

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Кафедра інформаційних технологій та кібербезпеки**

*Присвячується
30-річчю кафедри
інформаційних технологій
та кібербезпеки*

В.А. Кудінов

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Словник термінів

Київ – 2019

Укладач:

Кудінов В.А. – кандидат фізико-математичних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ.

Рецензенти:

Бурячок В.Л. – доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки Державного університету телекомунікацій.

Хахановський В.Г. – доктор юридичних наук, професор, професор кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ.

Гавловський В.Д. – кандидат юридичних наук, старший науковий співробітник, провідний науковий співробітник Міжвідомчого НДЦ з проблем боротьби з організованою злочинністю при РНБО України.

Словник термінів обговорено та схвалено на засіданнях кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ від 31.08.2017 (протокол № 1), 07.03.2019 (протокол № 17), засіданні Вченої ради Національної академії внутрішніх справ від 28.11.2017 (протокол № 27/5-10).

Матеріали подано в авторській редакції

Кудінов В. А. Інформаційне забезпечення органів Національної поліції: словник термінів / В. А. Кудінов. – Київ : Нац. акад. внутр. справ, 2019. – 236 с.

Наведено основні терміни та визначення з усіх чотирьох тем навчальної дисципліни «Інформаційне забезпечення органів Національної поліції», яка викладається для здобувачів ступеня вищої освіти бакалавра на 3 курсі в навчально-наукових інститутах № 1, № 2 та № 3, заочного та дистанційного навчання Національної академії внутрішніх справ. Зазначена навчальна дисципліна протягом минулого навчального року для деяких категорій здобувачів мала іншу назву, а саме: «Інформаційне забезпечення професійної діяльності».

Призначено також для науково-педагогічних працівників закладів вищої освіти системи МВС України.

Може бути корисним для слухачів докторантури та аспірантури, наукових та практичних працівників органів та підрозділів МВС України, Національної поліції України.

**УДК 004:34
ББК 423**

ЗМІСТ

Перелік умовних скорочень.....	4
Інформація про кафедру.....	6
Епіграфи до навчальної дисципліни.....	8
ТЕМА I. Інформаційне забезпечення органів Національної поліції України: основні поняття, завдання, структура системи, характеристика інформаційних підсистем.....	11
<i>Додаткова інформація до теми I.....</i>	<i>79</i>
ТЕМА II. Введення у технологію баз даних. Система управління базами даних Microsoft Access.....	88
<i>Додаткова інформація до теми II.....</i>	<i>101</i>
ТЕМА III. Використання інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» у боротьбі зі злочинністю.....	105
<i>Додаткова інформація до теми III.....</i>	<i>121</i>
ТЕМА IV. Проведення навчально-ділової гри «Лінія-102».....	126
<i>Додаткова інформація до теми IV.....</i>	<i>132</i>
СЛОВНИК найбільш поширених загальних термінів.....	136
Предметний покажчик.....	192
Список рекомендованої літератури.....	211
Додаток 1. Перелік пріоритетних інформаційних ресурсів єдиної інформаційної системи МВС України.....	220
Додаток 2. Перелік основних наборів даних, які підлягають оприлюдненню у формі відкритих даних.....	223
Додаток 3. Перелік корисних відкритих реєстрів та баз даних України.....	227
Додаток 4. Витяг з Переліку відомостей, що становлять службову інформацію в системі МВС України.....	230
Додаток 5. Витяг з Переліку відомостей, що становлять службову інформацію в системі Національної поліції України.....	232

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АІС ОП	– Автоматизована інформаційна система оперативного призначення єдиної інформаційної системи МВС
АРМ	– Автоматизоване робоче місце
АЦСК	– Акредитований центр сертифікації ключів
БД	– База даних
БЕН	– Безконтактний електронний носій
ВРУ	– Верховна Рада України
ГУНП	– Головне управління Національної поліції
ДЗТ	– Департамент зв'язку та телекомунікацій Національної поліції України
ДІАП	– Департамент інформаційно-аналітичної підтримки
ДСА	– Державна судова адміністрація
ЕЦП	– Електронний цифровий підпис
ЄДР	– Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань
ЄДРСР	– Єдиний державний реєстр судових рішень
ЄІС	– Єдина інформаційна система
ЄРДР	– Єдиний реєстр досудових розслідувань
ЄЦВТМ	– Єдина цифрова відомча телекомунікаційна мережа
ІПС	– Інтегрована інформаційно-пошукова система
ІПНП	– Інформаційний портал Національної поліції України
ІПС	– Інформаційно-пошукова система
ІС	– Інформаційна система
ІТ	– Інформаційні технології
КМУ	– Кабінет Міністрів України
КП	– Комп'ютерна програма
КПК	– Кримінальний процесуальний кодекс
КСЗІ	– Комплексні системи захисту інформації
КУпАП	– Кодекс України про адміністративні правопорушення

МВС	– Міністерство внутрішніх справ
НАВС	– Національна академія внутрішніх справ
НПА	– Нормативно-правовий акт
НПУ	– Національна поліція України
НЦБ	– Національне центральне бюро
ОРД	– Оперативно-розшукова діяльність
ПД	– Персональні дані
Служба	– Національна поліція України, Державна міграційна служба України, Адміністрація Державної прикордонної служби України, Державна служба України з надзвичайних ситуацій, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України
СУБД	– Система управління базами даних
ТЗІ	– Технічний захист інформації
ТСЦ	– Територіальні сервісні центри
УІАП	– Управління інформаційно-аналітичної підтримки
УОАЗОР	– Управління організаційно-аналітичного забезпечення та оперативного реагування
УРТЗІ	– Управління режиму та технічного захисту інформації
ЦОВВ	– Центральні органи виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України
ЦУНАМІ	– Централізоване управління нарядами патрульної служби поліції
ЧЧ	– Чергова частина

ІНФОРМАЦІЯ ПРО КАФЕДРУ

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

<i>ДАТА</i>	<i>НАЗВА КАФЕДРИ</i>	
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
27.08.2010		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	



На кафедрі за час її існування працювало понад 60 працівників.

На кафедрі панують: *Порядність, Взаємодопомога, Професіоналізм.*

Штатна чисельність кафедри станом на 2018/2019 навчальний рік складає 18 посад: 13 – науково-педагогічного персоналу, 5 – навчально-допоміжного персоналу (4 – завідувачі навчальною лабораторією, 1 – старший лаборант).

Структура кафедри: 1) завідувач – *Корнейко* Олександр Васильович (к.т.н., професор); 2) професори кафедри – *Хахановський* Валерій Георгійович (д.ю.н., професор), *Рибальський* Олег Володимирович (д.т.н., професор), *Кудінов* Вадим Анатолійович (к.ф.-м.н., доцент); 3) доценти кафедри – *Краснощок* Віктор Миколайович (к.т.н., доцент), *Пакриш* Олександр Євгенійович (к.т.н., доцент), *Скачек* Людмила Миколаївна (к.т.н., доцент), *Смаглюк* Вячеслав Михайлович (к.т.н., доцент); 4) старші викладачі кафедри – *Ігнатушко* Юрій Іванович (к.ю.н.), *Тарасенко* Володимир Петрович (к.ф.-м.н.), *Чукаєва* Аліна Валеріївна (к.ю.н.), *Мельников* Ілля Миколайович; 5) викладачі кафедри – *Школьніков* Владислав Ігорович; 6) завідувачі навчальною лабораторією – *Грищенко* Олег Ігорович, *Ключник* Петро Володимирович, *Остапчук* Микола Миколайович, *Швець* Микола Миколайович; 7) старший лаборант – *Товолжанська* Світлана Борисівна.

Кафедра здійснює організацію навчального процесу в усіх навчальних підрозділах академії з понад 20 навчальних дисциплін.

Електронна пошта кафедри: *kafedra@i.ua*.

ЕПІГРАФИ ДО НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

– «Хто володіє інформацією, той володіє світом».

Вінстон Черчилль

– «Найбільшого успіху досягає той, хто володіє кращою інформацією».

Бенджамін Дізраелі

– «Кожні 100 років засоби масової інформації змінюються. Зараз настає час тотального обміну інформацією між конкретними людьми».

Марк Елліот Цукерберг

– «Недалеко той час, коли електронні машини будуть коморами не тільки технічних і наукових знань людства, але і все, що було створено ним за багато століть свого існування; вони стануть величезною і вічною пам'яттю».

В. М. Глушков

– «Якщо цього немає в Інтернеті – виходить, цього взагалі не існує».

Українські інформатики

– «Головною причиною, чому люди будуть купувати собі додому комп'ютер, стане можливість бути пов'язаними з національною комунікаційною мережею. Ми зараз на самому початку цього етапу, але це буде справжній прорив. Приблизно такий, як поява телефону».

Стівен Пол Джобс

– «Якщо тебе немає в Інтернеті, то ти не існуєш».

Білл Гейтс

– «Людина в ХХІ столітті, який не буде вміти користуватися ЕОМ, буде подібний людині ХХ століття, не вміло ні читати, ні писати».

В. М. Глушков

– «Створення першого екземпляру обчислювальної машини завжди коштує, щонайменше, у п'ять разів більше ніж створення другого екземпляру».

Чарлз Біббідж

– «Елементи машин і самі машини безперервно вдосконалюються. Якщо на першому етапі для їх створення використовувались елементи, створені для інших галузей техніки, то надалі створюватимуться спеціальні елементи саме для обчислювальної техніки».

С. О. Лебедєв

– «Найдешевші, швидкі і надійні компоненти обчислювальної системи – ті, яких в ній немає».

Гордон Белл

– «Ви кажете, що машина не може зробити усе? Якщо Ви скажете точно, що саме вона не може зробити, я зможу створити машину, що це зробить».

Джон фон Нейман

– «Людина надає кібернетичних машин здатність творити і створює цим собі могутнього помічника».

Норберт Вінер

– «Я не відчуваю страху перед комп'ютерами, я жахаюсь їх відсутності».

Айзенк Азімов

– «Найновіший комп'ютер – це комп'ютер, що або вчора застарів, або з'явиться завтра».

Сідні Бреннер

– «Спершу машини зроблять за нас багато роботи і не будуть дуже розумними. Через кілька десятиліть по тому інтелект буде достатньо сильним щоб бути загрозою. Я не розумію, чому деякі люди не стурбовані».

Білл Гейтс

– «Скоро залишаться лише дві групи працівників: ті, хто контролює комп'ютери, і ті, кого контролюють комп'ютери. Постарайтеся потрапити в першу».

Дейв Баррі

– «Аналітична машина не претендує на те, щоб створювати щось дійсно нове. Машина може виконати усе те, що ми можемо їй запрограмувати».

Августа Ада Кінг

– «Один з найважливіших уроків, що було надано комп'ютерній індустрії, є тим, що для користувача цінність комп'ютера визначається головним чином якістю та різноманітністю існуючих програм».

Білл Гейтс

– «Комп'ютерна програма завжди буде робити те, що Ви сказали, але рідко те, що побажали».

Українські інформатики

– «Пишіть програми в першу чергу для людей і тільки потім для машин».

Стівен Макконнелл

– «Хороший програміст – це той, хто дивиться у обидва боки, переходячи дорогу з одностороннім рухом».

Дуглас Ліндер

– «Три найдорожчих помилки всіх часів були викликані зміною одного символу в раніше коректних програмах».

Стівен Макконнелл

– «Непрацююча програма зазвичай приносить менше шкоди, ніж працююча погано».

Енді Гант та Дейв Томас

– «Комп'ютери ненадійні, однак люди ще менш надійні. Будь-яку систему, функціонування якої залежить від людини, не можна вважати надійною».

Українські інформатики

– «Брехня встигає обійти півсвіту, поки правда одягає штани».

Вінстон Черчилль

За даними:

URL: <http://annserduk.blogspot.com/>

URL: <http://vislovi.blogspot.com/>

URL: <https://ukrainianinformatics.home.blog/> цитати-про-інформатику/

URL: https://uk.wikipedia.org/wiki/Головна_сторінка



1. *«Хто має та вміло використовує інформаційні технології, той володіє інформацією».*

В.А. Кудінов (2010 р.)

2. *«Хто завжди перевіряє інформацію (зокрема, з Інтернет), той не має проблем з FACE у разі використання FAKE».*

– «REAL INFO – NORMAL FACE. FAKE INFO – PROBLEM FACE».

В.А. Кудінов (2019 р.)

3. *«Хто правильно робить копії унікальної інформації, той захищає себе від небажаних стресів у майбутньому у разі можливої її втрати».*

– «Хто правильно робить копії унікальної інформації, той молодець».

В.А. Кудінов (2013 р.)

4. *«Хто своєчасно володіє достовірною та повною інформацією, правильно її застосовує, той володіє ситуацією».*

В.А. Кудінов (2012 р.)

5. *«Хто вирішив продати ІзОД, той зробив до строку крок».*

В.А. Кудінов (2019 р.)

Примітка: ІзОД – інформація з обмеженим доступом.

ТЕМА І. ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ: ОСНОВНІ ПОНЯТТЯ, ЗАВДАННЯ, СТРУКТУРА СИСТЕМИ, ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНИХ ПІДСИСТЕМ

Автоматизована інформаційна система оперативного призначення єдиної інформаційної системи МВС (далі – АІС ОП) – є сукупністю програмно-технічних і телекомунікаційних засобів та призначена для накопичення й обробки відомостей, що утворюються в процесі оперативно-розшукової діяльності (далі – ОРД) Національної поліції України (далі – НПУ). АІС ОП утворена для наповнення та підтримки в актуальному стані бази даних (далі – БД) єдиної інформаційної системи (далі – ЄІС) Міністерства внутрішніх справ та є її складовою частиною [83].

Автоматизовані робочі місця на веб-порталі Національної академії внутрішніх справ – станом на сьогодні працівниками НАВС розроблено 4 автоматизованих робочих місця (далі – АРМ), які використовуються в освітній діяльності: 1) АРМ працівника підрозділу по боротьбі з незаконним обігом наркотиків; 2) АРМ слідчого; 3) АРМ дільничного офіцера поліції; 4) АРМ працівника карного розшуку [119].

Адміністратор бази даних центрального вузла АІС ОП – це працівник Департаменту інформаційно-аналітичної підтримки (далі – ДІАП), який згідно зі своїми функціональними (посадовими) обов'язками відповідає за експлуатацію програмних модулів та БД АІС ОП. Повноваження адміністратора БД регіонального вузла АІС ОП надаються працівнику Управління інформаційно-аналітичної підтримки (далі – УІАП), відповідальному за експлуатацію регіонального вузла бази даних. Адміністратор бази даних центрального вузла АІС ОП координує діяльність адміністраторів бази даних регіональних вузлів та відповідає за: 1) цілодобове функціонування програмних модулів та бази даних АІС ОП; 2) супроводження типових програмних засобів інформаційних підсистем АІС ОП; 3) технологічне забезпечення обміну інформаційними ресурсами між АІС ОП відповідних рівнів; 4) здійснення контролю за формуванням та підтриманням в актуальному стані інформаційних ресурсів АІС ОП [83].

Адміністратор безпеки центрального вузла АІС ОП – це працівник ДІАП, який згідно зі своїми функціональними (посадовими) обов'язками відповідає за дотримання політики безпеки в АІС ОП. Повноваження адміністратора безпеки АІС ОП на регіональному рівні надаються працівнику УІАП, відповідальному за дотримання політики безпеки в регіональному вузлі АІС ОП. Адміністратор безпеки центрального вузла АІС ОП координує діяльність адміністраторів безпеки регіональних вузлів системи та відповідає за: 1) *постійний захист* інформаційних ресурсів АІС ОП; 2) *розмежування доступу* до інформаційних ресурсів АІС ОП, реєстрацію та авторизацію користувачів; 3) *забезпечення захисту* відомостей інформаційних ресурсів АІС ОП від блокування, порушення цілісності та несанкціонованого доступу; 4) *здійснення контролю* за дотриманням правил і процедур обробки інформації користувачами; 5) *збереження* інформаційних масивів шляхом створення резервного банку даних [83].

Адміністратор єдиної інформаційної системи МВС – є державне підприємство, яке належить до сфери управління МВС. Він: 1) *забезпечує*: адміністрування, технічну підтримку та безперерйне функціонування центральної підсистеми ЄІС МВС; розроблення її програмного забезпечення; електронну інформаційну взаємодію суб'єктів ЄІС МВС; розроблення та здійснення заходів щодо захисту ЄІС МВС та інформації, що міститься в ній; гарантоване збереження інформації, що міститься в ЄІС МВС; 2) *здійснює*: постійний моніторинг технічного стану ЄІС МВС та захищеності інформації, що міститься в ній; впровадження механізмів електронної ідентифікації особи, зокрема для доступу до інформаційних ресурсів ЄІС МВС; надання доступу користувачам ЄІС МВС до її інформаційних ресурсів; надання/позбавлення доступу користувачам ЄІС МВС до центральної підсистеми відповідно до законодавства; ведення обліку користувачів ЄІС МВС, яким надано доступ до інформаційних ресурсів ЄІС МВС з використанням засобів електронної ідентифікації особи, з фіксуванням відомостей про дату і час отримання доступу, обсяг інформації, до якої отримано доступ; технічну та інформаційну підтримку користувачів ЄІС МВС, зокрема за допомогою відкритих веб-ресурсів, телефонного інформаційного центру тощо; 3) *проводить* навчання користувачів суб'єктів ЄІС МВС під час її впровадження та функціонування [52].

Бази даних поліції, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції – містять відомості, зокрема, стосовно: 1) повідомлень про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, що надійшли технічними каналами зв'язку; 2) щодобових переліків та складу нарядів поліції та слідчо-оперативних груп, що заступають на чергування; 3) завдань та орієнтувань, що доводились до нарядів поліції для реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події; 4) звітування нарядів поліції за результатами реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, виявлення додаткових обставин на місці пригоди; 5) пересувань нарядів поліції, які отримані із планшетних комп'ютерів та засобами GPS [87].

Банки даних інформаційної системи Міжнародної організації кримінальної поліції – Інтерполу – складова інформаційної системи (далі – ІС) Інтерполу, яка являє сукупність інформаційних ресурсів, що містять дані щодо осіб, предметів і явищ, які обробляються Генеральним секретаріатом Інтерполу з метою забезпечення співробітництва правоохоронних органів держав – членів Інтерполу в боротьбі зі злочинністю. *Поліцейським забороняється:* 1) використовувати БД в особистих цілях або цілях, не пов'язаних із службовою діяльністю; 2) розголошувати інформацію, яка стала відома їм у зв'язку з використанням БД, третім особам [105].

Використання поліцією інформаційних ресурсів – поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних» [6]. Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів, передбачених статтями 26, 27 Закону України «Про Національну поліцію» [8], фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій (далі – ІТ) МВС України. В електронному архіві фіксуються прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів [8].

Використання правових інформаційно-пошукових систем в юридичній діяльності дозволяє одержати наступні результати: 1) *інтенсифікація* пошукових процесів шляхом одержання за одиницю часу більших обсягів правових матеріалів і створення умов для їх більш глибокого аналізу та документального оформлення на комп'ютері; 2) *економія* часу, засобів і ресурсів при здійсненні пошуку необхідної інформації, відстеженні всіх змін і доповнень у чинних правових актах; 3) широкі можливості для ведення *аналітичної роботи* з документами; 4) *зростання результативності* прийнятих рішень, що пов'язано з підвищенням швидкості реагування на зміни законодавчої бази; 5) *підвищення якості* професійної діяльності юристів [108].

Вимога – письмове звернення про надання відомостей з персонально-довідкового обліку, що подається державними органами, які здійснюють правоохоронні функції та мають повноваження на отримання таких відомостей [106].

Вимоги до запитів до Національного центрального бюро Інтерполу в Україні – запити та інші документи, які надсилаються до Національного центрального бюро (далі – НЦБ), повинні мати *необхідні реквізити*: назва органу, його повна адреса, телефон, телетайп або факс, вихідний номер та номер посилення (при його наявності), прізвище та телефон виконавця. Запити та інші документи виконуються лише у друкованому вигляді, підписуються керівниками органу. Прізвища, імена іноземних громадян, назви закордонних фірм, підприємств, організацій або установ, при наявності їх написання мовою запитуваної країни, відтворюються в оригіналі. Перевірка з використанням каналів та можливостей НЦБ може здійснюватися стосовно будь-яких діянь, визначених кримінальним законодавством як злочини, окрім тих, які мають військовий, політичний, релігійний чи расовий характер [95].

Відомості з Єдиного реєстру досудових розслідувань (далі ЄРДР) – надаються у вигляді витягу в порядку, встановленому Кримінальним процесуальним кодексом (далі – КПК) України. 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 [100].

Відомості, що не можуть бути розголошені в текстах судових рішень, відкритих для загального доступу – у текстах судових рішень, що відкриті для загального доступу, не можуть бути розголошені такі відомості: 1) місце проживання або перебування фізичних осіб із зазначенням адреси, номери телефонів чи інших засобів зв'язку, адреси електронної пошти, реєстраційні номери облікової картки платника податків, реквізити документів, що посвідчують особу, унікальні номери запису в Єдиному державному демографічному реєстрі; 2) реєстраційні номери транспортних засобів; 3) номери банківських рахунків, номери платіжних карток; 4) інформація, для забезпечення захисту якої розгляд справи або вчинення окремих процесуальних дій відбувалися у закритому судовому засіданні; 5) інші відомості, що дають можливість ідентифікувати фізичну особу. Такі відомості замінюються літерними або цифровими позначеннями. З мотивів безпеки у текстах судових рішень у кримінальних справах, відкритих для загального доступу відповідно до цього Закону, можуть не зазначатися відомості щодо імен (ім'я, по батькові, прізвище) суддів, які розглядали судову справу, та учасників судового процесу [23].

Відповідальність за внесення інформації до ЄРДР – Реєстратор є відповідальною особою за *своєчасність, повноту та об'єктивність* внесених до ЄРДР відомостей згідно з чинним законодавством. Реєстратори та користувачі відповідають за порушення вимог відповідного Положення, втрату, пошкодження електронних ключів доступу та незаконне втручання в роботу ЄРДР згідно з чинним законодавством [100].

Власник і розпорядник ЄІС МВС України – є держава в особі МВС [52].

Внесення відомостей до ЄРДР – здійснюється шляхом фіксації Реєстратором інформації в ЄРДР та вибору даних у довідниках для заповнення документів первинного обліку про: 1) кримінальне правопорушення; 2) наслідки досудового розслідування кримінального правопорушення; 3) заподіяні збитки, результати їх відшкодування та вилучення предметів злочинної діяльності; 4) особу, яка вчинила кримінальне правопорушення та яка підозрюється у його вчиненні; 5) рух кримінального провадження. Установлені форми документів первинного обліку, довідників є єдиними для Реєстраторів усіх правоохоронних органів [108].

Внесення інформації в банки даних Генерального секретаріату Інтерполу – здійснюється: 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.

Володілець інформації Єдиного державного реєстру судових рішень (далі – ЄДРСР) – Державна судова адміністрація (далі – ДСА) України, яка вживає організаційних заходів, пов'язаних із забезпеченням ведення Реєстру [64].

Володілець інформації, що обробляється в центральній підсистемі ЄІС МВС – є МВС [52].

