлуатацію магазину безмитної торгівлі
Реєстр гарантів
Перелік об'єктів права інтелектуальної власності, зареєстрованих у митному реєстрі*
Інформація про взяття на облік осіб, які під час провадження діяльності є учасниками відносин, що регулюються законодавством з питань митної справи
Реєстр підприємств, яким надано дозвіл на відкриття та експлуатацію вільної митної зони комерційного або сервісного типу

Інформація про кількість іноземних транспортних засобів комерційного призначення, що в’їхали на митну територію України, в розрізі країни реєстрації
Інформація про середній час митного оформлення товарів у митних режимах експорту, імпорту, транзиту (без реагування автоматизованої системи управління ризиками)
Знеособлена аналітична інформація
Знеособлена зведена інформація для статистичних цілей
Знеособлена інформація щодо конкретних експортно-імпортних операцій, внесених декларантами до митної декларації відповідно до частини восьмої статті 257 Митного кодексу України, за винятком пунктів 2, 4, підпунктів “б”, “в”, “д”, “є”, “з” пункту 5, пунктів 6, 7 і 9 частини восьмої зазначеної статті, включаючи інформацію, що стосується митної вартості товарів
Знеособлена інформація щодо загальних питань роботи митного органу Знеособлена інформація, яка стосується правопорушень
Держфінмоніторинг
Типологічні дослідження методів та схем легалізації (відмивання) доходів, одержаних злочинним шляхом, або фінансування тероризму чи фінансування розповсюдження зброї масового знищення
Відомості про стан запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення в державі
Перелік осіб, пов’язаних з провадженням терористичної діяльності або стосовно яких застосовано міжнародні санкції*
Національне агентство із забезпечення якості вищої освіти
Перелік незалежних установ оцінювання та забезпечення якості вищої освіти
Інформація про результати акредитаційних експертиз освітніх програм
Інформація про результати інституційних акредитацій
Національна асоціація адвокатів
Єдиний реєстр адвокатів*
Рішення з’їзду адвокатів України
Рішення Ради адвокатів України

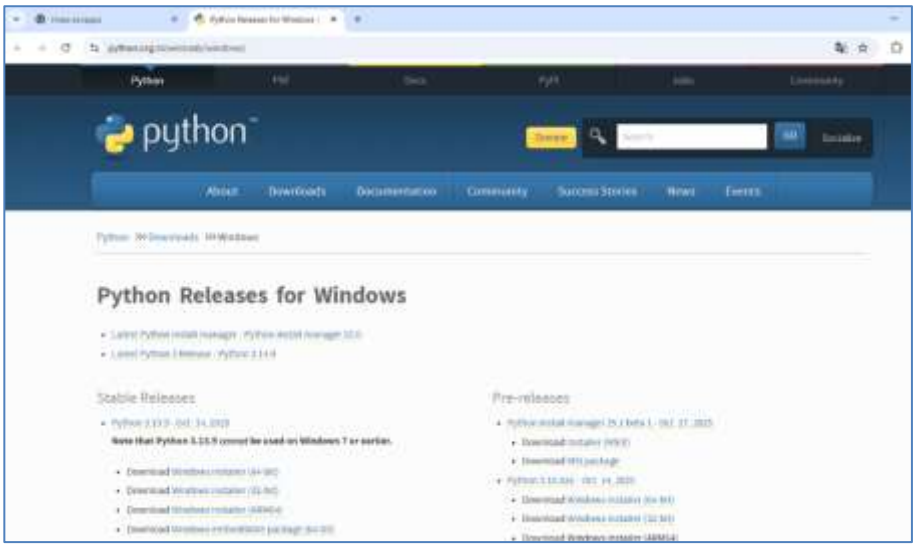
*Набір даних, який становить високу цінність.

Додаток 2

Встановлення компілятора для мови програмування Python

1. Запускаємо браузер і переходимо за посиланням https://python.org/downloads/windows/

Завантажується сайт програми Python (сторінка Download)

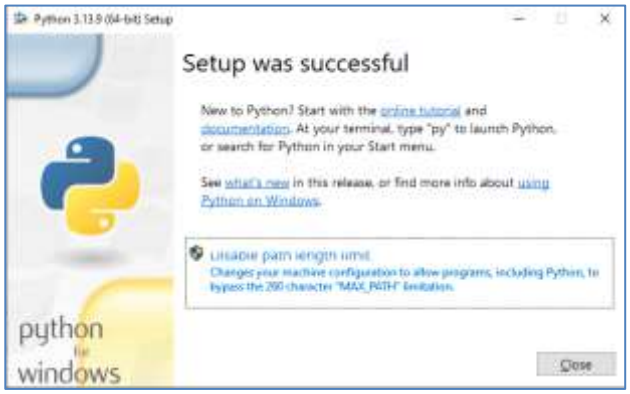


2. Вибираємо останню стабільну реалізацію (станом на 10.11.2025 версія 3.13.9) і завантажуємо на свій комп'ютер файл (Download **Windows installer (64-bit) ,** якщо у Вас 64-розрядна версія операційної системи.