Володільцями інформації, що обробляється у функціональних підсистемах ЄІС МВС – є суб'єкти ЄІС МВС, які забезпечують захист інформації від випадкової втрати або знищення, незаконної обробки та незаконного доступу до інформації [52].

Вузол зв'язку єдиної цифрової відомчої телекомунікаційної мережі (далі – ЄЦВТМ) – це сукупність телекомунікаційного обладнання, яке забезпечує потреби в послугах зв'язку та передачі даних користувача ЄЦВТМ [85].

Вузол мережі ЄЦВТМ – це сукупність телекомунікаційного обладнання, яке забезпечує надання телекомунікаційних послуг. До вузла мережі ЄЦВТМ з протилежних сторін підключаються відповідно канали (засоби) передавання інформації до інших вузлів та кінцеве обладнання, за допомогою якого надаються послуги зв'язку користувачам [85].

Департамент інформатизації МВС України – є структурним підрозділом апарату МВС, який забезпечує визначення та реалізацію пріоритетних напрямів інформатизації апарату Міністерства та його територіальних органів з надання сервісних послуг МВС, Національної гвардії України, закладів, установ і підприємств, що належать до сфери управління МВС та за дорученням Міністра внутрішніх справ України центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України (далі – КМУ) через Міністра внутрішніх справ України (далі – ЦОВВ). Департамент безпосередньо підпорядкований державному секретареві МВС України [84].

Департамент міжнародного поліцейського співробітництва Національної поліції України – є структурним підрозділом апарату центрального органу управління Національної поліції України, який забезпечує планування, організацію, взаємодію та координацію дій 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, Інтерполу та Європолу, тобто виконує функції Національного центрального бюро Інтерполу в Україні (http://interpol.np.gov.ua/?page_id=28).

Держатель ЄРДР – є Генеральна прокуратура України. Держатель здійснює: 1) розробку засобів організаційного, методологічного та програмно-технічного ведення Реєстру; 2) виконання функцій адміністратора електронної бази даних (технічне і технологічне створення та супроводження програмного забезпечення Реєстру, адміністрування та моніторинг використання системи, зберігання та захист даних Реєстру, контроль права доступу тощо); 3) організацію взаємодії з іншими державними інформаційними системами, реєстрами та базами даних; 4) розробку та удосконалення нормативних документів щодо створення, ведення та користування даними Реєстру. Виконання функцій адміністратора Реєстру покладається на Генеральну прокуратуру України, прокуратури областей та міста Києва, якими забезпечуються адміністрування та моніторинг використання системи, надання (обмеження) реєстраторам доступу до Реєстру у визначених випадках, перевірка дотримання дисципліни та системи безпеки, проведення навчання щодо наповнення та користування Реєстром, а також виконання інших функцій [74, 100].

Джерела накопичення інформації в НЦБ Інтерполу в Україні – є: 1) матеріали та інформація, отримувані з Генерального секретаріату Інтерполу; 2) запити, повідомлення, матеріали, отримувані з Національних центральних бюро та правоохоронних органів інших країн; 3) запити, повідомлення, матеріали, отримувані від органів Національної поліції та інших правоохоронних органів України; 4) офіційні матеріали міністерств, відомств, установ та організацій, які не є правоохоронними. Залежно від потреб НЦБ може створювати інші підсистеми обліку, а також змінювати і вдосконалювати існуючі [95].

Довідка з персонально-довідкового обліку – документ, який містить відомості з персонально-довідкового обліку ЄІС МВС України та який залежно від обсягу запитуваної особою інформації може містити відомості про: 1) відсутність (наявність) судимості; 2) притягнення до кримінальної відповідальності, відсутність (наявність) судимості або обмежень, передбачених кримінально-процесуальним законодавством України [106].

Доступ до відкритої інформації ЄІС МВС – реалізується через сервіси на офіційних веб-сайтах суб'єктів єдиної інформаційної системи МВС без електронної ідентифікації особи [52].

Доступ до відомостей, внесених до ЄРДР – право доступу до відомостей, внесених до Реєстру, мають: 1) Держатель – у повному обсязі з урахуванням повноважень, якими наділені прокурори та керівники підрозділів Генеральної прокуратури України; 2) Директор Національного бюро та його перший заступник, керівник Підрозділу детективів Національного бюро та керівник Управління внутрішнього контролю Національного бюро – у межах, визначених статтею 17 Закону України «Про Національне антикорупційне бюро України»; 3) прокурори та керівники регіональних, місцевих та військових прокуратур – у межах кримінальних правопорушень, щодо яких слідчими прокуратури та слідчими піднаглядних їм органів проводиться досудове розслідування; 4) керівники органів прокуратури та досудового розслідування, слідчі органів прокуратури, поліції, безпеки, органів, що здійснюють контроль за додержанням податкового законодавства, 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; 5) 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 [100].

Доступ уповноважених працівників до сервісів ЄІС МВС – здійснюється з використанням засобів електронної ідентифікації, що відповідають вимогам законодавства, у межах реалізації своїх повноважень [52].

Доступ фізичної особи до інформації про себе, що обробляється в ЄІС МВС – здійснюється з використанням засобів електронної ідентифікації особи, що відповідають вимогам законодавства [52].

Електронна адреса суб'єкта владних повноважень – адреса електронної пошти, що складається з ідентифікатора, позначки “@” та доменного імені. При цьому ідентифікатором є адреса електронної пошти, визначена як офіційна суб'єктом владних повноважень, а доменним іменем – ім'я у домені gov.ua, зареєстроване суб'єктом владних повноважень [61].

Електронний кабінет – захищений веб-сервіс, за допомогою якого, в тому числі, забезпечується взаємодія авторизованого користувача з Реєстром у режимі реального часу. З дня початку функціонування Єдиної судової інформаційно-телекомунікаційної системи сервіс електронного кабінету починає функціонувати як сервіс офіційної електронної адреси [64].

Електронний примірник судового рішення – створений в автоматизованій системі документообігу суду електронний документ, підписаний електронним цифровим підписом (далі – ЕЦП) судді, що ухвалив таке судове рішення, в разі колегіального розгляду – електронними цифровими підписами всіх суддів, що входять до складу колегії, або іншої особи, визначеної згідно з пунктом 2 розділу III Порядку. Такий документ має бути ідентичним за документарною інформацією та реквізитами оригіналу судового рішення в паперовій формі [64].

Електронний цифровий підпис – електронний цифровий підпис у форматі, що забезпечує можливість встановлення дійсності ЕЦП у довгостроковому періоді (після закінчення строку чинності сертифіката), визначеному відповідно до вимог законодавства [64].

Ефективне функціонування ЄІС МВС – для цього її суб'єкти забезпечують своєчасне: 1) внесення до єдиної інформаційної системи МВС достовірної та повної інформації; 2) надання/позбавлення доступу користувачам єдиної інформаційної системи МВС до функціональних підсистем відповідно до законодавства; 3) інформування адміністратора єдиної інформаційної системи МВС про проблеми, що виникають під час функціонування єдиної інформаційної системи МВС [52].

Єдина база даних електронних адрес, номерів факсів (телефаксів) суб'єктів владних повноважень – автоматизована система накопичення та зберігання інформації про електронні адреси, номери факсів (телефаксів) суб'єктів владних повноважень, яка використовується судами для надсилання суб'єктові владних повноважень тексту повістки. *Держателем* Єдиної бази даних є Державна судова адміністрація, яка забезпечує її ведення, контролює здійснення заходів, пов'язаних із захистом інформації, що в ній міститься, укладає договори, відповідно до яких фінансуються витрати, пов'язані з веденням Єдиної бази даних, та виконує інші функції. *Адміністратором* цієї бази даних є визначена ДСА відповідно до законодавства юридична особа. Створення Єдиної бази даних здійснюється на підставі відомостей, поданих суб'єктом владних повноважень. Суб'єкти владних повноважень несуть відповідальність за достовірність відомостей, що подаються для внесення до Єдиної бази даних, і своєчасність їх подання. Право доступу та користування інформацією про суб'єктів владних повноважень, що міститься у Єдиній базі даних, мають усі заінтересовані особи. Доступ до зазначеної інформації здійснюється безоплатно через веб-сторінку, адреса якої розміщується на офіційному веб-сайті ДСА [61].

Єдина звітність про кримінальні правопорушення, осіб, які їх учинили, та рух кримінальних проваджень відповідно до ЄРДР – Адміністраторами Реєстру формується єдина звітність про кримінальні правопорушення, осіб, які їх учинили, та рух кримінальних проваджень. Коригування даних звітності допускається впродовж звітного періоду. У разі виявлення помилок минулих років коригування у звітах не проводиться, ці помилки відображаються у спеціальній доповідній записці, що додається до звіту [100].

Єдина інформаційна система МВС – багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супроводження їх діяльності і становить сукупність взаємозв'язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію [52].

Єдиний державний веб-портал відкритих даних – створення та забезпечення його функціонування здійснюється Державним агентством з питань електронного урядування, яке є його держателем. *Адміністратором* Єдиного державного веб-порталу відкритих даних є державне підприємство, яке належить до сфери управління Державного агентства з питань електронного урядування. *Розпорядники* інформації оприлюднюють у формі відкритих даних набір даних, визначений у переліку наборів даних, які підлягають оприлюдненню у формі відкритих даних, та будь-які інші наявні дані, що відповідають визначенню публічної інформації у формі відкритих даних. Набори даних оприлюднюються та регулярно оновлюються розпорядником інформації на Єдиному державному веб-порталі відкритих даних. У разі внесення змін до переліку наборів даних, які підлягають оприлюдненню у формі відкритих даних, розпорядник інформації у тримісячний строк з дати набрання чинності такими змінами здійснює їх оприлюднення та подальше оновлення на Єдиному державному веб-порталі відкритих даних [62].

Єдиний державний реєстр судових рішень – автоматизована система збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень. Суд загальної юрисдикції вносить до Реєстру всі судові рішення (рішення, судові накази, постанови, вирoki, ухвали) і окремі думки суддів, викладені у письмовій формі, не пізніше наступного дня після їх ухвалення або виготовлення повного тексту. Ці судові рішення є *відкритими для безоплатного цілодобового доступу* на офіційному веб-порталі судової влади України. Для реалізації права доступу до судових рішень, внесених до Реєстру, користувачу надаються можливості пошуку, перегляду, копіювання та роздрукування судових рішень або їхніх частин. Обмеження права вільного користування офіційним веб-порталом судової влади України допускається настільки, наскільки це необхідно для захисту інформації, яка за рішенням суду щодо розгляду справи у закритому судовому засіданні підлягає захисту від розголошення. Загальний доступ до ухвал про дозвіл на обшук (про відмову у задоволенні клопотання про обшук) житла чи іншого володіння особи, про дозвіл на проведення (про відмову у задоволенні клопотання про проведення) негласної слідчої (розшукової) дії забезпечується через 1 рік після внесення ухвал до Реєстру [23]. *Або: Єдиний державний реєстр судових рішень* – державна інформаційна система, що входить до складу

Єдиної судової інформаційної системи і забезпечує збирання, облік (реєстрацію), накопичення, зберігання, захист, пошук та перегляд інформаційних ресурсів Реєстру та їх образів. База даних ЄДРСР містить інформацію довідкового характеру, яка станом на 30.04.2019 містить 79 452 987 документів. З дня початку функціонування Єдиної судової інформаційно-телекомунікаційної системи Реєстр переходить до її складу. Інформаційні ресурси Реєстру зберігаються у вигляді електронних даних, які за допомогою програмно-апаратних засобів можуть бути перетворені у візуальну форму. Електронні примірники судових рішень та окремих думок суддів є документами *безстрокового зберігання*. Особи, яким надано дозвіл на повний доступ до судових рішень, зобов'язані *не допускати розголошення* у будь-який спосіб інформації, що стала їм відома у зв'язку з користуванням Реєстром у режимі повного доступу. Посадові особи органів, яким стала відома інформація, що не може бути відкрита для загального доступу, зобов'язані не допускати її розголошення [64].

Єдиний облік – прийняття та реєстрація органами поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події [80].

Єдиний реєстр досудових розслідувань – це 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, внесені до Реєстру, з дотриманням вимог КПК та законодавства, яким врегульовано питання захисту персональних даних та доступу до інформації з обмеженим доступом [74, 100].

ЄЦВТМ – є сучасною логічно цілісною мультисервісною багаторівневою інформаційно-телекомунікаційною мережею МВС, що здійснює взаємодію із загальнодержавними телекомунікаційними мережами спеціального зв'язку та включає сукупність технічних засобів й обладнання мережі доступу і транспортної телекомунікаційної мережі для забезпечення передачі інформації (даних), яка (які) належить (належать) до державних інформаційних ресурсів регіонального (між МВС, Національною гвардією України, ЦОВВ, Автономною Республікою Крим, областями, містами Київ та Севастополь), районного та міського рівнів, для потреб користувачів,

а також надає підключеним до неї віддаленим один від одного користувачам системи МВС весь різновид телекомунікаційних послуг і сервісів фіксованого телефонного, документального, радіозв'язку, аудіо- та відеоселекторного зв'язку тощо як у звичайних умовах, так і під час особливого періоду чи запровадження в державі надзвичайного стану. МВС є власником ЄЦВТМ та володільцем інформації, яка створена її користувачами та циркулює в ЄЦВТМ [85].

Завдання ЄІС МВС – це: 1) *створення єдиного інформаційного простору* системи МВС та ЦОВВ, діяльність яких спрямовується і координується КМУ через Міністра внутрішніх справ шляхом логічного об'єднання їх інформаційних ресурсів, оптимізація процесів спільного використання технічних та програмних ресурсів; 2) *інформаційна підтримка діяльності* суб'єктів ЄІС МВС під час виконання завдань та функцій, покладених на них законодавством, з метою підвищення її ефективності; 3) *створення умов для електронної взаємодії* суб'єктів ЄІС МВС з метою оперативного виконання завдань, покладених на них законодавством, зменшення часових та фінансових витрат на адміністративно-управлінські, інформаційно-пошукові, розрахункові та аналітичні роботи, формування звітності; 4) *забезпечення інформаційної взаємодії* з державними органами, органами місцевого самоврядування, міжнародними організаціями, суб'єктами господарювання та правоохоронними органами інших держав, у тому числі з використанням загальнодержавних інформаційно-телекомунікаційних систем, а саме системи електронної взаємодії державних електронних інформаційних ресурсів “Трембіта” та інтегрованої системи електронної ідентифікації [52].

Завдання системи інформаційного забезпечення органів Національної поліції: 1) забезпечення можливості оперативного отримання інформації у повному систематизованому та зручному для користування вигляді; 2) збір, обробка та узагальнення аналітичної, статистичної і контрольної інформації для оцінки ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях управління; 3) забезпечення динамічної та ефективної інформаційної взаємодії усіх їх галузевих служб, інших правоохоронних органів та державних установ; 4) забезпечення захисту інформації [108].

Загальна характеристика банків даних Генерального секретаріату Інтерполу (http://interpol.np.gov.ua/?page_id=40) – 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: 1) вноситься до банків даних всіма країнами-членами Інтерполу (на даний час в Інтерполі 192 країн-членів); 2) 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 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) [108].

Загальний доступ до судових рішень – доступ до образів інформаційних ресурсів Реєстру. Образи інформаційних ресурсів Реєстру відкриваються для загального доступу не пізніше наступного робочого дня після завершення оброблення та знеособлення відповідних інформаційних ресурсів Реєстру. Для *неавторизованих користувачів* надання безоплатного цілодобового доступу до образів інформаційних ресурсів Реєстру здійснюється через *офіційний веб-портал* “Судова влада України”. Для *авторизованих користувачів* надання безоплатного цілодобового доступу до образів інформаційних ресурсів Реєстру здійснюється за допомогою *електронного кабінету*. Адміністратор з метою запобігання несанкціонованому доступу до Реєстру забезпечує відстеження та облік дій авторизованих користувачів [64].

Замовник і утримувач Національного реєстру електронних інформаційних ресурсів – є Державне агентство з питань електронного урядування, яке координує та контролює роботи, пов'язані із створенням, веденням і забезпеченням функціонування Національного реєстру, визначає організаційні та методичні засади ведення Національного реєстру та правила користування ним [63].

Засоби передавання інформації в ЄЦВТМ – мережа передавання інформації оператора зв'язку або канал, створений фізичними лініями кабелю та модемами (у межах міста) [85].

Захист відомостей, внесених до ЄРДР – Адміністратор здійснює комплекс програмних, технологічних та організаційних заходів щодо захисту відомостей, що містяться у Реєстрі, від несанкціонованого доступу. Адміністратор за кожним фактом втрати або пошкодження Реєстратором електронного ключа доступу невідкладно вживає заходів до його блокування та повідомляє про це Держателя Реєстру. Адміністратор негайно інформує відповідного керівника прокуратури та органу досудового розслідування про намагання Реєстратора отримати інформацію за межами наданого йому доступу [100].

Захист інформації в НЦБ Інтерполу в Україні – НЦБ вживає заходи щодо забезпечення режиму таємності, конфіденційності та захисту інформації. Працівники НЦБ *зобов'язані* зберігати державну та службову таємницю. Їм *забороняється* виправлення та знищення інформації з власної ініціативи. Виправлення і знищення інформації можливе лише на підставі прохання НЦБ або органу, які були ініціаторами її надсилання в НЦБ, з дозволу керівництва НЦБ. Органи, які одержали інформацію з НЦБ, зобов'язані забезпечити ефективний захист її змісту від сторонніх осіб, а також від викривлення та розголошення. Наявна в НЦБ інформація призначена лише для використання правоохоронними органами та судами у попередженні, розкритті, розслідуванні злочинів та судовому розгляді кримінальних проваджень. Відомості, що знаходяться в НЦБ і стосуються конкретних розслідувань, конкретних осіб, можуть бути передані засобом масової інформації лише з *дозволу* тих НЦБ або тих органів, які повідомили їх Укрбюро Інтерполу. Якщо та чи інша інформація частково або повністю втратила достовірність, орган-ініціатор або виконавець запиту повинен звернутися до НЦБ з проханням виправити або, при потребі, знищити її [95].

Захист інформації, внесеної до Єдиного державного реєстру судових рішень – Інформація, внесена до Реєстру, повинна мати захист від її *викрадення, перекручення чи знищення. Не допускається вилучення судових рішень із Реєстру. Не допускається внесення будь-яких змін до судових рішень, які внесені до Реєстру, крім випадків, що пов'язані з необхідністю виправлення технічної помилки, допущеної під час внесення судового рішення до Реєстру чи ведення Реєстру. У разі виправлення судового рішення відповідно до процесуального закону його текст у Реєстрі не змінюється. До Реєстру додатково вноситься судові рішення, яким внесені зміни до відповідного судового рішення [23].*

Заявникові відмовляється в наданні відомостей з персонально-довідкового обліку в разі, якщо: 1) запит подано особою, яку *неможливо ідентифікувати* або яка не підтвердила повноваження щодо його подання, або установчі дані в запиті зазначені не в повному обсязі чи некоректно; 2) у запиті *не вказано мету отримання відомостей*; 3) у запиті *не вказано вид запитуваної інформації* (відомості про відсутність (наявність) судимості, притягнення до кримінальної відповідальності або обмежень, передбачених кримінальним процесуальним законодавством України); 4) відомості про фізичну особу, зазначені в запиті в електронній формі, *не відповідають* реквізітам підписувача, що зазначені в посиленому сертифікаті відкритого ключа електронного цифрового підпису. Про відмову в наданні відомостей з персонально-довідкового обліку Заявник повідомляється в письмовому вигляді або на його вимогу в електронному із зазначенням причини відмови та роз'ясненням порядку оскарження такого рішення. Строк вмотивованої відмови в наданні Довідки не може перевищувати 10 робочих днів з дня надходження запиту [106].

Зберігання інформаційних ресурсів ЄІС МВС, що створені в системі МВС – в центральній підсистемі єдиної інформаційної системи МВС [52].

Зберігання інформаційних ресурсів інших суб'єктів ЄІС МВС – у центрах обробки даних відповідних суб'єктів єдиної інформаційної системи МВС [52].

Зміст Національного реєстру електронних інформаційних ресурсів – включається інформація про державні електронні реєстри, кадастри, державні та інші обов’язкові класифікатори, а також інформаційні системи, які забезпечують їх функціонування та використовують інформацію з них (далі – *е-ресурси*). До Національного реєстру включаються е-ресурси суб’єктів владних повноважень. Включення до Національного реєстру е-ресурсів приватної форми власності здійснюється на добровільних засадах. До Національного реєстру не включаються е-ресурси, які містять: 1) відомості, що становлять державну таємницю; 2) інформацію, розповсюдження якої заборонене законодавством [63].

Знеособлення – *процедура маскування* в тексті електронного примірника судового рішення або окремої думки судді відомостей, що не можуть бути розголошені відповідно до вимог законодавства за допомогою спеціалізованого програмного забезпечення з подальшою вибірковою візуальною перевіркою результатів такого маскування. Результатом процедури знеособлення є створення образу електронного документа [64].

Зобов’язання користувачів ЄІС МВС – дотримуватися визначеного МВС порядку роботи з інформаційними ресурсами єдиної інформаційної системи МВС та використовувати отриману інформацію відповідно до законодавства [52].

Інструкція про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідуванні злочинів – визначає порядок використання правоохоронними органами України можливостей НЦБ Інтерполу в Україні для співробітництва з Генеральним секретаріатом Інтерполу та правоохоронними органами зарубіжних держав під час здійснення діяльності, пов’язаної із попередженням, розкриттям та розслідуванням злочинів, які мають транснаціональний характер або виходять за межі України [95].

Інтеграція інформаційних ресурсів ЄІС МВС – комплекс методів та процедур, спрямованих на логічне функціональне об’єднання інформаційних ресурсів єдиної інформаційної системи МВС у визначених форматах, за узгодженими показниками, для їх автоматизованої обробки, використання та надання користувачам в уніфікованому вигляді [52].

Інтерфейс прикладного програмування відкритих даних – має забезпечувати можливість автоматизованого (без участі людини) доступу до всієї інформації оприлюдненого набору даних шляхом їх перегляду та читання (без можливості внесення змін) за запитом у цілодобовому режимі без вихідних та достовірність такої інформації на момент її запиту. Доступ до оприлюднених наборів даних надається за допомогою інтерфейсу прикладного програмування, якщо відповідний набір даних містить великий обсяг інформації та часто оновлюється (щотижня або частіше). Вимоги до інтерфейсу прикладного програмування визначаються держателем Єдиного державного веб-порталу відкритих даних. *Не допускається* припинення надання доступу до оприлюднених наборів даних за допомогою інтерфейсу прикладного програмування протягом 12 місяців з моменту початку надання доступу та з моменту прийняття розпорядником інформації рішення про припинення надання доступу до оприлюдненого відповідного набору даних. *Допускається тимчасове припинення* надання доступу до оприлюднених наборів даних за допомогою інтерфейсу прикладного програмування для профілактичних робіт на час, що не перевищує 24 години на місяць. Тимчасове припинення не повинно тривати понад 4 години. Тимчасовому припиненню надання доступу до оприлюднених наборів даних за допомогою інтерфейсу прикладного програмування для профілактичних робіт повинне передувати відповідне попередження на головній сторінці Єдиного державного веб-порталу відкритих даних не менш як за 24 години до такого тимчасового припинення [62].

Інформаційна служба МВС України – станом на сьогодні це *Департамент інформатизації* (з 2018 р.). Попередні назви: Республіканський науково-дослідний інформаційний центр (створений 17 травня 1971 року), Головне інформаційне бюро (1993 р.), Головний інформаційний центр (1997 р.), Управління оперативної інформації (1999 р.), Департамент інформаційних технологій (2002 р., 2012 р.), Департамент інформаційно-аналітичного забезпечення (2010 р.).

Інформаційна служба Національної поліції України – станом на сьогодні це *Департамент інформаційно-аналітичної підтримки* (з 2018 р.). Попередня назва: Департамент інформаційної підтримки та координації поліції «102» (2015 р.).

Інформаційні ресурси АІС ОП – є об’єктивно поєднаний набір відомостей, що безпосередньо стосуються осіб та подій (кримінальних правопорушень), які накопичуються в процесі здійснення ОРД Національної поліції України. Обліку в АІС ОП підлягають відомості про осіб, відносно яких заведено оперативно-розшукові справи, отримані: 1) від осіб, які конфіденційно співробітничать з оперативними підрозділами Національної поліції України; 2) в ході проведення оперативно-розшукових заходів у рамках оперативно-розшукових справ. Інформаційні ресурси АІС ОП є складовою державних інформаційних ресурсів. Інформація про особу надається на запит органів досудового розслідування, прокуратури та суду. Найвищим ступенем обмеження доступу до інформації, що обробляється в АІС ОП, є ступінь секретності «таємно». Інформація щодо осіб, стосовно яких проводилися оперативно-розшукові заходи та за результатами ухвали або вироку суду доведено їх причетність до злочинної діяльності, перебуває на обліку АІС ОП 5 років з дня закриття оперативно-розшукової справи, після чого знищується в установленому законодавством України порядку. У разі якщо причетність до правопорушення особи, щодо якої здійснювались оперативно-розшукові заходи, не підтвердилась, така інформація зберіганню не підлягає та знищується в установленому законодавством України порядку. Обсяг, структура, порядок формування та використання інформаційних ресурсів АІС ОП визначаються окремими нормативно-правовими актами (далі – НПА) МВС [83].

Інформаційні ресурси Єдиного державного реєстру судових рішень – сукупність електронних примірників судових рішень та електронних примірників окремих думок суддів [64].

Інформаційні ресурси єдиної інформаційної системи МВС – визначені групи взаємозв’язаних задокументованих одиниць інформації, які формуються і об’єднуються в автоматизованих інформаційних системах суб’єктів єдиної інформаційної системи МВС за певними ознаками, у тому числі зазначені в переліку пріоритетних інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ, затвердженому постановою Кабінету Міністрів України від 14 листопада 2018 р. № 1024 [52].

Інформаційно-пошукова система «Законодавство України» – є сучасним і простим засобом для роботи з *правовою інформацією*. Система має потужний пошуковий апарат та різноманітні засоби відображення документів, кількість яких станом на 26.04.2019 складає 233 492 документів. Вона містить: 1) документи органів влади України (Президента України, Верховної Ради України (далі – ВРУ), КМУ, Конституційного Суду України, Верховного Суду України, міністерств та відомств); 2) міжнародні угоди; 3) деякі нормативні документи органів влади; 4) документи регіонального законодавства. Актуалізація БД здійснюється *щоденно*. База даних «Законодавство України» має інформаційний характер і не є офіційним друкованим виданням. Вона використовується згідно із Положенням про веб-ресурси ВРУ [108, 113, 116].

Інформаційно-правові системи «Ліга: Закон» – найповніше джерело систематизованої та достовірної правової інформації зі зручними інструментами для пошуку. Дають змогу швидко знайти й проаналізувати правову інформацію на будь-який момент часу, оцінити ситуацію та прийняти правильне рішення [108, 113].

Інформаційно-телекомунікаційна система Інтерполу I-24/7 (Інтерпол 24 години на добу – 7 днів на тиждень) – була впроваджена у діяльність Організації в 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 Національними центральними 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 телекомунікаційними системами і є доступною для використання всім правоохоронцям, які безпосередньо здійснюють розкриття та розслідування злочинів [108].

Інформація експертно-криміналістичних обліків – поділяється на: 1) оперативно-пошукові обліки; 2) інформаційно-довідкові обліки [108].

Інформація оперативних обліків – умовно поділяється на: 1) облік осіб і їх характеристик; 2) облік подій; 3) облік предметів та речей [108].

Класифікація основних видів обліків Міністерства внутрішніх справ України та Національної поліції – їх можна умовно класифікувати на: 1) оперативного призначення; 2) експертно-криміналістичного призначення; 3) статистичного та аналітичного призначення; 4) адміністративного (управлінського) та загального призначення [108].

Комплексні системи захисту інформації (далі – КСЗІ) – забезпечують захист інформації в підсистемах єдиної інформаційної системи МВС шляхом здійснення комплексу технічних, криптографічних, організаційних та інших заходів і використання засобів захисту інформації, спрямованих на недопущення блокування доступу до інформації, несанкціонованого ознайомлення з нею та/або її модифікації [52].

Контроль та нагляд за внесенням інформації до ЄРДР – прокурори, керівники органів досудового розслідування усіх рівнів забезпечують у відомствах контроль за *своєчасним, повним та достовірним* внесенням інформації до Реєстру у строки, визначені КПК України та Положенням. Керівники підрозділів організаційного забезпечення ЄРДР та інформаційно-аналітичної роботи Генеральної прокуратури України, підрозділів ведення ЄРДР та інформаційно-аналітичної роботи прокуратур регіонального рівня забезпечують проведення *систематичних перевірок* об'єктивного внесення Реєстраторами до Реєстру відомостей про кримінальні правопорушення та результати їх розслідування з урахуванням вимог КПК України та цього Положення. У разі встановлення фактів невідповідності внесеної до Реєстру інформації матеріалам кримінального провадження або її неповноти вживаються заходи щодо усунення виявлених порушень [100].

Користувачі АІС ОП – це посадові особи Національної поліції України, яким в установленому порядку надано право наповнювати, підтримувати в актуальному стані та використовувати інформаційні ресурси АІС ОП. Користувачі АІС ОП відповідають за *достовірність інформації*, що вводиться ними до АІС ОП, та зобов'язуються *не розголошувати* у будь-який спосіб інформацію, що міститься у системі, крім випадків, передбачених законодавством України [83].

Користувачі ЄІС МВС – це фізичні особи та уповноважені посадові особи суб'єктів ЄІС МВС, яким в установленому порядку надано відповідні права доступу до інформації в єдиній інформаційній системі МВС [52].

Користувачі ЄРДР – це: 1) *керівники* прокуратур та органів досудового розслідування; 2) *прокурори*; 3) *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; 4) 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) відповідно до чинного законодавства [74, 100].

Користувачі ЄЦВТМ – це посадові особи підрозділів (структурних підрозділів), які використовують послуги і сервіси ЄЦВТМ. Інші посадові особи органів державної влади можуть стати користувачами ЄЦВТМ в установленому законодавством порядку [85].

Користувачі робочого місця віддаленого доступу до персонально-довідкового обліку – посадові особи Департаменту інформатизації МВС та Департаменту інформаційно-аналітичної підтримки і територіальних підрозділів інформаційно-аналітичної підтримки поліції НПУ, що проводять перевірки за персонально-довідковим обліком, територіальних сервісних центрів (далі – ТСЦ) МВС, що формують та надсилають запити щодо перевірки фізичних осіб за персонально-довідковим обліком ЄІС МВС України [106].

МВС відповідно до покладених на нього завдань –

- 1) *забезпечує ведення обліку* знарядь кримінального правопорушення та інших речових доказів, отриманих відповідно до закону від судів, органів, що здійснюють ОРД, органів досудового розслідування, а також натурних зразків або каталогів продукції, технічної документації та іншої інформації, необхідної для створення і оновлення методичної та нормативної бази судової експертизи;
- 2) *забезпечує належне функціонування* ЄІС МВС, формує та підтримує в актуальному стані інформаційні ресурси, що входять до єдиної інформаційно-телекомунікаційної системи МВС, здійснює обробку персональних даних в межах повноважень, передбачених законом, забезпечує режим доступу до інформації, надає інформаційні послуги;
- 3) *здійснює інформаційну взаємодію* з іншими державними органами, правоохоронними органами іноземних держав та міжнародними організаціями;
- 4) *організовує розроблення* нових видів засобів спеціальної техніки, озброєння, засобів зв'язку, технічних засобів захисту інформації, спеціальних технічних засобів для оперативної діяльності, спеціального транспорту, пожежної та бронетанкової техніки, спеціальних засобів самозахисту та активної оборони, засобів індивідуального бронезахисту, криміналістичної та комп'ютерної техніки, програмного забезпечення, форменого одягу тощо;
- 5) *забезпечує* в межах повноважень, передбачених законом, *захист інформації*, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом тощо [53].

МВС для виконання покладених на нього завдань має право – 1) *отримувати* в установленому порядку *безоплатно* від міністерств, інших центральних та місцевих органів виконавчої влади, органів місцевого самоврядування необхідні для виконання покладених на нього завдань інформацію, документи і матеріали; 2) *користуватися* відповідними *інформаційними базами даних* державних органів, державною системою урядового зв'язку та іншими технічними засобами тощо [53].

Мета ведення ЄРДР – Реєстр утворений та ведеться відповідно до вимог КПК України з метою забезпечення: 1) *реєстрації* кримінальних правопорушень (проваджень) та *обліку* прийнятих під час досудового розслідування рішень, осіб, які їх учинили, та результатів судового провадження; 2) *оперативного контролю* за додержанням законів під час проведення досудового розслідування; 3) *аналізу* стану та структури кримінальних правопорушень, вчинених у державі; 4) *інформаційно-аналітичного забезпечення* правоохоронних органів [74, 100].

Мета ведення Національного реєстру електронних інформаційних ресурсів – запровадження *єдиної системи обліку* електронних інформаційних ресурсів держави і формується з використанням новітніх досягнень у сфері інформаційно-телекомунікаційних технологій. Створення, функціонування та вдосконалення ведення Національного реєстру забезпечується за рахунок бюджетних коштів, передбачених на цю мету Державному агентству з питань електронного урядування. Органи державної влади, органи місцевого самоврядування та інші юридичні особи публічного права користуються інформаційним фондом Національного реєстру *безоплатно* [63].

Мета обробки інформації у функціональних підсистемах єдиної інформаційної системи МВС – установлюється нормативно-правовими актами, які регулюють діяльність відповідних суб'єктів ЄІС МВС, окремо для кожного визначеного пріоритетного інформаційного ресурсу [52].

Мета системи інформаційного забезпечення органів Національної поліції – це всебічна інформаційна підтримка практичної діяльності органів та підрозділів Національної поліції України [108].

Мета створення ЄЦВТМ – ЄЦВТМ є необхідною для створення *єдиного* інтегрованого телекомунікаційного простору МВС для забезпечення *надійної доставки інформації*, яка циркулює в ЄЦВТМ, підвищення ефективності *управління та контролю*, прискорення та покращення *взаємодії* між окремими підрозділами (користувачами), *упровадження* сучасних цифрових телекомунікацій у діяльність підрозділів (користувачів), проведення технічного *переоснащення та інтеграції* функціонуючих розрізнених мереж зв'язку і передачі даних окремим підрозділів (користувачів), *заощадження коштів* на послугах зв'язку мережі загального користування [85].

Мета функціонування єдиної інформаційної системи МВС – оптимізація інформаційної взаємодії суб'єктів ЄІС МВС на рівні загальнодержавних інформаційних ресурсів 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), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших категорій мігрантів [52].

На сторінці кожного набору даних на Єдиному державному веб-порталі відкритих даних розміщується: 1) паспорт набору даних шляхом відображення на веб-сторінці та шляхом розміщення файлу у відкритому машиночитаному форматі, який може бути завантажений або доступний за допомогою інтерфейсу прикладного програмування; 2) структура набору даних у відкритому машиночитаному форматі (електронний файл, який може бути завантажений, або інтерфейс прикладного програмування); 3) набір даних в одному чи кількох форматах; 4) форма для зворотного зв'язку користувачів; 5) інформація про подальше використання набору даних; 6) інформація про умови використання відкритої ліцензії [62].

На сторінці кожного набору даних, що оприлюднюється, розпорядник інформації розміщує таку інформацію: публічна інформація у формі відкритих даних оприлюднюється для *вільного та безоплатного доступу* до неї. Відкриті дані дозволені для їх подальшого *вільного використання та поширення*. Будь-яка особа може вільно копіювати, публікувати, поширювати, використовувати, зокрема в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до складу власного продукту відкриті дані з *обов'язковим посиланням* на джерело їх отримання. Умовою будь-якого подальшого використання відкритих даних є обов'язкове посилання на джерело їх отримання (у тому числі гіперпосилання на веб-сторінку відкритих даних розпорядника інформації) [62].

Надання відомостей з ЄДР – відомості з Реєстру надаються у вигляді витягу в порядку, встановленому КПК України, за відповідною формою [100].

Надання інформації з персонально-довідкового обліку – здійснюється на *запити* державних органів або фізичних осіб, що оформлені з дотриманням вимог законодавства, у *письмовій або електронній формі*. Спеціальні програмні засоби ведення інформаційної підсистеми «Оперативно-довідкова картотека», яка входить до ЄІС МВС України, забезпечують автоматичне внесення до системних журналів даних щодо запитів до персонально-довідкового обліку, зокрема щодо ініціатора запиту, його змісту, дати та часу виконання, виконавця, реквізитів та змісту відповіді. *Право на запит та отримання відомостей* з персонально-довідкового обліку мають: 1) державні органи, які здійснюють правоохоронні функції; 2) суди всіх рівнів; 3) органи державної влади та їх територіальні органи, органи місцевого самоврядування у зв'язку зі здійсненням ними повноважень, визначених законодавством; 4) фізичні особи [106].

Направлення запитів до оперативно-довідкового і дактилоскопічного обліків та їх одержання – здійснюється: 1) *поштою* або через спеціально виділених працівників (*кур'єрів*), які є уповноваженими особами; 2) *засобами електронного зв'язку* з використанням спеціалізованого програмного забезпечення; 3) через *спецвідділ* (шифром). Вимоги, як правило, направляються нетаємним порядком. Засекречування їх здійснюється лише в тих випадках, коли це викликано службовою необхідністю [97].

Національна поліція відповідно до покладених на неї завдань – 1) здійснює заходи з контролю за місцезнаходженням осіб, які в установленому законом порядку зобов'язані носити електронні засоби контролю; 2) *організовує взаємодію* правоохоронних та інших державних органів України з Інтерполом, Європолом, а також компетентними органами інших держав з питань, що належать до сфери діяльності Інтерполу та Європолу; 3) *використовує та надає* іншим правоохоронним органам України *доступ* до інформаційно-телекомунікаційних систем і банків даних Інтерполу та Європолу, а також *вносить* до цих банків даних інформацію правоохоронних органів України; 4) *виконує* в межах компетенції *запити* органів правопорядку (правоохоронних органів) інших держав або міжнародних організацій поліції відповідно до закону, міжнародних договорів України, установчих актів та правил міжнародних організацій поліції, членом яких є Україна; 5) *звертається* в межах своєї компетенції *із запитами* до органів правопорядку (правоохоронних органів) інших держав або міжнародних організацій поліції відповідно до закону, міжнародних договорів України, установчих актів та правил міжнародних організацій поліції, членом яких є Україна; 6) у межах інформаційно-аналітичної діяльності *формує* бази (банки) даних, що входять до ЄІС МВС, *користується* базами (банками) даних МВС та інших державних органів, *здійснює* інформаційно-пошукову та інформаційно-аналітичну роботу, а також оброблення персональних даних у межах повноважень, передбачених законом; 7) *забезпечує* в межах повноважень, передбачених законом, *криптографічний захист інформації*, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої визначена законом тощо [54].

Національна поліція для виконання покладених на неї завдань має право – 1) одержувати в установленому законодавством порядку від державних органів та органів місцевого самоврядування, підприємств, установ, організацій незалежно від форми власності та їх посадових осіб, а також громадян та їх об'єднань інформацію, документи і матеріали, необхідні для виконання покладених на неї завдань; 2) користуватися відповідними інформаційними базами даних державних органів, державною системою урядового зв'язку та іншими технічними засобами тощо [54].

Національна поліція України – це центральний орган виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку. Діяльність поліції спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України згідно із законом [3].

Національне центральне бюро Інтерполу в Україні – робочий апарат Укрбюро Інтерполу забезпечує співробітництво правоохоронних органів України та зарубіжних країн як у цілому, так і в окремих напрямках боротьби із злочинністю і надає можливості для: 1) підготовки та надсилання *ініціативних запитів* за кордон; 2) підготовки та надсилання *відповідей на запити* зарубіжних правоохоронних органів; 3) *обміну* оперативно-розшуковою, оперативно-довідковою та криміналістичною інформацією про підготовку і вчинення злочинів та причетних до них осіб, а також архівною та, в окремих випадках, процесуальною інформацією; 4) *обміну* досвідом роботи, законодавчими та іншими нормативними актами, учбово-методичною літературою з питань діяльності правоохоронних органів; 5) *обміну* науково-технічною та іншою інформацією з питань боротьби із злочинністю [95].

Національний реєстр електронних інформаційних ресурсів – це інформаційно-телекомунікаційна система, призначена для реєстрації, обліку, накопичення, оброблення і зберігання відомостей про склад, зміст, розміщення, умови доступу до електронних інформаційних ресурсів та задоволення потреб юридичних і фізичних осіб в інформаційних послугах [63].

НЦБ Інтерполу України відмовляє повністю або частково у виконанні запитів: 1) які *не стосуються компетенції* Інтерполу; 2) які *пов'язані із злочинами* політичного, військового, релігійного чи расового характеру; 3) виконання яких *призведе до порушення:* суверенітету та безпеки України; законодавства України чи держави, куди надсилається запит; прав людини; 4) якщо вони *оформлені з порушенням вимог* відповідної Інструкції; 5) якщо вони надійшли від відомств, установ та організацій, що відповідно до законодавства України *не є правоохоронними органами*; 6) якщо вони надійшли від *фізичних осіб*. Про відмову у виконанні запиту НЦБ письмово інформує ініціатора із зазначенням причин відмови [95].

Об'єкти оперативно-довідкового і дактилоскопічного обліків – є особи, які на території України обвинувачуються у вчиненні злочинів або засуджені, розшукуються, а також громадяни України, що вчинили злочини за її межами і відомості про яких надійшли офіційними каналами згідно з міжнародними договорами у сфері обміну інформацією, які набрали чинності в установленому порядку. Облік здійснюється шляхом ведення алфавітних оперативно-довідкових картотек і дактилоскопічних картотек, у тому числі з використанням автоматизованих банків даних та автоматизованих дактилоскопічних інформаційних систем [97].

Он-лайн будинок юстиції (веб-портал 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* (Веб-портал 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).

Основним завданням взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України – є запобігання кримінальним правопорушенням, їх виявлення та розслідування, притягнення до встановленої законодавством відповідальності осіб, які їх учинили, відшкодування завданої кримінальними правопорушеннями шкоди, відновлення порушених прав та інтересів фізичних і юридичних осіб.

Швидке та повне розслідування і розкриття кримінальних правопорушень досягається шляхом *поєднання зусиль* усіх органів та підрозділів поліції, забезпечення належного рівня їх *взаємодії* відповідно до вимог законодавства щодо отримання, збирання, накопичення та використання *інформації про осіб*, які вчинили кримінальні правопорушення, а також *про події і факти*, які можуть сприяти їх розслідуванню і розкриттю, що є невід’ємним завданням для всіх працівників поліції [90].

Основні завдання АІС ОП – є: 1) підвищення рівня інформаційно-аналітичного забезпечення оперативно-розшукової діяльності Національної поліції України; 2) забезпечення процесу підтримки управлінських рішень керівництвом Національної поліції України; 3) об’єднання отриманої в процесі оперативно-розшукової діяльності Національної поліції України інформації в єдиному інформаційному просторі з використанням сучасних ІТ, комп’ютерного і телекомунікаційного обладнання; 4) протидія злочинності та проведення профілактичної роботи, спрямованої на запобігання вчиненню правопорушень [83].

Основні завдання Департаменту інформатизації МВС України: 1) організовує заходи з впровадження програми інформатизації системи МВС та за дорученням Міністра ЦОВВ, здійснює координацію та моніторинг її виконання; 2) організовує роботу із залучення та реалізації проектів міжнародної технічної допомоги для інформатизації системи МВС та за дорученням Міністра ЦОВВ; 3) готує проекти спільних нормативно-правових актів про електронну інформаційну взаємодію МВС з іншими державними органами; 4) забезпечує організацію взаємодії з інформаційними ресурсами інших державних органів; 5) забезпечує в доступ державних службовців та працівників МВС до інформаційних ресурсів ЄІС МВС та інших державних органів, а також доступ уповноважених представників інших державних органів до інформаційних ресурсів ЄІС МВС; 6) організовує створення та забезпечує функціонування систем інформаційно-аналітичної підтримки діяльності системи МВС та за дорученням Міністра ЦОВВ; 7) безпосередньо розробляє та погоджує розроблені в системі МВС та в ЦОВВ проекти нормативно-правових та інших актів у сферах інформатизації, формування і використання електронних інформаційних ресурсів, інформаційної безпеки та ЕЦП;

8) забезпечує інтеграцію інформаційних ресурсів системи МВС та за дорученням Міністра ЦОВВ у ЄІС МВС; 9) здійснює організаційне та методологічне забезпечення функціонування персонально-довідкового обліку, єдиного державного номерного обліку вогнепальної зброї та інших визначених законодавством обліків; 10) організовує створення та забезпечує функціонування захищеного дата-центру для потреб системи МВС та за дорученням Міністра ЦОВВ; 11) забезпечує функціонування інформаційних, інформаційно-телекомунікаційних систем у МВС та розробляє пропозиції щодо їх розвитку; 12) здійснює заходи, спрямовані на організацію забезпечення правової охорони інтелектуальної власності та легалізації комп'ютерних програм у структурних підрозділах апарату МВС; 13) погоджує заходи щодо закупівлі (передачі) програмного забезпечення в системі МВС та за дорученням Міністра в ЦОВВ; 14) забезпечує адміністрування серверних програмно-технічних комплексів МВС, реєстрацію та адміністрування користувачів сегменту мережі Інтернет та електронної пошти МВС; 15) забезпечує технічну підтримку програмно-технічного комплексу веб-порталу МВС; 16) організовує впровадження та забезпечує контроль функціонування в системі МВС та за дорученням Міністра в ЦОВВ систем управління інформаційною безпекою, аналізує стан кібербезпеки, уживає заходів щодо профілактики кібератак та кіберінцидентів, протидії кіберзагрозам, забезпечення кіберзахисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури системи МВС та за дорученням Міністра ЦОВВ; 17) організовує роботи з проектування, створення, експлуатації та модернізації КСЗІ в інформаційних ресурсах ЄІС МВС (крім тих, де обробляється таємна інформація), а також бере участь у заходах щодо контролю за станом захищеності інформації в інформаційних, інформаційно-телекомунікаційних системах у системі МВС та за дорученням Міністра в ЦОВВ; 18) організовує заходи щодо забезпечення функціонування акредитованого центру сертифікації ключів (далі – АЦСК) МВС та його модернізації; 19) організовує створення представництв АЦСК МВС, супроводжує їх діяльність з питань надання ними послуг електронного цифрового підпису; 20) здійснює за запитами юридичних та фізичних осіб перевірки щодо наявності відповідної інформації в інформаційних ресурсах ЄІС МВС; 21) забезпечує запровадження та розвиток он-лайн сервісів для доступу до відомостей інформаційних ресурсів ЄІС МВС;

22) здійснює інформаційне супроводження діяльності територіальних органів з надання сервісних послуг МВС; 23) забезпечує проведення спеціальної перевірки стосовно осіб, які претендують на зайняття посад, які передбачають зайняття відповідального або особливо відповідального становища, та посад з підвищеним корупційним ризиком у частині наявності в особи судимості, її зняття, погашення; 24) здійснює інші повноваження відповідно до завдань, передбачених цим Положенням та іншими нормативно-правовими актами; 25) забезпечує обслуговування засобів зв'язку та телекомунікацій МВС; 26) забезпечує функціонування телекомунікацій та сервісів ЄЦВТМ МВС; 27) організовує зв'язок та контролює умови технічної експлуатації засобів телекомунікацій пунктів управління МВС, а також забезпечує зв'язком керівництво МВС в умовах надзвичайних ситуацій та під час особливого періоду; 28) забезпечує формування та розподіл відомчого телефонного номерного ресурсу та ресурсу ЄЦВТМ МВС; 29) забезпечує цілодобове функціонування в апараті МВС телефонного зв'язку, підтримку урядового та спеціального зв'язку; 30) координує реалізацію у МВС технічної політики у сфері надання телекомунікаційних послуг, стандартизації, підтвердження відповідності технічних засобів телекомунікацій; 31) контролює належне забезпечення системи МВС та ЦОВВ засобами зв'язку, телекомунікаціями та сервісами ЄЦВТМ МВС відповідно до табелів належності; 32) здійснює моніторинг доступу користувачів до глобальної інформаційної мережі Інтернет, інформаційних мереж МВС та сервісів ЄЦВТМ МВС; 33) упроваджує сучасні технології в галузі зв'язку та телекомунікацій; 34) здійснює погодження технічних завдань та проектної документації на впровадження і розвиток систем зв'язку та телекомунікацій у системі МВС та ЦОВВ; 35) надає консультативну, методичну та практичну допомогу суб'єктам системи МВС та ЦОВВ у формалізації та описі процесів їх діяльності; 36) організовує та здійснює супроводження технічних проектів тощо [84].