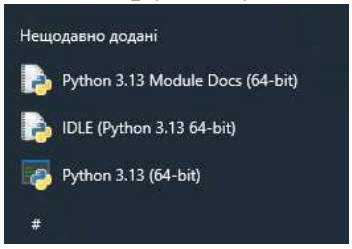
3. Переміщуємо щойно завантажений файл python-3.13.9-amd64.exe в кореневий каталог диску C: та запускаємо його на виконання.

4. З'явиться діалогове вікно **Python 3.13.9 (64-bit) Setup.** Встановіть обидва прапорці в нижній частині вікна та виберіть опцію **Install Now.**

5. У випадку успішної інсталяції повинно з'явитись нижченаведене повідомлення.



А в меню Пуск з'явиться нова група пунктів, пов'язаних з Python.



Додаток 3

Словник термінів з навчальної дисципліни

Nickname – це вигадане, особисте ім'я, яке людина використовує замість реального, найчастіше в Інтернеті (на форумах, в чатах, онлайн-іграх тощо). Українською мовою це означає прізвисько, кличка або нік.

Автентифікація – електронний процес, що дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних.

Автор електронного документа – фізична або юридична особа, яка створила електронний документ.

Авторизація з безпеки – рішення щодо можливості функціонування (експлуатації) відповідної інформаційної, електронної комунікаційної, інформаційно-комунікаційної, технологічної системи з урахуванням її відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах технічного захисту, криптографічного захисту та кіберзахисту, що приймається у встановленому законодавством порядку.

Авторизована система з безпеки – інформаційна, електронна комунікаційна, інформаційно-комунікаційна, технологічна система або її окремі елементи, об'єкт критичної інформаційної інфраструктури, в яких запроваджені заходи та/або системи з безпеки інформації, що пройшли авторизацію з безпеки.

Адміністратор безпеки – уповноважена посадова особа органу Національної поліції України, яка забезпечує захист інформації від несанкціонованого доступу, знищення, модифікації та блокування доступу до неї шляхом здійснення організаційних і технічних заходів, упровадження засобів та методів технічного захисту інформації в системі «ІПНП».

Адміністратор користувачів – уповноважена посадова особа органу Національної поліції України, яка адмініструє, супроводжує та координує роботу користувачів системи «ІПНП».

Адміністратор публічного електронного реєстру – юридична особа публічного права, що забезпечує функціонування та здійснює адміністрування публічного електронного реєстру, визначена законом або іншим нормативно-правовим актом, згідно з яким створено публічний електронний реєстр.

Адміністрування засобу інформатизації – вид управлінської діяльності власника та/або технічного адміністратора засобу інформатизації під час експлуатації засобу, спрямований на забезпечення керованості (управління) таким засобом інформатизації та/або його доступності для користувачів інформаційно-комунікаційних систем і засобів інформатизації.

Адресат – фізична або юридична особа, якій адресується електронний документ.

Активна протидія агресії у кіберпросторі – дії, спрямовані на підвищення рівня кіберзахисту шляхом нейтралізації кібератак держави-агресора, його систем і мереж, а також джерел походження кіберзагроз та кібератак, які використовуються для завдання шкоди національній безпеці України.

Багатофакторна автентифікація – автентифікація з використанням двох або більше факторів автентифікації, що належать до різних груп факторів автентифікації.

База даних – систематизована сукупність даних, що відображає стан об'єктів та їх взаємозв'язків у визначеній предметній сфері.

База персональних даних – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних.

Банк даних – система програмно-апаратних, організаційних та технічних засобів, призначених для централізованого накопичення, обробки та використання даних.

Безпека мереж і послуг – здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги.

Блокування інформації в системі – дії, внаслідок яких унеможливлюється доступ до інформації в системі.

Вебсайт – сукупність програмних засобів, розміщених за унікальною адресою в обчислювальній мережі, у тому числі в мережі Інтернет, разом з інформаційними ресурсами, що перебувають у розпорядженні певних суб'єктів і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інших інформаційних послуг через обчислювальну мережу.

Види інформації за змістом – інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля (екологічна інформація); інформація про товар (роботу, послугу); науково-технічна інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; критична технологічна інформація тощо.

Виток інформації – результат дій або бездіяльності, внаслідок яких інформація, що обробляється в системі чи пристроєм обробки інформації, стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

Відкритий формат – формат даних, незалежний від платформи та доступний без обмежень, які перешкоджають його повторному використанню.