Основні завдання єдиної цифрової відомчої телекомунікаційної мережі МВС – це: 1) створення єдиної мережі, яка включатиме логічно окремі мережі для різних користувачів; 2) забезпечення підрозділів (користувачів): усіма видами сучасного відомчого зв'язку та зв'язком мережі загального користування; надійною високошвидкісною передачею даних із доступом до інформаційних баз даних підключених до ЄЦВТМ користувачів та можливістю доступу до необхідних інформаційних ресурсів інших органів державної влади; надійним безперебійним та якісним зв'язком телефонними лініями спецсерії «102» (з подальшою інтеграцією до системи екстреної допомоги населенню за єдиним телефонним номером «112») для отримання від населення повідомлень про кримінальні, адміністративні правопорушення та інші події й оперативного реагування на них; 3) оптимізація інформаційного обміну між підрозділами (користувачами), а також покращення інформаційного обміну з іншими органами державної влади; 4) обмін фінансово-статистичною інформацією для поліпшення функціонування і взаємодії користувачів підрозділів ресурсного та фінансового забезпечення; 5) спрощення надання послуг та сервісів ЄЦВТМ; 6) забезпечення максимальної уніфікації різновидів та кількості діючого обладнання користувачів з метою уникнення непрогнозованого та некерованого зниження якості і ефективності роботи ЄЦВТМ; 7) забезпечення резервування напрямків зв'язку (два незалежні напрямки доступу міжміськими магістральними каналами до МВС обласних користувачів та відповідні резервні зонові й місцеві канали зв'язку); 8) здійснення централізованого моніторингу і керування мережею з єдиного центру оперативно-технічного управління ЄЦВТМ; 9) проведення оперативного перепрограмування та налаштування технічних характеристик обладнання в разі зміни вимог або дислокації користувачів; 10) здійснення централізованого технічного обслуговування та ремонту обладнання мережі; 11) забезпечення комплексу заходів із захисту інформації в ЄЦВТМ [85].

Основні функції територіального сервісного центру МВС – відповідно до чинного законодавства: 1) надає платні та безоплатні послуги; 2) здійснює комплекс заходів, пов'язаних з проведенням державної реєстрації (перереєстрації) та зняттям з обліку призначених для експлуатації на вулично-дорожній мережі загального користування транспортних засобів усіх типів; 3) проводить реєстрацію (перереєстрацію) транспортних засобів з видачою свідоцтв про реєстрацію, тимчасових реєстраційних талонів та номерних знаків на транспортні засоби, здійснення обміну реєстраційних документів та номерних знаків на транспортні засоби, зняття з обліку зареєстрованих транспортних засобів; 4) здійснює в установленому порядку державний облік зареєстрованих транспортних засобів юридичних та фізичних осіб – власників транспортних засобів і формування Єдиного державного реєстру МВС; 5) вносить до Єдиного державного реєстру МВС інформацію про накладення або зняття обмежень щодо транспортних засобів або їх власників; 6) видає довідки про притягнення до кримінальної відповідальності, відсутність (наявність) судимості, її зняття, погашення; 7) взаємодіє з фахівцями експертної служби МВС під час здійснення комплексу заходів із проведення державної реєстрації (перереєстрації) та зняття з обліку транспортних засобів тощо [98].

Отримання відомостей з персонально-довідкового обліку за запитами органів державної влади та їх територіальних органів, органів місцевого самоврядування, установ та організацій, у зв'язку зі здійсненням ними повноважень, визначених законодавством – *Звернення* органів державної влади та їх територіальних органів, органів місцевого самоврядування, установ та організацій, у зв'язку зі здійсненням ними повноважень, визначених законодавством, щодо отримання інформації про наявність чи відсутність в особи судимості та притягнення її до кримінальної відповідальності *реєструється* відповідно до встановлених правил діловодства та *подається* до Департаменту інформатизації або підрозділів інформаційно-аналітичної підтримки НПУ. Надання відомостей з персонально-довідкового обліку або вмотивованої відмови в їх наданні здійснюється протягом 30 календарних днів, якщо інше не передбачено законодавством. Організація надання інформації з даного обліку в *електронному вигляді* визначається Департаментом інформатизації [106].

Отримання відомостей з персонально-довідкового обліку за зверненнями державних органів, які здійснюють правоохоронні функції – Перевірка осіб за персонально-довідковим обліком проводиться за *Вимогою*. Підставою перевірки осіб є проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у межах досудового розслідування та проведення оперативно-розшукових заходів за оперативно-розшуковими справами в порядку, визначеному кримінальним процесуальним законодавством та законодавством про оперативно-розшукову діяльність. У Вимозі *зазначається*: 1) підстава перевірки (із зазначенням номера кримінального провадження або оперативно-розшукової справи); 2) установчі дані особи, яка перевіряється; 3) прізвище, ініціали та посада ініціатора звернення; 4) найменування та місцезнаходження органу ініціатора звернення. Вимога *реєструється* відповідно до встановлених законодавством правил діловодства. Вимога формується *окремо на кожну особу*, яка перевіряється за персонально-довідковим обліком. Установчі дані вносяться *українською та російською мовами*. Прізвище, ім'я та по батькові вживаються в *називному відмінку*. Вимога *підписується* визначеними посадовими особами відповідних підрозділів. Вимога, заповнена з порушенням визначених умов повертається ініціатору звернення без виконання із зазначенням причини повернення. Вимоги *подаються* до підрозділів інформаційно-аналітичної підтримки НПУ. Засекречування їх здійснюється у випадках, коли це викликано службовою необхідністю, з дотриманням вимог законодавства про захист інформації. У підрозділі інформаційно-аналітичної підтримки НПУ вимоги вносяться з робочих місць віддаленого доступу до *електронної форми запиту* для надсилання на перевірку за персонально-довідковим обліком. Надання відомостей з персонально-довідкового обліку на електронний запит здійснюється Департаментом інформатизації у строк до 10 робочих днів, за винятком виконання Вимог щодо осіб, стосовно яких вирішується питання про обрання запобіжного заходу – тримання під вартою, що виконуються протягом доби. Результати перевірки за персонально-довідковим обліком за допомогою спеціалізованого програмного забезпечення надсилаються користувачам, які їх друкують на звороті Вимоги, підписують та надсилають ініціатору запиту [106].

Отримання відомостей з персонально-довідкового обліку за зверненнями судів усіх рівнів – Підставою проведення перевірки осіб за персонально-довідковим обліком з наданням відомостей про це на звернення судів є *судовий розгляд справ* у порядку кримінального або цивільного судочинства. Звернення суду подається у вигляді *Вимоги*, заповненої належним чином, та *підписується* головою суду, його заступниками або суддею, у провадженні якого перебуває справа у порядку кримінального або цивільного судочинства. Звернення судів *подаються* до підрозділів інформаційно-аналітичної підтримки НПУ або Департаменту інформатизації, де з робочого місця віддаленого доступу вносяться до *електронної форми запиту* для надіслання на перевірку за персонально-довідковим обліком. Надання відомостей з персонально-довідкового обліку на електронний запит здійснюється Департаментом інформатизації у строк до 10 робочих днів. Результати перевірки за персонально-довідковим обліком за допомогою спеціалізованого програмного забезпечення надсилаються користувачам, які їх друкують у визначеному порядку та надсилають ініціатору запиту [106].

Отримання відомостей з персонально-довідкового обліку за зверненнями фізичних осіб – Фізична особа, яка досягла 14-річного віку, має право на отримання з персонально-довідкового обліку відомостей про себе. Відомості з обліку надаються Заявнику у формі *Довідки* з дотриманням вимог законодавства про звернення громадян та захист персональних даних на підставі *запиту* на отримання довідки про притягнення до кримінальної відповідальності, відсутність (наявність) судимості або обмежень, передбачених кримінально-процесуальним законодавством України. Запит подається в *письмовій або електронній формі*. Запит у письмовій формі подається особисто Заявником або уповноваженою ним у встановленому порядку особою до Департаменту інформатизації або ТСЦ МВС, незалежно від реєстрації місця проживання Заявника. Заявник під час подання запиту особисто пред'являє документ, що посвідчує його особу, та надає його копію. Запит друкується або заповнюється письмово від руки розбірливими літерами без виправлень. Для замовлення декількох примірників Довідки на запиті вказується їх кількість, яка не може перевищувати трьох одиниць.

Користувач, що приймає запит, *перевіряє* повноту і якість його заповнення, відповідність персональних даних, указаних у запиті, даним документа, що посвідчує особу, та з робочого місця віддаленого доступу *вносить до електронної форми* для перевірки за персонально-довідковим обліком. Запит в електронній формі *подається* за умови ідентифікації Заявника з використанням ЕЦП чи іншого альтернативного засобу ідентифікації особи через офіційний веб-сайт МВС та офіційні веб-сайти ТСЦ МВС. У разі якщо під час роботи із запитом посадовими особами ТСЦ МВС встановлено, що Заявник, який звернувся за Довідкою, *перебуває в розшуку*, – інформується найближчий територіальний орган НПУ. У випадку виявлення даної інформації посадовими особами Департаментом інформатизації – інформується безпосередньо Департамент карного розшуку НПУ. Інформування здійснюється телефоном, факсом або іншим доступним способом з подальшим письмовим повідомленням. Сформована в електронній формі Довідка *завіряється* спеціально призначеним для таких цілей ЕЦП Департаменту інформатизації та надсилається до робочого місця віддаленого доступу, з якого надійшов запит. Посадова особа Департаменту інформатизації або ТСЦ МВС на робочому місці віддаленого доступу *роздруковує* Довідку та *заповнює* серію і номер використаного бланку. У разі якщо інформація, яка надається у відповідь на запит, містить дві сторінки, друга сторінка друкується на зворотному боці бланку. У разі якщо інформація, яка надається у відповідь на запит, містить більше двох сторінок, третя і наступні сторінки друкуються на стандартному аркуші паперу формату А4 або А5. Довідки, надруковані за допомогою інших програмних засобів, є недійсними. Роздрукована Довідка *підписується* заступником керівника Департаменту інформатизації відповідно до розподілу функціональних обов'язків (або особою, яка виконує його обов'язки), керівником ТСЦ МВС (або особою, яка виконує його обов'язки), *скріплюється печаткою* цього органу та видається Заявнику. У разі, якщо Довідка містить *декілька сторінок*, на всіх сторінках проставляється печатка, а остання сторінка Довідки засвідчується заступником керівника Департаменту інформатизації, керівником ТСЦ МВС та видається Заявнику. На вимогу Заявника Довідка, скріплена спеціально призначеним для таких цілей електронним цифровим підписом Департаменту інформатизації, може надаватися на вказану ним *електронну адресу* в з дотриманням вимог законодавства про захист інформації.

У разі незгоди з відомостями, що надані в Довідці, Заявник може надати до Департаменту інформатизації офіційні документи (вирок суду, довідку з місць позбавлення волі тощо) для внесення відповідних змін до персонально-довідкового обліку. Для уточнення наявної в Департаменті інформатизації інформації або установчих даних Заявника, що вказані в запиті, можливе проведення додаткових перевірок за територіальними персонально-довідковими картотеками НПУ або уточнення інформації, наданої в запиті, у посадової особи ТСЦ МВС. *Легітимність* Довідки може бути перевірена через офіційний веб-сайт МВС. У випадку, коли під час опрацювання запиту встановлено, що фізична особа, щодо якої здійснюється запит, *перебуває в розшуку*, відомості про її розшук зазначаються в Довідці незалежно від форми запитуваної довідки. Надання Довідки здійснюється *безоплатно* в строк до 30 календарних днів з дня надходження запиту. Довідка видається станом на дату здійснення перевірки фізичної особи за персонально-довідковим обліком. Фізична особа також має *право* отримати інформацію про те, чи обробляються її персональні дані (далі – ПД) в персонально-довідковому обліку, а також отримувати їх зміст за умови дотримання вимог Закону України «Про захист персональних даних» [6, 106].

Отримання інформації або перевірка тих чи інших відомостей за банками даних Інтерполу – здійснюється: 1) безпосередньо, *в режимі on-line* – через інформаційно-телекомунікаційну систему Інтерполу I-24/7 (банки даних щодо осіб, транспортних засобів, документів, творів мистецтва); 2) 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 [108].

Паспорт набору даних повинен містити такі елементи:

1) ідентифікаційний номер набору даних; 2) найменування набору даних (до 254 символів); 3) стислий опис змісту набору даних (до 4000 символів); 4) підстава та призначення збору інформації, що міститься в наборі даних; 5) відомості про мову інформації, яка міститься у наборі даних; 6) формат (формати), в якому доступний набір даних; 7) формат стиснення набору даних (за наявності такого стиснення); 8) дату і час першого оприлюднення набору даних; 9) дату і час внесення останніх змін до набору даних; 10) дату актуальності даних у наборі даних; 11) періодичність оновлення набору даних; 12) ключові слова, які відображають основний зміст набору даних; 13) гіперпосилання на набір даних (електронний файл для завантаження або інтерфейс прикладного програмування); 14) гіперпосилання на структуру набору даних (електронний файл для завантаження або інтерфейс прикладного програмування); 15) відомості про розпорядника інформації, у володінні якого перебуває набір даних; 16) відомості про відповідальну особу розпорядника інформації, яка відповідає за оприлюднення інформації згідно із Законом України «Про доступ до публічної інформації» [4], та адресу її електронної пошти. Паспорт набору даних може також містити гіперпосилання на попередні версії набору даних, номери версій набору даних, а також інші елементи. Для розміщення паспорта та структури набору даних використовуються формати XSD, JSON, CSV або інші відкриті машиночитані формати [62].

Паспорти на алфавітні та дактилоскопічні картотеки – створюються в Департаменті та управліннях інформаційної служби та містять дані про площу приміщень, які вони займають, їх оснащення, наявність охоронних засобів, санітарний і протипожежний стан, а також відомості про проведені інвентаризації. У ці паспорти щокварталу вносяться дані про кількість облікових карток, розміщених у масивах картотек і вилучених із них [97].

Перевірка за дактилоскопічними картотеками – Здійснюється за наявності оригіналу дактилоскопічної карти з чіткими відбитками на ній десятих пальців рук з контрольними відбитками. Якщо є відбитки не всіх пальців, то з цими дактилокартами працюють експерти-криміналісти [97].

Перевірка наявності вже розпочатих досудових розслідувань – здійснюється за однією ознакою або сукупністю відомостей про кримінальні правопорушення, внесені до ЄРДР всіма Реєстраторами, а саме про: 1) дату вчинення кримінального правопорушення; 2) територію вчинення правопорушення; 3) прізвище, ім'я, по батькові (найменування) потерпілого або заявника; 4) найменування юридичної особи; 5) інше джерело, з якого виявлені обставини, що можуть свідчити про вчинення кримінального правопорушення; 6) прізвище, ім'я, по батькові та дату народження особи, яку повідомлено про підозру [100].

Перевірка осіб за оперативно-довідковим обліком працівниками правоохоронних органів – Здійснюється лише за офіційними запитами. Запит для перевірки особи може бути у вигляді: 1) вимоги; 2) дактилоскопічної карти (долучена до вимоги або окремо); 3) шифротелеграми; 4) мотивованого листа-запиту довільної форми. Вимога друкується *окремо на кожну особу*, що перевіряється. Якщо особа має *декілька прізвищ*, на кожне з них складається окрема вимога. При цьому установчі дані записуються *українською та російською мовами*, чітко, розбірливо, друкованими літерами, в *називному відмінку*. При встановленні наявності інформації про судимість та реєстрацію особи під іншими установчими даними складається *довідка*. Така сама довідка складається при встановленні особи трупа [97].

Перелік автоматизованих систем інформаційно-технологічного забезпечення діяльності Верховної Ради України: 1. «Контроль проходження законопроектів». 2. «Проходження законопроектів у структурних підрозділах Апарату». 3. Комп'ютерна технологія інтегрованої обробки текстів законопроектів для підготовки до розгляду Верховною Радою України («ЗАКОНОТВОРЕЦЬ») (порівняльні таблиці до проектів законодавчих актів). 4. «Автоматизована система документообігу». 5. «Листи та звернення громадян». 6. «Автоматизована система запитів народних депутатів України, доручень Верховної Ради України». 7. «Кадри». 8. Інформаційно-пошукова система (далі – ІПС) «ЗАКОНОДАВСТВО». 9. Система «РАДА». 10. Система «Графіт». 11. Інформаційно-пошукова система «Адміністративно-територіальний устрій України». 12. Програмний комплекс «Відрядження» [71].

Перелік інформації, що подається до Міждержавного інформаційного банку:

1. Відомості про осіб, які підлягають облікові: 1.1. Засуджених, які згідно з нормативними правовими актами держав Сторін підлягають постановці на централізовані оперативно-довідкові обліки. 1.2. Категорії засуджених, зазначених у підпункті 1.1 цього Переліку, які прибули (вибули) для відбування покарання, стосовно яких змінено вироки, і тих, які звільнилися з місць позбавлення волі. 1.3. Осіб, що знаходяться в міждержавному розшуку, бізвісти зниклих, осіб, не здатних за станом здоров'я або за віком повідомити відомості про себе, невідомі труп. 1.4. Організаторів злочинних груп. 1.5. Підозрюваних, які обвинувачуються в скоєнні або яких засуджено за скоєння таких видів злочинів: 1.5.1. Статеві злочини, скоєні з особливою жорстокістю, а також стосовно завідомо неповнолітніх. 1.5.2. Розкрадання культурних, історичних цінностей. 1.5.3. Торгівля людьми, викрадення людини, а також інші злочини, пов'язані з експлуатацією людей. 1.5.4. Виготовлення й розповсюдження порнографічних матеріалів, у тому числі тих, які містять зображення неповнолітніх. 1.5.5. Виготовлення та збут підроблених грошових знаків, цінних паперів, кредитних або розрахункових карт й інших платіжних засобів, а також злочини, скоєні у сфері високих технологій. 1.5.6. Контрабанда. 1.5.7. Організації каналів незаконної міграції. 1.5.8. Незаконний перетин державного кордону. 1.5.9. Розпалювання міжнаціональної, расової та релігійної ворожнечі, а також причетність до діяльності екстремістських, диверсійних і терористичних організацій. 1.5.10. Організація терористичних груп та (або) підготовки й скоєння терористичних актів, а також скоєння злочинів, пов'язаних з легалізацією доходів, отриманих злочинним шляхом, та фінансуванням тероризму. 1.6. Осіб, перерахованих у підпункті 1.5 цього Переліку, у разі зміни раніше поданих облікових даних.

2. Відомості про предмети злочинного зазіхання, загублені, вилучені та безгосподарні речі, знаряддя злочинної діяльності: 2.1. Нарізну вогнепальну зброю. 2.2. Транспортні засоби. 2.3. Історичні та культурні цінності. 2.4. Радіо-, відео-, фото-, комп'ютерну та іншу техніку, яка має індивідуальні номери. 2.5. Номерні цінні папери й документи, що мають державний обіг.

3. Відомості про нерозкриті злочини: 3.1. Вбивства та умисні завдання тяжкої шкоди здоров'ю.

3.2. Статеві злочини, скоєні з особливою жорстокістю, а також стосовно неповнолітніх. 3.3. Розбої, скоєні із застосуванням вогнепальної зброї. 3.4. Шахрайства у великому та особливо великому розмірах. 3.5. Виготовлення та збут підроблених грошових знаків, цінних паперів, кредитних або розрахункових карт й інших платіжних засобів, а також злочини, скоєні у сфері високих технологій. 3.6. *Розкрадання*: 3.6.1. Вогнепальної зброї, боєприпасів, вибухових речовин та підривних пристроїв. 3.6.2. Радіоактивних, отруйних, сильнодійних та отрутних речовин. 3.6.3. Наркотичних засобів і психотропних речовин. 3.6.4. Стратегічно важливих сировинних товарів. 3.6.5. Автотранспорту. 3.6.6. Із сейфів та інших металічних сховищ. 3.6.7. З квартир, скоєних у характерний спосіб. 3.6.8. Культурних й історичних цінностей. 3.7. Пов'язані з незаконними фінансовими, біржовими та валютними операціями. 3.8. Викрадення людей. 3.9. Здирства із застосуванням насилля. 3.10. Торгівлю людьми, органами й тканинами людини. 3.11. Терористичні й диверсійні акти, злочини екстремістської спрямованості. 4. *Статистична інформація про стан злочинності й результати розслідування злочинів в деяких державах* [70].

Періодичність оновлення наборів даних – розпорядник інформації самостійно визначає періодичність оновлення наборів даних, які перебувають у його володінні та оприлюднюються, якщо інше не передбачено законодавством. Може встановлюватися така періодичність оновлення наборів даних: 1) для наборів даних, оприлюднених за допомогою інтерфейсу прикладного програмування, – відразу після внесення змін; 2) для наборів даних, що мають планову періодичність оновлення: більш як один раз на день; щодня; щотижня; щомісяця; щокварталу; кожного півріччя; щороку; 3) для наборів даних, зміни до яких були внесені позапланово, – протягом трьох робочих днів з моменту внесення таких змін [62].

Персонально-довідковий облік – систематизований банк (база) даних інформаційної підсистеми «Оперативно-довідкова картотека» єдиної інформаційної системи Міністерства внутрішніх справ України стосовно осіб, яким повідомлено про підозру в учиненні кримінального правопорушення, та осіб, яких засуджено за вчинення кримінального правопорушення [106].

Персонально-довідковий облік єдиної інформаційної системи МВС України – систематизований банк (база) даних інформаційної підсистеми «Оперативно-довідкова картотека» стосовно осіб, яким повідомлено про підозру в учиненні кримінального правопорушення, та осіб, яких засуджено за вчинення кримінального правопорушення рішень. До її складу входять підсистеми «Мігрант» та «Рубін-2002». Підсистема «Мігрант» – веде облік осіб, затриманих за порушення законодавства України про державний кордон та про правовий статус іноземця. Підсистема «Рубін-2002» – дозволяє реалізувати технології віддаленого оперативного доступу до банків даних з метою введення інформації і перевірки вимог на судимості. *Вимога* – письмове звернення про надання відомостей з персонально-довідкового обліку, що подається державними органами, які здійснюють правоохоронні функції та мають відповідні повноваження. *Довідка* – документ, який містить відомості про притягнення до кримінальної відповідальності, відсутність (наявність) судимості або обмежень, передбачених кримінально-процесуальним законодавством України [106, 110].

Підсистема «Мігрант» – веде облік осіб, затриманих за порушення законодавства України про державний кордон та про правовий статус іноземця [110].

Підсистема «Рубін-2002» – дозволяє реалізувати технології віддаленого оперативного доступу до банків даних з метою введення інформації і перевірки вимог на судимості [110].

Підсистеми у структурі ЄЦВТМ – діють такі підсистеми: 1) телефонного зв'язку; 2) телеграфної кореспонденції; 3) передачі даних апарату МВС, закладів, установ і підприємств, що належать до сфери управління МВС; 4) передачі даних Головного центру з надання сервісних послуг МВС та територіальних центрів з надання сервісних послуг МВС; 5) передачі даних Національної поліції України; 6) передачі даних Національної гвардії України; 7) передачі даних Робочого апарату Укрбюро Інтерполу; 8) передачі даних Державної міграційної служби України; 9) передачі даних інших центральних органів виконавчої влади, діяльність яких спрямовує та координує Міністр внутрішніх справ України; 10) селекторних аудіо- та відеоконференцзв'язку; 11) трансляції зображень з камер внутрішнього та зовнішнього відеоспостереження [85].

Підходи, якими керується МВС щодо забезпечення реалізації цілей Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року – 1) служіння суспільству; 2) підзвітність і демократичний цивільний контроль; 3) залучення суспільства до процесу створення безпечного середовища; 4) застосування сучасних методів державного управління; 5) інформатизація діяльності (передбачає підвищення ефективності роботи і взаємодії органів системи МВС шляхом максимального використання інформаційно-комунікаційних технологій) [56].

Повноваження МВС щодо функціонування єдиної інформаційної системи МВС – здійснює організаційне забезпечення функціонування єдиної інформаційної системи МВС, а також визначає права і обов'язки персоналу служби та адміністратора єдиної інформаційної системи МВС [52].

Повноваження поліції у сфері інформаційно-аналітичного забезпечення – поліція в рамках інформаційно-аналітичної діяльності: 1) формує бази (банки) даних, що входять до ЄІС МВС України; 2) користується базами (банкami) даних МВС 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 [8].

Поліція забезпечує збирання, накопичення мультимедійної інформації та біометричних даних – збирання, накопичення мультимедійної інформації (фото, відео-, звукозапис) та біометричних даних (дактилокартки, зразки ДНК) здійснюється під час наповнення баз (банків) даних, визначених у п 7 ч. 1 ст. 26 Закону України «Про Національну поліцію», а саме: стосовно 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].

Порядок взаємодії Генеральної прокуратури України та Міністерства внутрішніх справ України щодо обміну інформацією з Єдиного реєстру досудових розслідувань та інформаційних систем МВС – 1) суб'єктами інформаційної взаємодії є: органи прокуратури та МВС України; 2) при здійсненні обміну даними задіяні електронні інформаційні ресурси: а) Генеральної прокуратури України – Єдиний реєстр досудових розслідувань; б) Міністерства внутрішніх справ України – автоматизовані інтегровані інформаційно-пошукові системи (далі – ІПС); 3) обмін даними здійснюється інформаційно-телекомунікаційними засобами в електронному вигляді; 4) об'єм інформації ЄРДР, за винятком даних щодо руху кримінальних проваджень, об'єм інформації ІПС МВС, технічні специфікації реалізації механізмів обміну інформацією, форматів даних та терміни виконання вказаних заходів визначаються спільним протоколом Управління статистики, організації та ведення Єдиного реєстру досудових розслідувань, Управління інформатизації і зв'язку Генеральної прокуратури та Департаменту інформатизації і Департаменту державного майна та ресурсів МВС України; 4) Генеральна прокуратура України надає МВС України відомості з ЄРДР про правопорушення, що виявлені або провадження за якими здійснюється працівниками органів поліції, осіб, яким вручено повідомлення про підозру та стосовно яких закінчено досудове розслідування у кримінальному провадженні, у форматі атрибутів, визначених спільним протоколом; 5) ці дані після внесення у встановленому порядку до ЄРДР формуються автоматично та відповідно до технічної специфікації стають доступними інформаційним системам МВС України; 6) відомості про результати судового розгляду кримінального провадження стосовно особи формуються з інформаційних систем Державної судової адміністрації України та відповідно до технічної специфікації стають доступними автоматизованим інформаційним системам МВС України із ЄРДР; 7) Міністерство внутрішніх справ України забезпечує доступ суб'єктів інформаційної взаємодії до ІПС та їх реєстрацію згідно вимог чинного законодавства і з урахуванням їх повноважень та рівня доступу; 8) доступ до ІПС МВС працівникам органів прокуратури забезпечується одночасно з під'єднанням робочих місць до Єдиної відомчої телекомунікаційної мережі Міністерства внутрішніх справ України [102].

Порядок взаємодії Міністерства внутрішніх справ України з центральними органами виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України – визначає організаційні та процедурні питання взаємодії Міністерства внутрішніх справ України з Національною поліцією України, Державною міграційною службою України, Адміністрацією Державної прикордонної служби України, Державною службою України з надзвичайних ситуацій, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України (далі – Служба), у процесі формування та реалізації державної політики у відповідних сферах. Цей Порядок спрямовано на забезпечення узгодженості, плановірності та цілісності формування державної політики, а також ефективності її реалізації у сферах охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, забезпечення публічної безпеки і порядку, надання поліцейських послуг, міграції (імміграції та еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів, захисту державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні, у сферах цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності. Організація опрацювання документів, які надсилаються зі Служб до МВС, відповідно до цього Порядку покладається на Управління відповідно до компетенції. Строк опрацювання в МВС проєктів нормативно-правових актів, розроблених Службою, визначається в межах, встановлених законодавством, якщо Службою не встановлено іншого обґрунтованого терміну виконання. Строк опрацювання в МВС нормативно-правових актів, розроблених центральними органами та надісланих Службою для погодження своєї позиції, становить 15 робочих днів з дня, наступного після надходження його до МВС [103].

Порядок внесення відомостей до ЄРДР – Внесення відомостей здійснюється шляхом фіксації Реєстратором інформації в ЄРДР та вибору даних у довідниках для заповнення електронних карток про: 1) кримінальне правопорушення; 2) наслідки досудового розслідування кримінального правопорушення; 3) заподіяні збитки, результати їх відшкодування та вилучення предметів злочинної діяльності; 4) особу, яка вчинила кримінальне правопорушення та яка підозрюється у його вчиненні; 5) рух кримінального провадження. Установлений перелік реквізитів електронних карток, довідників є єдиним для Реєстраторів усіх правоохоронних органів. Унесення змін та доповнень до них здійснює Держатель Реєстру. 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 [100].

Порядок дій органів (підрозділів) Національної поліції в разі виявлення осіб, транспортних засобів і документів, відомості щодо яких містяться в банках даних інформаційної системи Міжнародної організації кримінальної поліції – Інтерполу – визначає чітку послідовність дій та механізм взаємодії поліцейських у разі виявлення осіб, транспортних засобів і документів, відомості щодо яких містяться в банках даних інформаційної системи Інтерполу, та/або таких, інформація про які отримана органами (підрозділами) НПУ під час здійснення службової діяльності та місцезнаходження яких невідоме. Порядок містить дії поліцейського, керівника уповноваженого територіального підрозділу, уповноваженого підрозділу у разі: 1) виявлення особи, щодо якої в банках даних є відомості, що передбачають її затримання (арешт) та подальшу екстрадицію; 2) виявлення особи, щодо якої в банках даних є відомості, що не передбачають затримання (арешт) цієї особи; 3) виявлення особи, щодо якої в банках даних є відомості як про зниклу безвісти особу; 4) виявлення транспортного засобу, щодо якого в банках даних є інформація як про викрадений; 5) виявлення збігу даних про викрадені/втрачені чи визнані недійсними документи, інформація про які міститься в банках даних, з даними документів, отриманих із джерел інформації про вчинені кримінальні правопорушення та інші події [105].

Порядок оголошення в Україні в розшук Інтерполу (<https://antikor.com.ua/articles/274830>) – В Україні стадії цього процесу виглядають наступним чином: 1) У разі, якщо у компетентного правоохоронного органу є підстави вважати, що особа, яка проходить по справі перебуває за межами України, в такому разі посадова особа цього органу направляє запит до Департаменту міжнародного поліцейського співробітництва НПУ. 2) Після отримання запиту співробітники НЦБ здійснюють його первинну перевірку на предмет правильності оформлення й відповідності національному та міжнародному законодавству. 3) За результатами цієї перевірки НЦБ пересилає запит до Генерального секретаріату Інтерполу. 4) Генеральний секретаріат здійснює повторну перевірку запиту. 5) У разі успішного проходження цієї перевірки Генеральний секретаріат публікує оголошення в розшук запитуваної особи, повідомляючи при цьому всі країни-учасниці Інтерполу. 6) Опісля, у разі встановлення місцезнаходження та затримання особи (у випадку з обвинуваченим чи засудженим), компетентний орган країни- перебування цієї особи (в Україні – суд) приймає рішення стосовно її екстрадиції державі, яка здійснила запит щодо неї. Повідомлення щодо оголошення в розшук публікується у вигляді так званої «картки» (notices). Більшість з «карток» є непублічними, а ту решту, яким все ж таки було надано розголосу, розміщуються на офіційному сайті Інтерполу. В залежності від мети розшуку «картки» (а точніше її лівому куту) надається наступний колір: 1) *червоний* (розшук осіб з метою їх арешту та екстрадиції); 2) *блакитний* (збирання матеріалів щодо певної особи в інтересах слідства); 3) *зелений* (інформування щодо потенційних злочинців, якими зазвичай є рецидивісти); 4) *жовтий* (пошук зниклих безвісти осіб); 5) *чорний* (встановлення особи невпізнаних трупів); 6) *фіолетовий* (пошук або інформування стосовно злочинних схем, знарядь злочинів, способів їх вчинення); 7) *помаранчевий* (попередження щодо існування загрози життю, здоров'ю та майну людей); 8) *блакитно-біла* (використовується для позначення груп осіб або індивідів, які перебувають під санкціями Радбезу ООН). В рамках Інтерполу існує ще один механізм міжнародного розшуку особи, який має назву «розсилка» (diffusion). «Розсилка» спрямовується від НЦБ безпосередньо до інших країн-членів, оминаючи Генеральний секретаріат. Таким чином, diffusions є менш формальними, але, як і notices, вони так само мають відповідати Конституції Інтерполу.

Права Департаменту інформатизації МВС України:

1) отримувати в установленому порядку від суб'єктів системи МВС та ЦОВВ інформацію, необхідну для виконання покладених на Департамент завдань; 2) доступу в установленому порядку до інформаційних ресурсів системи МВС і ЦОВВ та інших інформаційних ресурсів відповідно до законодавства; 3) здійснювати перевірки стану дотримання вимог законодавства щодо правової охорони інтелектуальної власності та легалізації комп'ютерних програм у системі МВС та за дорученням Міністра в ЦОВВ; 4) розробляти проекти договорів не фінансового характеру щодо інформаційної взаємодії, надання інформаційних послуг, проведення експертиз тощо; 5) створювати комісії та робочі групи з питань, що належать до компетенції Департаменту; 6) брати участь у нарадах, конференціях, семінарах тощо на території України та за її межами, а також у роботі консультативних, дорадчих та інших допоміжних органів за напрямками діяльності Департаменту; 7) за дорученням керівництва МВС у межах компетенції Департаменту представляти інтереси Міністерства в державних органах, органах місцевого самоврядування, міжнародних організаціях; 8) доступу до службових приміщень системи МВС та за дорученням Міністра ЦОВВ, у яких експлуатуються засоби інформаційних, інформаційно-телекомунікаційних систем, а також до відповідних документів для перевірки діяльності суб'єктів забезпечення кібербезпеки, стану впровадження систем управління інформаційною безпекою та повноти виконання заходів з інформаційної безпеки; 9) тимчасово блокувати доступ користувачів до інформаційних, інформаційно-телекомунікаційних систем у МВС у разі виявлення порушень встановлених правил інформаційної безпеки; 10) відповідно до законодавства отримувати і перевіряти документи та інформацію, що необхідні для надання послуг ЕЦП; 11) надавати в установленому порядку державним службовцям та працівникам апарату Міністерства, його територіальних органів з надання сервісних послуг МВС, Державного науково-дослідного інституту та Державного науково-дослідного експертно-криміналістичного центру в користування надійні засоби ЕЦП, захищені носії особистих ключів, вести їх облік та здійснювати контроль за їх використанням; 12) брати участь у заходах щодо стандартизації обліково-реєстраційних документів, розроблення проектів форм державної та відомчої звітності за напрямками діяльності МВС [84].

Приклади інформаційно-довідкових обліків експертно-криміналістичного призначення – це 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 підшов 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 [108].

Приклади оперативних обліків – це: 1) оперативно-розшукові; 2) оперативно-профілактичні; 3) оперативно-довідкові.

Приклади оперативно-пошукових обліків експертно-криміналістичного призначення – це: 1) дактилоскопічні обліки; 2) колекції слідів злomu; 3) колекції слідів взуття; 4) колекції слідів транспортних засобів; 5) колекції волокон; 6) колекції замків і ключів; 7) колекції фальшивих грошей; 8) колекції підроблених рецептів і бланків документів; 9) колекції кулегільзотеки; 10) колекції суб'єктивних портретів; 11) колекція фонограм з голосами осіб, які анонімно повідомляли про загрозу вибуху тощо [108].

Принципи формування загальновідомчих та галузевих інформаційних підсистем, які складають основу системи інформаційного забезпечення органів Національної поліції: 1) функціонального призначення; 2) нормативно-правової забезпеченості; 3) фактичності даних; 4) доцільності впровадження та експлуатації; 5) нарощення та розвитку.

Реєстр оприлюднених наборів даних – на Єдиному державному веб-порталі відкритих даних ведеться реєстр оприлюднених наборів даних у форматі відкритих даних, який дає змогу ідентифікувати кожен з оприлюднених наборів даних, отримати їх метадані, зокрема гіперпосилання для доступу до набору даних в Інтернеті. Реєстр повинен містити щонайменше такі відомості: 1) ідентифікаційний номер набору даних; 2) найменування набору даних (до 254 символів); 3) формати, в яких доступний набір даних; 4) гіперпосилання на сторінку набору даних. Реєстр оприлюднених наборів даних розміщується в одному з таких відкритих машиночитаних форматів з метою повторного використання: CSV, XML, JSON, RDFa, HTML Microdata тощо [62].

Реєстратори ЄРДР – це: 1) прокурори, у тому числі керівники прокуратур; 2) керівники органів досудового розслідування; 3) слідчі органів прокуратури, поліції, безпеки, органів, що здійснюють контроль за додержанням податкового законодавства та органів Державного бюро розслідувань; детективи підрозділів детективів та внутрішнього контролю Національного антикорупційного бюро України, уповноважені здійснювати досудове розслідування кримінальних правопорушень [74, 100].

Реєстрація заяв і повідомлень про вчинені кримінальні правопорушення та інші події – присвоєння кожній отриманій заяві і повідомленню про вчинене кримінальне правопорушення та іншу подію порядкового номера і фіксація у відповідних облікових документах стислих даних про заяви і повідомлення про вчинені кримінальні правопорушення та інші події [80].

Реєстри веб-порталу Міністерства юстиції України («Веб-портал Міністерства юстиції України» → «Відкриті дані» → «Інформація з Реєстрів у форматі відкритих даних», <https://minjust.gov.ua/information-from-register>) – це: 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 посиленних 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».

Рівні доступу для отримання інформації від НЦБ Інтерполу в Україні – встановлюються три рівні доступу до інформації: 1) *рівень 1* – щодо інформації, яку НЦБ може розповсюджувати без будь-яких обмежень; 2) *рівень 2* – щодо інформації, розповсюдження якої можливе тільки на підставі дозволу НЦБ чи органу-ініціатора її надсилання в Укрбюро Інтерполу; 3) *рівень 3* – щодо інформації, розповсюдження якої можливе лише з дозволу Міністра внутрішніх справ України або його заступників. Рівень доступу до інформації *встановлюється* НЦБ або органом-ініціатором її надсилання в Укрбюро Інтерполу. Орган, який надсилає інформацію до НЦБ, може спеціально зазначити, що відомості чи їх джерело не можна розкривати будь-кому або обмежити коло осіб, які можуть знайомитися з цією інформацією. Якщо в документі *відсутня вказівка* на рівень доступу до інформації, вона видається і обробляється згідно з правилами, встановленими для рівня 1 [95].

Робоче місце віддаленого доступу до персонально-довідкового обліку – спеціалізоване програмне забезпечення, що дозволяє надсилати запити та отримувати відомості з персонально-довідкового обліку [106].

Розпорядник АІС ОП – це Департамент інформаційно-аналітичної підтримки. Повноваження розпорядника АІС ОП на регіональному рівні надаються управлінням інформаційно-аналітичної підтримки. Розпорядник системи АІС ОП забезпечує управління (адміністрування) АІС ОП, контроль за формуванням та підтриманням в актуальному стані інформаційних ресурсів, надання користувачам прав доступу до АІС ОП, ведення їх обліку, ужиття заходів щодо розвитку і вдосконалення АІС ОП [83].

Розпорядник інформації, яка обробляється в АІС ОП – це Національна поліція України. Розпорядник вживає заходів із організації матеріально-технічного та кадрового забезпечення, що необхідні для ефективного функціонування системи [83].

Розшукові обліки на веб-порталі МВС України (<https://wanted.mvs.gov.ua>) – розміщено «РОЗШУК МВС УКРАЇНИ», який містить 10 БД. Даний пошуковий ресурс є копією офіційної бази МВС України і періодично оновлюється. Даний веб-ресурс призначений для надання допомоги органам та підрозділам НПУ:

1) зі встановлення місцезнаходження безвісті зниклих людей (БД «Зниклі громадяни»); 2) зі встановлення невпізнаних трупів (БД «Неопізнані трупи»); 3) з пошуку викрадених культурних цінностей (БД «Культурні цінності»); 4) з пошуку викрадених мобільних телефонів (БД «Мобільні телефони»); 5) з пошуку зброї, яка знаходиться у розшуку (БД «Зброя у розшуку»); 6) з пошуку транспортних засобів, які знаходяться у розшуку (БД «Транспортні засоби у розшуку»); 7) з розшуку тих осіб, хто переховується від органів влади (БД «Особи, які переховуються від органів влади»); 8) зі встановлення осіб, які втратили пам'ять (БД «Особи, що не можуть надати про себе відомостей внаслідок хвороби або неповнолітнього віку»); 9) зі встановлення легітимності довідки про судимість (БД «Перевірка легітимності довідки про судимість»); 10) з пошуку паспортів громадян України, які викрадені або втрачені (БД «Пошук паспорта громадянина України серед викрадених та втрачених»). На сайті також представлено детальну інформацію, куди громадянин може звернутися за вказаними телефонами, або зателефонувавши 102. Органи НПУ висловлюють вдячність за будь-яку допомогу.

Сервіс єдиної інформаційної системи МВС – спеціальний програмний засіб, що забезпечує доступ користувачів ЄІС МВС до інформаційних ресурсів єдиної інформаційної системи МВС [52].

Система інформаційного забезпечення органів 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 телекомунікаційних технологій; 5) матеріально-технічного та фінансового забезпечення [108].

Системний адміністратор центрального вузла АІС ОП – це працівник ДІАП, який згідно зі своїми функціональними (посадовими) обов'язками відповідає за експлуатацію програмно-технічного комплексу АІС ОП. Він координує діяльність системних адміністраторів регіональних вузлів (працівників УІАП) та відповідає за: 1) цілодобове функціонування програмно-технічного комплексу АІС ОП; 2) підключення нових або відключення існуючих апаратних модулів; 3) резервне копіювання системи; 4) інсталяцію програмних продуктів; 5) діагностику системи [83].

Склад Національного реєстру електронних інформаційних ресурсів – містить еталонний, робочий, страховий та інформаційний фонди. 1) *Еталонний фонд* – інформаційна система, призначена для накопичення, зберігання та обліку в контрольному стані відомостей про склад, зміст, розміщення та умови доступу до е-ресурсів. 2) *Інформаційний фонд* – інформаційна система загального доступу користувачів до відомостей Національного реєстру, яка містить копії його еталонного фонду. 3) *Робочий фонд* – інформаційна система, призначена для оброблення відомостей про склад, зміст, розміщення та умови доступу до е-ресурсів, інших робіт та внесення цих відомостей до Національного реєстру. 4) *Страховий фонд* – архівні копії еталонного фонду Національного реєстру, призначені для його відновлення у разі повної або часткової втрати [63].

Склад регіонального вузла АІС ОП – до нього належать: 1) *регіональний сервер баз даних, програмне забезпечення*, призначене для зберігання та обробки інформаційних ресурсів, *системні журнали реєстрації* роботи користувачів, програмних та технічних засобів, що входять до складу КСЗІ; 2) *комутаційний центр*, призначений для виконання функції комутації та маршрутизації потоків інформації АІС ОП у захищених локальних мережах УІАП; 3) *автоматизоване робоче місце адміністратора системи керування базами даних* регіонального вузла АІС ОП, що є складовою КСЗІ регіонального вузла і призначене для моніторингу системних журналів реєстрації роботи програмних та технічних засобів, аналізу порушень у роботі системи, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів регіонального вузла; 4) *автоматизоване робоче місце адміністратора безпеки*, що є складовою КСЗІ регіонального вузла і призначене для реалізації технології надання доступу користувачам до інформації в системі відповідно до наданих розпорядником АІС ОП прав доступу, моніторингу системних журналів реєстрації роботи користувачів та програмних засобів; 5) *автоматизовані робочі місця, що забезпечують авторизований доступ користувачів АІС ОП до інформаційних ресурсів (баз даних) регіонального вузла УІАП* [83].