Власник системи – фізична або юридична особа, якій належить право власності на систему.

Володілець інформації – фізична або юридична особа, якій належать права на інформацію.

Володілець персональних даних – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Дані – інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки, технічними та програмними засобами.

Державна електронна платформа ведення публічних електронних реєстрів – ІКС, призначена для уніфікованого, автоматизованого та стандартизованого процесу створення, адміністрування та ведення публічних електронних реєстрів з використанням загальних принципів проектування, програмування та захисту інформації в публічних електронних реєстрах.

Документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

Доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі.

Електронна демократія – форма суспільних відносин, за якої громадяни та організації залучаються до державотворення та державного управління, а також до місцевого самоврядування шляхом широкого застосування інформаційно-комунікаційних технологій у демократичних процесах, що дає змогу посилити участь, ініціативність та залучення громадян до публічного життя на загальнодержавному, регіональному та місцевому рівнях, підвищити прозорість процесу прийняття рішень та підзвітність демократичних інститутів, поліпшити зворотний зв'язок суб'єктів владних повноважень на звернення громадян, сприяти публічним дискусіям та привертати увагу громадян до процесу прийняття рішень.

Електронна довірча послуга – електронна послуга, що надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги.

Електронна ідентифікація – процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або уповноваженого представника юридичної особи.

Електронна комунікаційна мережа – комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг.

Електронна комунікаційна мережа загального користування – електронна комунікаційна мережа, доступ до якої відкритий для всіх кінцевих користувачів послуг.

Електронна комунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Електронна комунікація (телекомунікація, електрозв'язок) – передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій.

Електронна печатка – електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і використовуються для забезпечення достовірності походження пов'язаних електронних даних, або для засвідчення електронних підписів підписувачів на електронних документах, або для засвідчення відповідності копій документів оригіналам та виявлення порушення цілісності.

Електронна послуга – будь-яка послуга з надання певного матеріального чи нематеріального блага на користь іншої особи, яка надається через інформаційно-комунікаційну систему.

Контент-аналіз – це якісно-кількісний метод вивчення документів, який полягає в систематичній обробці змісту текстів, зображень, аудіо- чи відеоматеріалів для виявлення прихованих тенденцій, закономірностей та фактів. Метод перетворює неструктуровану інформацію на числові показники, що дозволяє отримати об'єктивні та строгі результати.

Лог – це спеціальний файл, який автоматично записує службову та статистичну інформацію про події, що відбуваються в системі, програмі або на вебсайті. Це, по суті, журнал подій, який використовується адміністраторами для аналізу роботи, виявлення помилок і збоїв, а також для збору статистики.

Нік – див. ***nickname.***

Фреймворк – це набір інструментів, бібліотек, стандартів і правил, який надає готову структуру для створення програмного забезпечення, прискорюючи та спрощуючи процес розробки. Він визначає загальну логіку та архітектуру проекту, дозволяючи розробникам зосередитись на унікальному функціоналі, а не на рутинних завданнях.

Додаток 4

Формати дати, які використовуються в документах

Хто складає документ, пам'ятай про дату
(Кудінов В.А., 2023)

1) *Короткий формат*:
01.09.2025 (Україна)
09/01/2025 або September 1, 2025 (США)

2) *Середній формат*:
01-вер-2025 (бази даних, тлф)

3) *Довгий формат*:
<u>спосіб 1 (нормативно-правові та фінансові документи):</u>
01 вересня 2025 р. (*або:* року)
<u>спосіб 2 (нотаріус):</u>
Перше вересня дві тисячі двадцять п'ятого року

4) *Повний формат*:
01.09.2025 08:05:10 (фіскальний чек, відеореєстратор, журнал дзвінків, sms, створення файлу, банківська транзакція, протокол слідчої дії)

5) *Особливий формат*:
01.IX.2025 (лікарі)
01
20 — 25
IX

Навчальне видання

КУДІНОВ Вадим Анатолійович

ПАКРИШ Олександр Євгенійович

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Навчально-практичний посібник

Комп’ютерна верстка: *В.А. Кудінова*

Підписано до друку 30.12.2025. Формат 60х84/16. Папір офсетний.
Обл.-вид. арк. 7,25. Ум. друк. арк. 6,74.
Тираж 50 прим.

Редакційно-видавниче відділення
Національної академії внутрішніх справ
03035, Київ, пл. Солом’янська, 1

Друк: ФОП Поліщук О.В.
Свідоцтво суб’єкта видавничої справи ДК № 2142 від 31.03.2015
07400, м. Бровари, вул. Незалежності, 2, кв. 148
тел. (044) 592-13-49