Склад центрального вузла АІС ОП – до нього належать:

1) *центральный сервер баз даних, система керування базами даних, програмне забезпечення*, призначене для зберігання та обробки інформаційних ресурсів, *системні журнали реєстрації роботи користувачів, програмні та технічні засоби КСЗІ*; 2) *комутаційний центр*, призначений для виконання функції комутації та маршрутизації потоків інформації АІС ОП у захищеній локальній мережі ДІАП; 3) *автоматизоване робоче місце адміністратора системи керування базами даних* центрального вузла АІС ОП, що є складовою КСЗІ центрального вузла і призначене для моніторингу системних журналів реєстрації роботи програмних та технічних засобів, аналізу порушень у роботі системи, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів центрального вузла; 4) *автоматизоване робоче місце адміністратора безпеки*, що є складовою КСЗІ центрального вузла і призначене для реалізації технології надання доступу користувачам до інформації в системі відповідно до наданих розпорядником АІС ОП прав доступу, моніторингу системних журналів реєстрації роботи користувачів та програмних засобів; 5) *автоматизовані робочі місця*, що забезпечують авторизований доступ користувачів АІС ОП до інформаційних ресурсів центрального банку даних АІС ОП [83].

Склад центральної підсистеми єдиної інформаційної системи

МВС – до нього належать: 1) *центральне сховище даних* – програмно-технічний комплекс, який складається із серверів баз даних та програмного забезпечення, призначених для безперервної обробки та зберігання інформації, ведення та зберігання системних журналів аудиту роботи користувачів єдиної інформаційної системи МВС, системних журналів реєстрації роботи програмних засобів і журналів аудиту засобів безпеки; 2) *центральный сервер обробки даних* – програмно-технічний комплекс, який складається з основного та резервних серверів, баз даних, програмного забезпечення, призначених для безперервного виконання операцій з інформаційного обміну між центральним сховищем даних та суб'єктами і користувачами ЄІС МВС, записування та зберігання системних журналів аудиту приймання-передачі інформації;

3) *сервери додатків* – програмно-технічні комплекси, які складаються із серверів та програмного забезпечення, призначених для безперервного функціонування програмних засобів обробки інформації в інтерактивному режимі реального часу, архівування та синхронізації інформації, записування та зберігання системних журналів аудиту приймання-передачі інформації, реєстрації роботи програмних засобів і журналів аудиту засобів безпеки; 4) *шлюзові сервери* – програмно-технічні комплекси, які складаються із серверів та програмного забезпечення, призначених для забезпечення захисту інформації під час її приймання та передавання до центрального сховища даних, а також для запобігання можливості блокування доступу до програмно-апаратних ресурсів єдиної інформаційної системи МВС; 5) *інші сервери та телекомунікаційне обладнання*, які можуть використовуватися в разі розширення завдань та функцій єдиної інформаційної системи МВС у процесі її роботи; 6) *автоматизовані робочі місця користувачів центральної підсистеми єдиної інформаційної системи МВС* – робочі місця, обладнані програмно-технічними засобами доступу до відповідних програмно-інформаційних комплексів функціональних підсистем ЄІС МВС, призначені для забезпечення користувачам можливості обробляти інформацію відповідно до наданих прав; 7) *автоматизовані робочі місця адміністраторів центральної підсистеми ЄІС МВС* – робочі місця, обладнані технічними засобами та програмним забезпеченням, призначеними для моніторингу системних журналів реєстрації роботи програмних засобів, аналізу порушень у роботі ЄІС МВС, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів центральної підсистеми єдиної інформаційної системи МВС; 8) *автоматизовані робочі місця адміністраторів безпеки єдиної інформаційної системи МВС* [52].

Служба єдиної інформаційної системи МВС – МВС України визначає структурний підрозділ апарату Міністерства, який забезпечує реалізацію пріоритетних напрямів інформатизації системи МВС та центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ [52]. Станом на сьогодні – це Департамент інформатизації МВС України.

Стратегічні пріоритети розвитку органів системи МВС на період до 2020 року – це: 1) створення безпечного середовища; 2) протидія злочинності; 3) дотримання та забезпечення прав людини; 4) ефективне інтегроване управління державним кордоном і збалансована міграційна політика; 5) забезпечення якості і доступності адміністративних послуг; 6) ефективне врядування, прозорість і підзвітність; 7) розвиток кадрового потенціалу та соціальний захист працівників.

1. Створення безпечного середовища – подолання викликів планується здійснювати такими шляхами: 1) упровадження та розвиток системи управління силами та засобами реагування в надзвичайних ситуаціях та екстреної допомоги населенню за єдиним телефонним номером 112 згідно з міжнародними нормами та правилами тощо. *2. Протидія злочинності* – подолання викликів здійснюватиметься такими шляхами: 1) розроблення і впровадження єдиної електронної системи роботи з даними і матеріалами досудових розслідувань у взаємодії з органами прокуратури і судами для забезпечення безперервності та підконтрольності проведення досудового розслідування; 2) запровадження використання різних джерел інформації в діяльності органів системи МВС, комплексне впровадження сучасних систем кримінального аналізу, в тому числі методології Європолу з оцінки загроз тяжких злочинів та організованої злочинності (SOCTA); 3) забезпечення належного рівня технічного і матеріального оснащення органів досудового розслідування і використання в їх діяльності сучасних експертно-криміналістичних засобів тощо. *3. Дотримання та забезпечення прав людини* – подолання викликів здійснюватиметься такими шляхами: 1) введення автоматизованого обліку затриманих осіб тощо. *4. Ефективне інтегроване управління державним кордоном і збалансована міграційна політика* – подолання викликів здійснюватиметься такими шляхами: 1) запровадження в органах системи МВС механізму приведення інформації про особу, що міститься в наявних державних та єдиних реєстрах, інших інформаційних базах, що перебувають у власності держави або підприємств, установ і організацій та використовуються з метою проведення ідентифікації осіб, у відповідність з єдиним ідентифікатором – унікальним номером запису в Єдиному державному демографічному реєстрі;

2) поширення використання документів, що посвідчують особу, підтверджують громадянство України чи спеціальний статус, які містять біометричні дані, і розвиток технічної інфраструктури їх застосування; 3) розвиток міжнародного співробітництва щодо обміну даними для забезпечення охорони та захисту державного кордону і дотримання міграційного режиму тощо. 5. *Якість і доступність адміністративних послуг* – подолання викликів здійснюватиметься такими шляхами: 1) упровадження сервіс-орієнтованого підходу в діяльності органів системи МВС; 2) забезпечення дерегуляції і спрощення процедур; 3) розширення доступності адміністративних послуг шляхом делегування повноважень з їх надання іншим уповноваженим суб'єктам; 4) побудова ефективної системи комунікації, пов'язаної з наданням адміністративних послуг тощо. 6. *Ефективне урядування, прозорість і підзвітність* – подолання викликів здійснюватиметься такими шляхами: 1) упровадження кращого управлінського досвіду в органах системи МВС і підтримка реалізації пілотних проектів; 2) розвиток електронного урядування в органах системи МВС; 3) об'єднання і захист інформаційних ресурсів органів системи МВС у межах єдиного інтегрованого інформаційного середовища; 4) упровадження сучасного авторизованого доступу користувачів до інформаційних ресурсів органів системи МВС та надання їм доступу до відкритих даних органів системи МВС і власних персональних даних; 5) підготовка інформаційних систем МВС до приєднання до Шенгенської інформаційної системи; 6) поглиблення і розширення знань, умінь та навичок працівників органів системи МВС у роботі з інформаційними системами, тощо. 7. *Розвиток кадрового потенціалу та соціальний захист працівників* – подолання викликів здійснюватиметься такими шляхами: 1) розвиток відомчої системи освіти та підготовки кадрів, яка відповідає професійним потребам персоналу органів системи МВС і сприяє формуванню його загальних цінностей; 2) розроблення і впровадження програм безперервного професійного розвитку персоналу тощо [56].

Строки зберігання інформації, порядок видалення та знищення інформації в єдиній інформаційній системі МВС – визначаються положеннями про відповідні функціональні підсистеми ЄІС МВС з урахуванням вимог законодавства [52].

Структура АІС ОП – побудована за такими рівнями: *перший рівень* – центральний вузол АІС ОП – розташовується в службових приміщеннях ДІАП, де накопичується та систематизується узагальнена інформація, здобута в результаті оперативно-розшукової діяльності Національної поліції України; *другий рівень* – регіональні (обласні) вузли АІС ОП – розташовуються в службових приміщеннях УІАП, де накопичується та систематизується інформація, здобута в результаті оперативно-розшукової діяльності Національної поліції України, за територіальним принципом [83].

Структура єдиної інформаційної системи МВС – складається з постійно діючих: 1) центральної підсистеми; 2) функціональних підсистем; 3) транспортної мережі передачі даних; 4) центрів обробки даних, телекомунікаційних мереж суб'єктів єдиної інформаційної системи МВС; 5) комплексних систем захисту інформації підсистем єдиної інформаційної системи МВС з підтвердженою в установленому законодавством порядку відповідністю [52].

Структура ЄЦВТМ – у системі ЄЦВТМ виділяються три основні рівні: I – апарати МВС та центральних органів виконавчої влади, діяльність яких спрямовує та координує Міністр внутрішніх справ України; II – територіальні органи, у тому числі міжрегіональні підрозділи в Автономній Республіці Крим, областях, містах Києві та Севастополі; III – територіальні органи та підрозділи в районах, містах, районах у містах [85].

Структура та порядок роботи функціональних підсистем єдиної інформаційної системи МВС – визначаються положеннями про ці підсистеми, які розробляються суб'єктами єдиної інформаційної системи МВС з урахуванням затвердженого МВС Типового положення про функціональну підсистему єдиної інформаційної системи МВС та затверджуються в установленому законодавством порядку [52].

Суб'єкти АІС ОП – це: 1) розпорядник інформації, яка обробляється в АІС ОП; 2) розпорядник АІС ОП; 3) адміністратор безпеки центрального вузла АІС ОП; 4) адміністратор бази даних центрального вузла АІС ОП; 5) системний адміністратор центрального вузла АІС ОП; 6) користувачі АІС ОП [83].

Суб'єкти єдиної інформаційної системи МВС – апарат МВС та його територіальні органи з надання сервісних послуг МВС, Національна гвардія, заклади, установи і підприємства, що належать до сфери управління МВС, центральні органи виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ, інші державні органи, які обробляють інформацію в єдиній інформаційній системі МВС для реалізації своїх повноважень [52].

Телекомунікаційна система Інтерполу I-24/7 (Інтерпол 24 години на добу – сім днів на тиждень) – це захищена від стороннього доступу глобальна телекомунікаційна система з обмеженим колом користувачів, яка не має аналогів в світі і є ефективним інструментом міжнародного співробітництва правоохоронних органів. Вона створена у 2003 році на основі протоколу передачі даних TCP/IP. Головний сервер розташований в м. Ліон (Франція). Цією системою користуються правоохоронні органи 192 країн. Україна – в десятці лідерів за якістю і інтенсивності співробітництва з МОКП-Інтерпол: за 3 роки кількість запитів до баз даних зросла майже в 370 разів і на сьогодні склала 34,7 млн. Кожну секунду Інтерпол обробляє 3 українських запити! (джерело: <https://censor.net.ua/ua/p463715>). Технології пошуку інформації: FIND – фіксована система бази даних Інтерполу (система підключена безпосередньо до Генерального секретаріату Інтерполу); MIND – мобільна система бази даних Інтерполу. Бази та банки даних Інтерполу: 1) *Банк зображень про знущання над дітьми* (складається з понад 520 тис. зображень, за допомогою програмного забезпечення дозволяє відсортувати зображення за фотосесією чи місцем зйомки, з моменту створення допоміг близько 700 жертвам); 2) *База даних «Розшук терористів»* (дані про 9 тис. осіб від 120 країн); 3) *база даних «Розшук»* (база Nominal Data містить інформацію про 178 тис. осіб, з них близько 600 надані Україною) (включно фотографії, імена, відбитки пальців осіб, які перебувають у міжнародному розшуку, зникли без звістки, а також дані про неідентифіковані трупи); 4) *Автоматична дактилоскопічна ідентифікаційна система* (ідентифікує в автоматичному режимі осіб на основі відбитків, поповнюється Національними бюро Інтерполу за допомогою єдиної форми чи за допомогою файлового формату NIST, налічує 80 тис. дактилограм);

5) Ідентифікаційна система на основі ДНК (вміщує в себе 77 тис. зразків, які надані 47 країнами світу); 6) База даних «Загублені та вкрадені документи» (вміщує в себе дані про 149 млн посвідчень осіб, які надані 133 країнами (Україною надано відомостей про близько 61 тис. документів), та 190 тис. інших документів); 7) База даних «Вкрадені предмети мистецтва» (дані про близько 32 тис. вкрадених виробів мистецтва); 8) База даних «Вкрадені транспортні засоби» (занесено 4,7 млн транспортних засобів (Україною надано відомості про близько 11 тис. засобів). Згідно з офіційним сайтом Інтерполу користувачі системи мають миттєвий онлайн доступ (через Національне бюро) до наступних баз даних в Україні: «Особи в розшуку», «Зниклі особи», «Вкрадені транспортні засоби», «Вкрадене майно», «Притягнення до кримінальної відповідальності», «Реєстрація транспортних засобів», «Права водія», через бюро Інтерполу в ручному режимі надають також відбитки пальців, фотографії підозрюваних, та дані про тих осіб, які відбувають покарання. Необхідно звернути увагу на наступне: «...У разі входу до цієї бази працівників будь-якого національного центрального бюро Інтерполу (крім ініціаторів її публікації), електронне повідомлення про факт звернення до тексту картки автоматично скеровується до національного центрального бюро Інтерполу держави, ініціатора її розповсюдження, яке таким чином має змогу відслідковувати, яка держава виявила інтерес до даної особи. Після отримання указанного електронного повідомлення країна-ініціатор запитує національне центральне бюро Інтерполу країни, що зверталась до інформації про особу у Системі автоматичного пошуку інформації “ASF” для отримання пояснень щодо підстав перегляду інформації та отримання нових відомостей відносно конкретної особи – об’єкта спільних перевірок...» (джерело: <https://uk.wikipedia.org/wiki/I-24/7>).

Територіальний сервісний центр МВС – є структурним підрозділом територіального органу МВС – регіонального сервісного центру МВС. З метою виконання покладених на нього завдань та функцій ТЦС МВС взаємодіє з територіальними органами МВС, іншими органами державної влади та місцевого самоврядування відповідно до чинного законодавства [98].

Терміни виконання запитів до оперативно-довідкового і дактилоскопічного обліків – 1) запити від органів та установ виконуються протягом десяти діб; 2) терміново, протягом доби, виконуються мотивовані запити, пов’язані з розкриттям тяжких злочинів і розшуком злочинців, а також щодо осіб, відносно яких вирішується питання про арешт; 3) запити юридичних та фізичних осіб виконуються в терміни, передбачені законодавством [97].

Терміни виконання запитів, одержаних правоохоронними органами України з НЦБ Інтерполу в Україні – 1) з поміткою “*терміново*” – протягом доби з часу надходження; 2) з поміткою “*звичайно*” – в якомога коротший термін, але не більше десяти діб; 3) з поміткою “*нетерміново*” – в якомога коротший термін або до вказаної у запиті дати, але не більше 1 місяця. Відповідальність за своєчасне і якісне виконання запитів НЦБ несе керівник органу, куди надійшов запит для виконання. При *неможливості своєчасно виконати запит* керівник зазначеного органу *письмово інформує* НЦБ про обставини та причини, що перешкоджають своєчасному виконанню. Змінити термін виконання запиту за наявності об’єктивних обставин, а також зняти з контролю виконаний запит може лише керівник, який дав доручення до виконання, або особа, яка його заміщає. Зупинити виконання запиту або скасувати його має право лише начальник НЦБ та його заступники, НЦБ країни – ініціатора запиту, або Генеральний секретаріат Інтерполу [95].

Терміни зберігання облікових документів в дактилоскопічних картотеках – у дактилоскопічних картотеках дактилоскопічні карти зберігаються незалежно від термінів зберігання облікових карток, до досягнення особами, що стоять на обліку, 80-річного віку; особи, які досягли 80-річного віку в період відбування покарання, з дактилоскопічного обліку знімаються після звільнення; терміни зберігання облікових матеріалів, які мають науково-історичне значення, можуть продовжуватись рішенням керівництва інформаційної служби [97].

Терміни зберігання облікових документів в оперативно-довідкових картотеках (банках даних) – облікові документи зберігаються незалежно від погашення або зняття судимості. В оперативно-довідкових картотеках облікові документи зберігаються: 1) *постійно*: а) на засуджених за злочини проти основ національної безпеки України, проти миру, безпеки людства та міжнародного правопорядку; б) на засуджених до довічного позбавлення волі (у тому числі тих, хто раніше був засуджений до смертної кари); в) на осіб, померлих у місцях позбавлення волі та під час слідства; г) на осіб, що стали жертвами політичних репресій; 2) *на засуджених до позбавлення волі за скоєння*: а) особливо тяжких злочинів – 50 років після відбування покарання; б) тяжких злочинів – 30 років після відбування покарання; в) злочинів середньої тяжкості – 20 років після відбування покарання; г) злочинів невеликої тяжкості – 10 років після відбування покарання; 3) *на осіб, засуджених до мір покарання без позбавлення волі*: а) один раз – 5 років після відбування покарання; б) два і більше разів – 10 років після відбування покарання за останньою судимістю; в) на осіб, засуджених до штрафу, – 5 років після винесення рішення тощо [97].

Термінологічний словник законодавства України інформаційно-пошукової системи «Законодавство України» – унікальний інформаційний ресурс ІПС, постійно актуалізований термінологічний словник законодавства України, які згруповані за алфавітом. Станом на 26.04.2019 ІПС «Законодавство України» містить 62 739 термінів та посилання на 6343 документа з термінами. Серед них за видами документів: кодекс України – 39; кодекс – 59; закон – 851; постанова – 1428; указ – 125; розпорядження – 168; декрет – 16; наказ – 2733 тощо.

Технології Інтерполу (http://interpol.np.gov.ua/?page_id=37) – міжнародні банки даних Інтерполу – є одним із ключових інструментів в боротьбі з транснаціональною злочинністю. Інформаційне наповнення банків даних Інтерполу здійснюється правоохоронними органами всіх держав-членів Організації. Доступ до цих банків даних забезпечується за допомогою інформаційно-телекомунікаційної системи Інтерполу I-24/7. Розширення доступу до цієї системи всім без виключення правоохоронним органам України є одним з основних завдань Укрбюро Інтерполу і одним з основних аспектів політики діяльності Інтерполу в цілому.

Установчі дані фізичної особи – інформація про прізвище, ім'я, по батькові фізичної особи, дату та місце її народження, що дозволяє ідентифікувати її в персонально-довідковому обліку [106].

Форми документів, що використовуються для формування та коригування оперативно-довідкового і дактилоскопічного обліків (банків даних) – 1) алфавітна картка форми 1; 2) розшукова картка; 3) алфавітна картка форми 1а на особу, яка затримана за підозрою в занятті бродяжництвом; 4) дактилоскопічна карта; 5) сповіщення про засудженого (заарештованого); 6) повідомлення про помилування засудженого; 7) повідомлення про внесення змін в анкетні дані осіб, що стоять на обліку; 8) повідомлення про засудженого (взятого під варту) іноземця; 9) висновок про відновлення родових даних; 10) постанова органу слідства про закриття кримінальної справи на підставі реабілітації; 11) виправдувальний вирок суду; 12) довідка відповідної форми про результати розгляду кримінальної справи в суді; 13) повідомлення компетентних органів іноземних держав про притягнення до кримінальної відповідальності громадян України. *Примітка:* у разі необхідності та на виконання міжнародних договорів у сфері обміну інформацією облікові та коригувальні документи (алфавітні картки форм 1 та 1а, дактилоскопічні карти, сповіщення тощо) заповнюються російською мовою [97].

Формування банків даних НЦБ Інтерполу в Україні – уся інформація, отримувана МВС України каналами Інтерполу, вміщується в інтегровану базу даних НЦБ за такими підсистемами: 1) «Документ»; 2) «Особи»; 3) «Транспорт»; 4) «Фірми»; 5) «Номерні речі»; 6) «Валюта»; 7) «Предмети мистецтва» [95].

Формування інформаційних ресурсів поліцією – поліція відповідно до ч. 1 ст. 26 Закону України «Про Національну поліцію» наповнює та підтримує в актуальному стані 18 баз (банків) даних, що входять до ЄІС МВС України (див. Додаток 1). Під час наповнення баз (банків) даних, визначених у п. 7 ч. 1 цієї статті, поліція забезпечує збирання, накопичення мультимедійної інформації (фото, відео-, звукозапис) та біометричних даних (дактилокартки, зразки ДНК). Поліція забезпечує внесення відомостей до Єдиного реєстру осіб, зниклих безвісти за особливих обставин, та здійснює підтримання таких відомостей в актуальному стані в межах, визначених законодавством [8].

Функції АІС ОП – це: 1) автоматизація процесів обліку отриманої в процесі оперативно-розшукової діяльності Національної поліції України інформації; 2) збір, зберігання, пошук та узагальнення інформації; 3) відображення повнотекстової, графічної, табличної та статистичної інформації, а також фото- і відеозображень; 4) утворення електронного дос'є; 5) формалізація технологічних процесів обробки інформації, визначення типових маршрутних технологічних схем для їх виконання; 6) забезпечення надійного зберігання інформаційних обліків та їх систематизація; 7) забезпечення комплексного захисту інформації та розмежування доступу до інформації, що зберігається в АІС ОП [83].

Функції єдиної інформаційної системи МВС – це: 1) *інтеграція* інформаційних ресурсів ЄІС МВС; 2) *обробка інформації*, що формується у процесі діяльності суб'єктів ЄІС МВС; 3) перевірка *своєчасності* внесення, *достовірності та повноти* інформації, яка відповідно до законодавства обробляється суб'єктами ЄІС МВС; 4) *систематизація та узагальнення* інформації, *перетворення* її до формату, придатного для проведення подальшого аналізу та забезпечення роботи автоматизованих підсистем підтримки прийняття рішень, сигнальних та контрольних сервісів; 5) *автоматизація та верифікація* процесів інформаційної діяльності суб'єктів ЄІС МВС в інтерактивному режимі реального часу; 6) забезпечення *електронної інформаційної взаємодії та електронного документообігу* між суб'єктами ЄІС МВС; 7) *розмежування прав доступу* та надання контрольованого доступу користувачам ЄІС МВС до інформаційних ресурсів ЄІС МВС; 8) забезпечення *резервного копіювання, зберігання та комплексного захисту інформації*, що міститься в інформаційних ресурсах єдиної інформаційної системи МВС [52].

Функції ЄЦВТМ – це: 1) забезпечення організації та функціонування фіксованого телефонного зв'язку: відомчого оперативного (місцевого та міжміського); ІР-телефонії; 2) забезпечення телекомунікаційного доступу до інформаційних баз даних МВС користувачів на базі узгодженого єдиного мережевого простору ІР-адрес у МВС відповідно до чинного законодавства, здійснення прийому та передавання різних видів інформації, забезпечення управління якістю послуг, що надаються, а також забезпечення доступу відповідних користувачів до ЄРДР;

3) забезпечення функціонування відомчого документального зв'язку (факсимільного, телеграфного та електронної пошти); 4) забезпечення організації та функціонування: відомчої системи аудіоселекторного та відеоселекторного зв'язку, що дає змогу організовувати і технічно супроводжувати проведення щотижневих нарад керівництва МВС, центральних органів виконавчої влади, діяльність яких спрямовує та координує Міністр внутрішніх справ України, з керівниками підрозділів (користувачами), у тому числі для потреб органів досудового розслідування; персональної аудіо- та відеоконференції Міністра внутрішніх справ України для проведення в автоматичному режимі відеоконференції з керівниками підрозділів (користувачами) ЄЦВТМ; 5) забезпечення організації та функціонування службового відеозображення для моніторингу державних та недержавних інформаційних телевізійних каналів; 6) забезпечення передачі зображень з камер зовнішнього та внутрішнього відеоспостереження: від відеокамер зовнішнього розташування, установлених у громадських місцях і на автомобільних дорогах України, до чергових частин (далі – ЧЧ) (оперативних штабів) ЦОВВ, апарату МВС з метою покращення охорони громадського порядку та безпеки дорожнього руху; від внутрішніх відеокамер, розташованих у приміщеннях ЧЧ користувачів, з метою контролю за роботою добових нарядів ЧЧ обласних, міських, районних, районних у містах, міських користувачів; від внутрішніх відеокамер, розташованих в адміністративних будівлях користувачів, до апарату МВС, ЦОВВ, з метою моніторингу додержання посадовими особами прав, свобод та законних інтересів громадян; 7) забезпечення функціонування апаратно-програмних комплексів чергових частин користувачів, у тому числі реєстраторів інформації, що озвучується; 8) забезпечення функціонування: аналогових стаціонарних засобів радіозв'язку УКХ та КХ-діапазонів з дистанційним керуванням; цифрової системи транкінгового радіозв'язку; 9) забезпечення функціонування електронних засобів контролю в структурних підрозділах Національної поліції України; 10) забезпечення функціонування засобів GPS-позиціонування для потреб відповідних користувачів; 11) забезпечення захисту інформації, яка обробляється в ЄЦВТМ, відповідно до вимог законодавства [85].

Функціональними підсистемами єдиної інформаційної системи МВС – є: 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) система екстреної допомоги населенню за єдиним телефонним номером 112; 7) інтегрована міжвідомча інформаційно-телекомунікаційна система щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон; 8) інформаційно-телекомунікаційна система прикордонного контролю “Гарт-1”; 9) інші системи, реєстри та бази (банки) даних, створені суб’єктами єдиної інформаційної системи МВС в межах реалізації владних повноважень [52].

Функціональні підсистеми єдиної інформаційної системи МВС – це сукупність технічних засобів та програмних комплексів, які автоматизують службові процеси суб’єктів ЄІС МВС до рівня стандартів операційних процедур та автоматизованого робочого місця користувача, забезпечують формування, зберігання, спільне використання і верифікацію інформаційних ресурсів єдиної інформаційної системи МВС [52].

Центральна підсистема єдиної інформаційної системи МВС – обчислювальне середовище функціонування автоматизованих сервісів, яке забезпечує безперервність їх обслуговування в інтерактивному режимі реального часу та високий рівень продуктивності. Центральна підсистема єдиної інформаційної системи МВС функціонує в основному та резервному центрах обробки даних, які забезпечують середовище для її роботи [52].

Цілі Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року – це створення безпечного середовища розвитку вільного суспільства, забезпечення високої ефективності діяльності органів системи МВС, зміцнення суспільної довіри до неї з урахуванням визначальної ролі громадянина у розбудові України як безпечної європейської держави [56].

Частина 1 статті 3 Конституції України – «Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю».

Частина 2 статті 3 Конституції України – «Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави».

Частина 2 статті 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].

Частина 1 статті 31 Конституції України – «Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинам чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо».

Частина 2 статті 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» [1].

Частина 3 статті 32 Конституції України – «Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею».

Частина 4 статті 32 Конституції України – «Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації».

ДОДАТКОВА ІНФОРМАЦІЯ ДО ТЕМИ I

Автоматизація оперативно-довідкового обліку – повинна забезпечувати уніфікацію і сумісність інформаційних систем, оброблення даних та обмін інформацією в єдиному форматі. Перевірка осіб з віддаленого терміналу за автоматизованим банком даних без спеціального дозволу категорично забороняється. Підключення до інформаційно-обчислювальної мережі не допускається без наявності спеціальної системи захисту від несанкціонованого доступу до даних та автоматизованого контролю за реєстрацією звернень. Працівникам забороняється розголошувати особам, що перевіряються, та іншим стороннім особам відомості про джерело одержання інформації про притягнення до кримінальної відповідальності та дані про наявність чи відсутність судимості [97].

Автоматизована система документообігу суду – сукупність розподілених комп'ютерних програм і відповідних програмно-апаратних комплексів, визначених Положенням про автоматизовану систему документообігу суду, затвердженим Радою суддів України [64].

Автоматизоване робоче місце ЄЦВТМ – це місце користувача, обладнане персональним комп'ютером з установленим програмним забезпеченням, апаратом телефонного зв'язку, пристроєм відображення відомчого телебачення, пристроєм аудіо- або відеоселекторного зв'язку та підключене до локальної мережі [85].

Авторизація користувача – це процедура отримання користувачем повноважень на доступ до інформаційних ресурсів ЄДРСР за допомогою його власного ЕЦП, який відповідно до вимог закону прирівнюється за правовим статусом до власноручного підпису користувача [64].

Авторизація на проведення операцій внесення до безконтактного електронного носія – процедура отримання дозволу на проведення операцій внесення до безконтактного електронного носія додаткової змінної інформації (про місце проживання, про народження дітей, про шлюб і розірвання шлюбу, про зміну імені, у разі наявності – інформація про податковий номер (реєстраційний номер облікової картки платників податків з Державного реєстру фізичних осіб – платників податків) або повідомлення про відмову від прийняття реєстраційного номера облікової картки платника податків (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомили про це відповідний контролюючий орган), інформації до захищених груп даних та зчитування інформації, внесеної до безконтактного електронного носія [104].

Адміністратор Єдиного державного реєстру судових рішень – адміністратор Єдиної судової інформаційної системи державне підприємство “Інформаційні судові системи”, віднесене до сфери управління ДСА України. Адміністратор вживає заходи, пов’язані із технічним та організаційно-технологічним забезпеченням функціонування Реєстру, у тому числі такі: створення, вдосконалення та супроводження державної ІС Реєстру; адміністрування Реєстру; надання доступу до Реєстру; забезпечення зберігання та захисту даних, що містяться в Реєстрі, у тому числі шляхом визначення моделі захисту від загроз витоку інформації та засобів обробки електронних документів у Реєстрі та надання до них безоплатного цілодобового доступу на офіційному веб-порталі “Судова влада України”; виконання інших функцій, передбачених цим Порядком [64].

Адміністратор Національного реєстру електронних інформаційних ресурсів – це державне підприємство, визначене Державним агентством з питань електронного урядування, що належить до сфери його управління. Адміністратор: 1) забезпечує функціонування Національного реєстру та цілодобовий доступ користувачів до його інформаційного фонду; 2) контролює доступ до фондів Національного реєстру, забезпечує комплексний захист інформації Національного реєстру, в тому числі від несанкціонованого доступу; 3) обробляє відомості про склад, зміст, розміщення та умови доступу до е-ресурсів, вносить ці відомості до відповідних фондів Національного реєстру та оновлює їх; 4) забезпечує ідентичність відомостей, що надаються користувачам, і відомостей держателів (розпорядників) е-ресурсів; 5) надає інформаційні послуги користувачам та методичну допомогу держателям (розпорядникам) е-ресурсів тощо [63].

Адміністрація Державної служби спеціального зв’язку та захисту інформації України (Адміністрація Держспецзв’язку) – є центральним органом виконавчої влади із спеціальним статусом, діяльність якого спрямовується і координується Кабінетом Міністрів України і який забезпечує формування та реалізує державну політику у сферах організації спеціального зв’язку, захисту інформації, кіберзахисту телекомунікацій і користування радіочастотним ресурсом України [60].

Безконтактний електронний носій (далі – БЕН) – імплантована в бланк документа безконтактна інтегральна схема для внесення персональних даних, параметрів, у тому числі біометричних, що дає змогу здійснювати комплекс заходів, пов’язаних з верифікацією особи, та може використовуватися як засіб електронного цифрового підпису у випадках, передбачених законом. *Групи даних* – зони БЕН, до яких вноситься інформація про особу, визначена в Законі України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус». *Захищені групи даних* – зони БЕН, до яких вноситься набір електронних даних, за допомогою яких забезпечується можливість підтвердження цілісності даних БЕН [104].

Вилучення облікових документів з оперативно-довідкових картотек – з оперативно-довідкових картотек вилучаються: а) раніше складені облікові документи у разі їх переоформлення на підставі постанов органів слідства (дізнання) або ухвал судів про уточнення (зміну) анкетних даних осіб, що стоять на обліку; б) алфавітні картки на осіб, притягнутих до кримінальної відповідальності, до яких не застосовувався запобіжний захід у вигляді взяття під варту, при заміні цих карток на арештантські або картки з рішенням суду; в) облікові документи на осіб, притягнутих до кримінальної відповідальності як обвинувачені, кримінальні справи стосовно яких припинені на стадії досудового слідства на підставі реабілітації або відносно яких судом прийнято виправдувальний вирок; г) облікові документи, що підлягають вилученню у зв'язку із закінченням строку їх зберігання. Правильність вилучення карток і дактилокарт контролюється керівниками відповідних підрозділів. Вилучені документи знищуються за затвердженням керівництвом інформаційної служби актом із зазначенням у ньому складу комісії, місця, часу, підстави вилучення і кількості облікових документів, що знищені [97].

Вимоги (рекомендації) щодо забезпечення захисту секретної інформації – встановлені характеристики, властивості, параметри, які висуваються до об'єктів інформаційної діяльності, інформаційно-телекомунікаційних систем, засобів обробки секретної інформації, засобів і комплексів (систем) технічного захисту інформації (далі – ТЗІ) та їх окремих складових з метою забезпечення захищеності секретної інформації [88].

Витяг з ЄДРП – згенерований програмними засобами ведення Реєстру документ, який засвідчує факт реєстрації в Реєстрі відомостей про кримінальне правопорушення, які є актуальними на момент його формування, та містить інформацію про: 1) номер та дату реєстрації кримінального провадження; 2) дату надходження заяви, повідомлення та дату і час внесення відомостей про заяву, повідомлення про вчинене кримінальне правопорушення до Реєстру, правову кваліфікацію кримінального правопорушення, наслідок розслідування кримінального правопорушення; 3) прізвище, ім'я, по батькові потерпілого, заявника (найменування юридичної особи та ідентифікаційний код Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань (далі – ЄДР)); 4) короткий виклад обставин, що можуть свідчити про вчинення кримінального правопорушення; 5) прізвище, ім'я, по батькові та дату народження особи, яку повідомлено про підозру, наслідки розслідування щодо особи та відомості про здійснення спеціального досудового розслідування щодо неї; 6) найменування, код ЄДР, юридичну адресу, розрахунковий рахунок, місце та дату державної реєстрації юридичної особи, щодо якої здійснюється кримінальне провадження, а також анкетні дані її представника; 7) орган досудового розслідування; 8) прізвище, ім'я, по батькові слідчого (слідчих) та прокурора (прокурорів). Реєстратори самостійно формують витяг з Реєстру та посвідчують його своїм підписом [74, 100].

Ефективність технічного захисту секретної інформації – ступінь відповідності вжитих заходів щодо технічного захисту секретної інформації установленим нормам і вимогам [88].

Загроза для секретної інформації – передумови витоку, можливості блокування чи порушення цілісності секретної інформації [88].

Засоби криптографічного захисту інформації – засоби шифрування інформації; засоби виготовлення ключових даних або ключових документів та управління ключовими даними, що використовуються в засобах криптографічного захисту інформації; засоби захисту від нав'язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізують алгоритми криптографічного перетворення інформації; засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані алгоритми криптографічного перетворення інформації [88].

Кваліфікація порушень ТЗІ – Порушення ТЗІ діляться на три категорії, які визначають можливість реалізації загроз безпеці інформації: 1) *перша категорія* – невиконання вимог НПА та нормативно-технічних документів з ТЗІ, унаслідок чого створюється *реальна загроза порушення конфіденційності* (зокрема за рахунок витоку (просочення) технічними каналами) та (або) цілісності й доступності інформації; 2) *друга категорія* – невиконання вимог НПА та нормативно-технічних документів з ТЗІ, унаслідок чого створюються *передумови для порушення конфіденційності* (зокрема за рахунок витоку (просочення) технічними каналами) та (або) цілісності й доступності інформації; 3) *третья категорія* – невиконання інших вимог з ТЗІ [99].

Комплекс технічного захисту інформації – сукупність організаційних та інженерних заходів, призначених для захисту секретної інформації від витоку технічними каналами та спеціального впливу [88].

Контроль за станом технічного захисту інформації в органах і підрозділах НПУ – здійснюється Управлінням режиму та технічного захисту інформації (далі – УРТЗІ) НПУ. Контроль за станом технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, здійснюється в органах, щодо яких здійснюється ТЗІ. Контроль за станом ТЗІ полягає в перевірці виконання вимог НПА і нормативно-технічних документів з ТЗІ та здійснюється з метою визначення стану ТЗІ в органах, виявлення порушень з ТЗІ та запобігання ним. Контроль за станом ТЗІ здійснюється в УРТЗІ НПУ шляхом організації та проведення контрольно-інспекторської роботи з питань ТЗІ стосовно органів, щодо яких здійснюється ТЗІ. Контроль заходів з ТЗІ в органах виконується відповідними підрозділами, на які письмовим наказом керівника територіального органу поліції покладено забезпечення ТЗІ в цих органах. Відповідальними особами за організацію та контроль заходів з ТЗІ в органах є їх керівники [99].

Контрольно-інспекторська робота з питань ТЗІ – діяльність, спрямована на визначення та вдосконалення стану ТЗІ в органах, щодо яких здійснюється ТЗІ. Контрольно-інспекторська робота з питань ТЗІ включає планування та проведення перевірок стану ТЗІ в органах, щодо яких здійснюється ТЗІ, аналіз їх результатів та надання рекомендацій щодо вдосконалення заходів з ТЗІ. Аналітичні матеріали щодо стану ТЗІ в органах, щодо яких здійснюється ТЗІ, доповідаються Голові НПУ або його заступникові відповідно до розподілу функціональних обов'язків [99].

Криптографічна система – сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що обробляється, зберігається та (або) передається [88].

Криптографічний захист інформації – вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо [88].

КСЗІ з підтвердженою відповідністю – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації. Основним завданням КСЗІ є забезпечення достатнього рівня доступності, цілісності й конфіденційності інформації шляхом здійснення заходів, спрямованих на захист інформації від несанкціонованого доступу та витоку технічними каналами. Ідентифікація користувачів та підтвердження цілісності даних, що обробляються в АІС ОП, забезпечується програмно-технічними засобами авторизації користувачів та забезпечення цілісності даних. Кожна дія користувача щодо отримання інформації з АІС ОП фіксується у відповідних електронних журналах системи. Контроль за дотриманням вимог законодавства України в інформаційній сфері під час функціонування АІС ОП здійснює керівник підрозділу поліції, де експлуатується система [83].

Мережеве обладнання ЄЦВТМ – це сукупність пристроїв, які забезпечують підключення АРМ до ЄЦВТМ [85].

Неавторизований користувач – користувач, що не пройшов авторизацію в державній інформаційній системі Реєстру за допомогою власного ЕЦП, який відповідно до вимог закону прирівнюється за правовим статусом до власноручного підпису користувача [64].

Об'єкт інформаційної діяльності – інженерно-технічна споруда (приміщення), транспортний засіб, де провадиться діяльність, пов'язана з державними інформаційними ресурсами та інформацією, вимога щодо захисту якої встановлена законом [99]. *Або: об'єкт інформаційної діяльності* – інженерно-технічна споруда (приміщення) з визначеною контрольованою зоною, де здійснюється діяльність, пов'язана з інформацією, що підлягає технічному захисту [88].

Об'єкт телекомунікацій – комплекс споруд або окрема споруда, обладнані технологічними засобами телекомунікацій, з територією, на якій розміщені ці споруди (споруда) [88].

Образ електронного примірника судового рішення або окремої думки судді – автоматично створена копія електронного примірника судового рішення або окремої думки судді, що не містить відомостей, які не можуть бути розголошені в текстах судових рішень, відкритих для загального доступу, відповідно до вимог законодавства [64].

Організація проведення перевірок стану ТЗІ – Перевірки стану ТЗІ діляться на комплексні, цільові (тематичні) та контрольні. Зазначені перевірки можуть бути плановими та позаплановими. При *комплексній перевірці* визначається відповідність комплексу ТЗІ (КСЗІ) вимогам НПА та нормативно-технічних документів системи ТЗІ. При *цільовій (тематичній) перевірці* перевіряються окремі складові комплексу ТЗІ (КСЗІ) на відповідність упроваджених заходів вимогам НПА та нормативно-технічних документів системи ТЗІ. При *контрольній перевірці* перевіряються повнота та достатність проведених заходів щодо усунення недоліків, які були виявлені в ході проведення попередньої комплексної або цільової перевірки. Контрольні перевірки проводяться після отримання письмового повідомлення про усунення недоліків. *Планові перевірки* здійснюються згідно з планом основних організаційних і практичних заходів УРТЗІ НПУ, який затверджується начальником УРТЗІ НПУ. *Позапланові перевірки* проводяться в разі наявності відомостей щодо порушень виконання вимог НПА з питань ТЗІ або в разі виникнення потреби у визначенні повноти та достатності заходів з ТЗІ, ужитих органами, щодо яких здійснюється ТЗІ. Керівництво органів, щодо яких здійснюється ТЗІ, повідомляється про проведення перевірки не менше ніж за десять діб до її початку (за винятком проведення позапланової перевірки). Перевірки стану ТЗІ здійснюються посадовими особами УРТЗІ НПУ, на яке покладено виконання завдань щодо здійснення контролю за станом ТЗІ [99].

Основні завдання Адміністрації Держспецзв'язку – це: 1) забезпечення формування та реалізація: державної політики у сферах криптографічного і ТЗІ, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку; у сферах захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, здійснення державного контролю у таких сферах; державної технічної політики в галузі зв'язку;

2) участь у формуванні та реалізації: державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації (з використанням електронних довірчих послуг), електронних довірчих послуг (у частині встановлення вимог з безпеки та захисту інформації під час надання та використання електронних довірчих послуг, контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг); державної тарифної політики у сферах телекомунікацій і користування радіочастотним ресурсом України [60].

Повний доступ до судових рішень – режим доступу до інформаційних ресурсів ЄДРСР. Повний доступ до інформаційних ресурсів Реєстру забезпечується за допомогою електронного кабінету виключно для авторизованих користувачів [64].

Порушення у сфері ТЗІ – невиконання вимог нормативно-правових актів та нормативно-технічних документів системи ТЗІ за категоріями, які визначають можливість реалізації загроз безпеці інформації [99].

Порядок використання безконтактного електронного носія, який імплантовано в паспорт громадянина України – установлює з урахуванням міжнародних стандартів та рекомендацій Міжнародної організації цивільної авіації (ICAO) механізм здійснення операцій із внесення інформації до безконтактного електронного носія, який імплантовано в паспорт громадянина України, а також установлює загальні вимоги до використання зазначеного безконтактного електронного носія [104].

Порядок проведення перевірок стану ТЗІ – 1) для проведення перевірки стану ТЗІ посадові особи УРТЗІ НПУ пред'являють керівникові органу, щодо якого здійснюється ТЗІ, або особі, яка виконує його обов'язки, *притис* на проведення перевірки та *службові посвідчення*; 2) при проведенні перевірки стану ТЗІ контролю підлягають *повнота та достатність* упроваджених на об'єктах інформаційної діяльності заходів з ТЗІ, їх *відповідність* вимогам нормативно-правових актів, *виконання рекомендацій* щодо усунення порушень з ТЗІ; 3) за результатами перевірок посадовими особами УРТЗІ НПУ складається відповідна *довідка* про результати перевірки стану ТЗІ; 4) довідки про результати перевірок стану ТЗІ складаються в *довільній формі*. Довідки про результати перевірок стану ТЗІ готуються у двох примірниках. *Перший* примірник довідки про результати перевірки надсилається до органу, щодо якого здійснюється ТЗІ, *другий* – до УРТЗІ НПУ. Усі примірники довідки *підписуються* посадовими особами УРТЗІ НПУ, які проводили перевірку. Керівник або особа, яка виконує його обов'язки, органу, щодо якого здійснюється ТЗІ, *ознайомлюється* з довідкою про результати перевірки та ставить свій *підпис*. У разі *відмови* керівника органу, щодо якого здійснюється ТЗІ, засвідчити факт ознайомлення з довідкою про результати перевірки своїм підписом посадові особи УРТЗІ НПУ, що здійснювали перевірку, роблять у довідці відповідний запис про це [99].

Працівникам картотек забороняється – з метою забезпечення збереження картотечних фондів і захисту інформації, що міститься в них, забороняється: 1) повідомляти стороннім особам відомості про структуру обліків і характер інформації, що міститься в оперативно-довідкових картотеках; 2) залишати приміщення картотек і робочих кабінетів відкритими у разі тимчасової відсутності посадових осіб, а також неопечатаними в неробочий час; 3) допускати в приміщення картотек сторонніх осіб; 4) передавати облікові документи в тимчасове користування працівникам, що не мають за родом своєї службової діяльності прямого допуску до картотек; 5) зберігати облікові документи поза картотечними приміщеннями; 6) вилучати облікові картки і дактилоскопічні карти до закінчення термінів їх зберігання; 7) проводити не обгрунтоване офіційними документами коригування інформації; 8) надавати довідки про облікованих осіб по телефону, якщо не встановлено звернення до обліку за паролем; 9) робити перевірки і надавати інформацію в письмовій або усній формі за неофіційними запитами посадових і приватних осіб [97].

Припинення існування е-ресурсу, включеного до Національного реєстру електронних інформаційних ресурсів – держатель (розпорядник) не пізніше ніж за 30 днів до такого припинення повідомляє про це з використанням засобів програмного комплексу Національного реєстру Державне агентство з питань електронного урядування. Факт припинення існування е-ресурсу відображається у Національному реєстрі [63].

Реєстрація е-ресурсу в Національному реєстрі електронних інформаційних ресурсів – держатель (розпорядник) подає заяву на реєстрацію е-ресурсу з використанням засобів програмного комплексу Національного реєстру з урахуванням вимог законодавства з питань документування управлінської діяльності, в якій зазначає загальні відомості про відповідний е-ресурс та види даних, що він формує. Оформлення заяви завершується створенням кваліфікованого електронного підпису керівника або уповноваженої керівником особи. Держатель (розпорядник) е-ресурсу несе відповідальність за достовірність поданих у заяві відомостей згідно із законодавством. Державне агентство з питань електронного урядування на підставі оформленої у належний спосіб держателем (розпорядником) заяви на реєстрацію е-ресурсу за умови дотримання вимог законодавства протягом десяти днів з дня її надходження здійснює державну реєстрацію е-ресурсу з використанням засобів програмного комплексу Національного реєстру або надає обгрунтовану відмову в реєстрації [63].

Сегмент ЄЦВТМ – це логічно чи фізично відокремлена частина ЄЦВТМ. Розбиття ЄЦВТМ на сегменти здійснюється для оптимізації мережевого трафіку та/або підвищення безпеки ЄЦВТМ в цілому [85].

Сервер ЄЦВТМ – це програмно-апаратний комплекс, призначений для централізованого зберігання й обробки інформації, необхідної для забезпечення функціонування ЄЦВТМ [85].

Склад ЄЦВТМ – 1) вузли ЄЦВТМ 6 типів (центральный – апарату МВС; Автономної Республіки Крим, міст Києва та Севастополя, областей; міських користувачів; районних користувачів, у тому числі районних у містах; відокремлених користувачів; польові (мобільні)); 2) центр оперативного-технічного управління; 3) віртуальні IP-мережі (IP-VPN); 4) канали та лінії зв'язку [85].

Технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації [5]. *Або: технічний захист інформації* – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації [50].

Умови обробки інформації в системі – визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством. Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням КСЗІ з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством. Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством [5].

Формуванню, використанню та захисту недержавних ресурсів сприятиме: 1) включення недержавних ресурсів до Національного реєстру електронних інформаційних ресурсів; 2) доступність недержавних ресурсів для фізичних і юридичних осіб; 3) збільшення переліку інформаційних послуг, які надаються з використання національних ресурсів. Особлива увага приділятиметься вдосконаленню інформаційного обслуговування масового споживача з використанням національних ресурсів [59].

Шляхи досягнення мети Концепції розвитку електронного урядування в Україні – слід забезпечити виконання комплексних заходів за такими напрямками: 1) модернізація публічних послуг та розвиток взаємодії влади, громадян і бізнесу за допомогою інформаційно-комунікаційних технологій; 2) модернізація державного управління за допомогою інформаційно-комунікаційних технологій; 3) управління розвитком електронного урядування [55].

ТЕМА II. ВВЕДЕННЯ У ТЕХНОЛОГІЮ БАЗ ДАНИХ. СИСТЕМА УПРАВЛІННЯ БАЗАМИ ДАНИХ MICROSOFT ACCESS

Автентифікація – електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-телекомунікаційної системи та/або походження та цілісність електронних даних [25]. *Або: автентифікація* – процедура встановлення належності користувачеві інформації в системі пред’явленого ним ідентифікатора [69].

Адміністратор бази даних – на стадії проектування – це ідеолог і головний конструктор системи; на стадії експлуатації – це відповідальна особа за функціонування інформаційної системи, керує режимом використання даних, відповідає за збереження даних, розробляє заходи щодо захисту даних від руйнування, забезпечення їх достовірності і ефективного використання [108].

База даних – іменована сукупність даних, що відображає стан об’єктів та їх відношень у визначеній предметній області [9]. *Або: база даних* – сукупність творів, даних або будь-якої іншої незалежної інформації у довільній формі, в тому числі – електронній, підбір і розташування складових частин якої та її упорядкування є результатом творчої праці, і складові частини якої є доступними індивідуально і можуть бути знайдені за допомогою спеціальної пошукової системи на основі електронних засобів (комп’ютера) чи інших засобів [14]. *Або: база даних* – це організована структура, яка призначена для зберігання інформації [108].

База знань – масив інформації у формі, придатній до логічної і смислової обробки відповідними програмними засобами [9].

База персональних даних – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних [6].

Банк даних – це сукупність бази даних та системи управління базами даних. *Або: банк даних* – це заснована на технології баз даних система програмних, мовних, організаційних і технічних засобів, призначених для централізованого нагромадження і колективного використання даних [108].

Бібліотека – інформаційний, культурний, освітній заклад (установа, організація) або структурний підрозділ, що має упорядкований фонд документів, доступ до інших джерел інформації та головним завданням якого є забезпечення інформаційних, науково-дослідних, освітніх, культурних та інших потреб користувачів бібліотеки [18].

Бібліотечний фонд – упорядковане зібрання документів, що зберігається в бібліотеці [18].

Бібліотечні ресурси – упорядковані бібліотечні фонди документів на різних носіях інформації, бази даних, мережні інформаційні ресурси, довідково-пошуковий апарат, матеріально-технічні засоби опрацювання, зберігання та передачі інформації [18].

Використання персональних даних – 1) передбачає будь-які дії володільця щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки ПД іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюються за згодою суб'єкта ПД чи відповідно до закону; 2) здійснюється у разі створення ним умов для захисту цих даних (володільцю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними); 3) працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків (ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом; таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом); 4) відомості про особисте життя фізичної особи не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості [6].

Вимоги до баз даних – це: 1) актуальність; 2) повнота; 3) вірогідність [108].

Відкритий формат – формат даних, незалежний від платформи та доступний без обмежень, які перешкоджають його повторному використанню [62].

Властивості полів бази даних системи управління базами даних Microsoft Access – це: 1) *ім'я поля* – визначає, яким чином слід звертатись до даних цього поля при автоматичних операціях з базою даних (за замовченням імена полів використовуються в якості назв стовпців таблиць); 2) *тип поля* – визначає тип даних, які можуть міститись у даному полі; 3) *розмір поля* – визначає максимальну довжину (у символах) даних, які можуть міститись у даному полі; 4) *формат поля* – визначає спосіб форматування даних у комірках, які належать полю; 5) *маска введення* – визначає форму, в якій вводяться дані у поле (засіб автоматизації введення даних); 6) *підпис* – визначає заголовок стовпця таблиці для даного поля (якщо підпис не вказаний, то у якості заголовка стовпця використовується властивість “Ім'я поля”); 7) *значення за замовчуванням* – те значення, яке вводиться у комірки поля автоматично (засіб автоматизації введення даних); 8) *умова на значення* – обмеження, що використовується для перевірки правильності введення даних (для даних числового типу, грошового типу та типу дата-час); 9) *повідомлення про помилку* – текстове повідомлення, яке видається автоматично при спробі введення в поле помилкових даних (коли задана властивість “Умова на значення”); 10) *обов'язкове поле* – визначає обов'язковість заповнення даного поля при наповненні бази; 11) *порожні рядки* – дозволяє введення порожніх рядків; 12) *індексоване поле* – при наявності цієї властивості всі операції, пов'язані з пошуком або сортуванням записів за значенням, яке зберігається у цьому полі, суттєво прискорюються [108].

Внутрішні користувачі інформаційної системи (бази даних) – розробляють інформаційну систему і підтримують її функціонування, поділяються на: 1) *адміністратора бази даних* (ідеолог і головний конструктор системи; відповідальна особа за функціонування інформаційної системи, керує режимом використання даних, відповідає за збереження даних, забезпечення їх достовірності); 2) *системних програмістів* (розробляють програми, що розширюють можливості системи управління базами даних (далі – СУБД), забезпечують контроль за функціонуванням банку даних); 3) *прикладних програмістів* (розробляють програми обробки даних, що містяться в базах даних, відповідно до потреб кінцевих користувачів). При експлуатації простих баз даних функції трьох категорій внутрішніх фахівців реалізуються однією людиною [108].

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 [6].

Дані – інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки [10]. *Або: дані* – інформація, яка подана у формі, придатній для її оброблення електронними засобами [26].

Довідково-інформаційний фонд – це сукупність упорядкованих первинних документів і довідково-пошукового апарату, призначених для задоволення інформаційних потреб [32].

Довідково-пошуковий апарат – це сукупність упорядкованих вторинних документів, створюваних для пошуку першоджерел [32].

Електронні дані – будь-яка інформація в електронній формі [25].

Етапи проектування бази даних в СУБД Microsoft Access – це: 1) визначити структуру бази даних, джерело даних, задачі бази даних; 2) скласти перелік даних, розділити їх на групи, які стануть таблицями; 3) визначити поля для кожної таблиці; 4) визначити ключові поля; 5) вибрати оформлення для форм і звітів; 6) визначити умови вибору для запитів [108].

Загальні вимоги до обробки персональних даних – 1) обробка персональних даних здійснюється *відкрито і прозоро* із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки; 2) персональні дані мають бути *точними, достовірними та оновлюватися* в міру потреби, визначеної метою їх обробки; 3) склад та зміст персональних даних мають бути *відповідними, адекватними та ненадмірними* стосовно визначеної мети їх обробки; 4) *первинними джерелами відомостей про фізичну особу є*: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе; 5) обробка персональних даних здійснюється для *конкретних і законних цілей*, визначених за згодою суб'єкта ПД, або у випадках, передбачених законами України, у порядку, встановленому законодавством; 6) *не допускається обробка даних про фізичну особу, які є конфіденційною інформацією*, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини;

7) якщо обробка персональних даних є необхідною для захисту *життєво важливих інтересів* суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим; 8) персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це *необхідно для законних цілей*, у яких вони збиралися або надалі оброблялися; подальша обробка персональних даних в історичних, статистичних чи наукових цілях може здійснюватися за умови забезпечення їх *належного захисту*; 9) типовий порядок обробки персональних даних *затверджується* Уповноваженим Верховної Ради України з прав людини [6].

Зберігання персональних даних – передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них [6].

Збирання персональних даних – 1) є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу; 2) суб'єкт ПД повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані: в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних; в інших випадках протягом тридцяти робочих днів з дня збору персональних даних [6].

Згода суб'єкта персональних даних – добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки [6].

Знеособлення персональних даних – вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу [6].

Ідентифікація – процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою [69].

Ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи [25].

Ієрархічна модель даних – будується на основі принципу підпорядкованості елементів даних і є деревоподібною структурою, що складається з вузлів (сегментів) і дуг (гілок). Дерево в ієрархічній структурі впорядковане за чинними правилами розміщення його сегментів і гілок: 1) на верхньому рівні перебуває один сегмент – кореневий (вихідний); 2) сегмент другого рівня – породжений – залежить від першого, вихідного; 3) доступ до кожного породженого (крім кореневого) відбувається через його вихідний сегмент; 4) кожен сегмент може мати по кілька примірників конкретних значень елементів даних, а кожен елемент породженого сегмента пов'язаний з примірником вихідного і створює один логічний запис; 5) примірник породженого сегмента не може існувати самостійно, тобто без кореневого сегмента; 6) при вилученні примірника кореневого сегмента також вилучаються всі підпорядковані і взаємопов'язані з ним примірники породжених сегментів [108].

Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [5].

Інформаційна система – автоматизована система, комп'ютерна мережа або система зв'язку [50]. *Або: інформаційна система* – організаційно-технічна система обробки інформації за допомогою технічних і програмних засобів [65]. *Або: інформаційна система* – це система, яка організовує накопичення і оперування інформацією у певній області [108].

Інформаційна система загального доступу – сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних [10].

Інформаційний ресурс – сукупність документів у інформаційних системах (бібліотеках, архівах, БД тощо) [9].

Інформаційні ресурси науково-технічної інформації – це систематизоване зібрання науково-технічної літератури і документації (книги, брошури, періодичні видання, патентна документація, нормативно-технічна документація, промислові каталоги, конструкторська документація, звітна науково-технічна документація з науково-дослідних і дослідно-конструкторських робіт, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксовані на паперових чи інших носіях [32].

Інформаційні ресурси спільного користування – це сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання [32].

Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. *Не допускаються* 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 захисту прав людини. *До конфіденційної інформації про фізичну особу* належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом [2].

Картотека – будь-які структуровані персональні дані, доступні за визначеними критеріями, незалежно від того, чи такі дані централізовані, децентралізовані або розділені за функціональними чи географічними принципами [6].

Картотека особового складу – каталог документальних матеріалів, що у систематизованому вигляді містить відомості про трудовий стаж, освіту, зарплату, службу в армії, соціальний стан, інші дані про окремих осіб [78].

Каталог документів – архівний довідник, що є систематизованим описом змісту документів [78].

Кінцеві користувачі – спеціалісти, які, як правило, не мають хорошої підготовки в області програмування, але які користуються базами даних у своїй повсякденній роботі (для цих користувачів і розробляються БД) [108].

Класифікація інформаційних систем – це: 1) *за призначенням* (документальні, фактографічні та змішані); 2) *за мовами* (замкнуті системи, системи з базовою мовою, змішані); 3) *за локалізацією* (локальні та розподілені); 4) *за схемою додаткової обробки даних* (з постобробкою, з попередньою обробкою); 5) *за структурами даних* (ієрархічні, мережного типу, реляційні) [108].

Класифікація інформаційно-пошукових систем в залежності від режиму організації пошуку – поділяються на: 1) *документальні* – в них реалізується пошук в інформаційному фонді документів чи текстів у відповідності з отриманим запитом з подальшим наданням користувачу цих документів чи їх копій. Вся обробка отриманої інформації в документальних інформаційно-пошукових системах здійснюється користувачем; 2) *бібліографічні* – пошук ведеться в інформаційному фонді вторинних джерел; 3) *бібліотечні* – пошук ведеться в інформаційному фонді, що складається з первинних документів; 4) *фактографічні* – реалізують пошук та видачу фактів, документів та текстів, що містять відомості, які можуть задовольнити запит користувача. Вони надають користувачу не конкретний документ, а в певній мірі опрацьовану інформацію [108].

Класифікація правових інформаційних систем – за такими напрямками: 1) *за рівнем або сферою діяльності* – державні, територіальні, галузеві, підприємств або установ та окремих технологічних процесів; 2) *за рівнем автоматизації процесів управління* – ПС, інформаційно-довідкові системи, інформаційно-керівні системи, інтелектуальні інформаційні системи, системи підтримки прийняття рішень; 3) *за ступенем централізації обробки інформації* – централізовані ІС, децентралізовані ІС, інформаційні системи колективного використання; 4) *за ступенем інтеграції функцій* – багаторівневі ІС з інтеграцією за рівнями управління (підприємство – об'єднання, об'єднання – галузь та ін.), багаторівневі ІС з інтеграцією за рівнями планування [108].

Ключ – кожний кортеж (запис) відношення має ключ. *Простий ключ* – це ключ, який складається з одного атомарного атрибута, значення якого унікальне (не повторюється). *Складний ключ* складається з двох і більше атрибутів. Для зв'язків відношень одного з одним у базі даних є *зовнішні ключі* [108].

Користувач інформації в системі – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі [5].

Користувачі інформаційної системи (бази даних) – це особи, які працюють з інформаційною системою і використовують відомості, що містяться у базах даних. Їх умовно можна розділити на такі групи: 1) *внутрішні* (розробляють інформаційну систему і підтримують її функціонування); 2) *кінцеві* (спеціалісти, які, як правило, не мають хорошої підготовки в області програмування, але які користуються базами даних у своїй повсякденній роботі; для цих користувачів і розробляються бази даних) [108].

Машиночитаний формат – формат даних, структурований таким чином, що дає змогу інформаційним системам ідентифікувати, розпізнавати, перетворювати і отримувати конкретні дані без участі людини [62].

Мережева модель даних – являє собою орієнтований граф з пойменованими вершинами та дугами. *Вершини графа* – записи, що є пойменованою сукупністю логічних взаємопов'язаних елементів даних або агрегатів даних. Під *агрегатом даних* розуміють пойменовану сукупність елементів даних, які є всередині запису [108].

Метадані – довідкова структурована інформація, що описує, роз'яснює, дає змогу ідентифікувати, спрощує використання та управління набором даних [62].

Набір даних – сукупність однорідних значень (записів) даних та метаданих, що їх описують [62].

Накопичення персональних даних – передбачає дії щодо поєднання та систематизації відомостей про фізичну особу чи групу фізичних осіб або внесення цих даних до бази персональних даних [6].

Об'єкти бази даних Microsoft Access – це: 1) *таблиці* – основний об'єкт будь-якої бази даних; 2) *запити* – для вибирання даних з таблиць і надання їх користувачу у зручному вигляді. Виконують добір даних, сортування і фільтрацію. За допомогою запитів можна виконувати перетворення даних за заданим алгоритмом, створювати нові таблиці і т.ін.; 3) *форми* – засіб для введення даних; 4) *звіти* – схожі на форми, але призначені для виводу на друк; 5) *сторінки* – об'єкт, що виконаний у кодї HTML, розміщений на Web-сторінці і переданий клієнту разом з нею. Здійснюють інтерфейс між клієнтом, сервером і базою даних, розміщеною на сервері; 6) *макроси та модулі* – для автоматизації повторюваних операцій та створення нових функцій шляхом програмування [108].

Обробка персональних даних – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем [6].

Одержувач – фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа [6].

Оприлюднення набору даних – розміщення розпорядником інформації набору даних в Інтернеті та забезпечення доступу до нього. Оприлюднення набору даних передбачає можливість їх перегляду і завантаження безоплатно та без проведення додаткової реєстрації, ідентифікації, авторизації, проходження автоматизованого тесту для розрізнення користувачів чи інших обмежень. Оприлюднення наборів даних на Єдиному державному веб-порталі відкритих даних здійснюється безоплатно відповідальною особою розпорядника інформації, яка заповнює та подає паспорт набору даних, а також подає структуру набору даних та набір даних. Розпорядники інформації несуть згідно із законом відповідальність за достовірність і актуальність оприлюднених наборів даних на цьому веб-порталі відкритих даних. Адміністратор його несе згідно із законом відповідальність за забезпечення цілісності інформації на веб-порталі відкритих даних після оприлюднення цієї інформації її розпорядниками. Розпорядник інформації забезпечує оприлюднення нового набору даних протягом 10 календарних днів [62].

Основні властивості баз даних – це: 1) для даних допускається така *мінімальна надлишковість*, що сприяє їх оптимальному використанню в одному чи кількох застосуваннях; 2) *незалежність* даних від програм; 3) для пошуку та модифікації даних використовуються *спільні механізми*; 4) як правило, у складі бази даних існують *засоби для підтримки її цілісності та захисту від несанкціонованого доступу*. Є також *механізми перевірки змісту даних* [108].

Паспорт набору даних – сукупність метаданих, що містить опис набору даних, необхідний для його ідентифікації та використання [62].

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [6].

Підстави для обробки персональних даних – це: 1) *згода* суб'єкта ПД на обробку його ПД; 2) *дозвіл* на обробку ПД, наданий володільцю ПД відповідно до закону виключно для здійснення його повноважень; 3) укладення та виконання *правочину*, стороною якого є суб'єкт ПД або який укладено на користь суб'єкта ПД чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта ПД; 4) *захист* життєво важливих інтересів суб'єкта ПД; 5) *необхідність виконання обов'язку* володільця ПД, який передбачений законом; 6) *необхідність захисту законних інтересів* володільця ПД або третьої особи, якій передаються ПД, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта ПД у зв'язку з обробкою даних переважають ці інтереси [6].

Правова інформаційна система – це організаційно-технічна система, яка забезпечує вироблення рішень на основі автоматизації інформаційних процесів у правовій сфері життя суспільства [108].

Прикладні програмісти – розробляють програми обробки даних, що містяться в базах даних, відповідно до потреб кінцевих користувачів [108].

Принципи оприлюднення наборів даних у формі відкритих даних: 1) відкритість за замовчуванням; 2) оперативність і чіткість; 3) доступність і використання; 4) порівнянність та інтероперабельність; 5) покращене урядування і залучення громадян; 6) інклюзивний розвиток та інновації [62].

Публічна інформація, що містить персональні дані фізичної особи, оприлюднюється та надається на запит у формі відкритих даних у разі додержання однієї з таких умов: 1) персональні дані *знеособлені та захищені* відповідно до Закону України «Про захист персональних даних»; 2) фізичні особи (суб'єкти даних), персональні дані яких містяться в інформації у формі відкритих даних, надали свою згоду на поширення таких даних відповідно до Закону України «Про захист персональних даних»; 3) надання чи оприлюднення такої інформації *передбачено законом*; 4) *обмеження доступу до такої інформації (віднесення її до інформації з обмеженим доступом) заборонено законом*. Створення та забезпечення функціонування єдиного державного веб-порталу відкритих даних здійснюється центральним органом виконавчої влади, що реалізує державну політику у сфері електронного урядування [4].

Реляційна модель даних – являє собою набір двовимірних плоских таблиць, що складаються з рядків і стовпців. Первинний документ або лінійний масив являє собою *плоску двовимірну таблицю*. Така таблиця називається *відношенням*, кожен стовпець – *атрибутом*, сукупність значень одного типу (стовпця) – *доменом*, а рядка – *кортежем*. Стовпці таблиці є традиційними *елементами даних*, а рядки – *записами*. Таблиці (відношення) мають імена. Імена присвоюються також і стовпцям таблиці. Кожний кортеж (запис) відношення має *ключ*. Ключі бувають прості та складні. *Простий ключ* – це ключ, який складається з одного атомарного атрибута, значення якого унікальне (не повторюється). Складний ключ складається з двох і більше атрибутів. Для зв'язків відношень одного з одним у базі даних є *зовнішні ключі*. Атрибут або комбінація атрибута відношення є зовнішнім ключем, якщо він не є основним (первинним) ключем цього відношення, але є первинним ключем для іншого відношення [108].

Розпорядник персональних даних – фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця [6].

Система управління базами даних – це комплекс програмних засобів, які забезпечують створення структури БД, ведення БД, взаємодію користувача з БД. Або: **СУБД** – це комплекс програмних засобів, призначених для створення структури нової БД, наповнення її вмістом, редагування вмісту і візуалізації інформації [108].

Системні програмісти – забезпечують контроль за функціонуванням банку даних, розробляють програми, що розширюють можливості СУБД [108].

Структура набору даних – сукупність метаданих, що містить опис складу (елементів) набору даних, їх формат, параметри та призначення [62].

Суб'єкт персональних даних – фізична особа, персональні дані якої обробляються [6].

Типи даних (типи полів таблиць) СУБД Microsoft Access – це: 1) *текстовий* (255 символів у комірці); 2) *поле Мемо* (для розміщення великих фрагментів тексту – до 65535 символів); 3) *числовий* (збереження дійсних чисел); 4) *дата/час* (календарні дати і поточний час); 5) *рахівник* (лічильник); 6) *логічний* (тільки два значення – “так” чи “ні”); 7) *грошовий* (тип даних для зберігання грошових сум); 8) *поле об'єкта OLE* (об'єкти, що створені іншими додатками); 9) *гіперпосилання* (спеціальне поле для збереження URL Web-об'єктів Internet) [108].

Третя особа – будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних [6].

Функції Microsoft Access – це: 1) визначення (завдання структури й опис) даних; 2) обробка даних; 3) управління даними [108].

Microsoft Access – це функціонально повна реляційна СУБД. У ній передбачені усі необхідні засоби для визначення й обробки даних, а також для керування ними при роботі з великими обсягами інформації [108].

ДОДАТКОВА ІНФОРМАЦІЯ ДО ТЕМИ II

Архів – організація або її структурний підрозділ, що здійснюють прийняття для зберігання і зберігання документів із метою використання ретроспективної документальної інформації [78].

Архівна довідка – документ архівної установи, оформлений відповідно до законодавства, що містить інформацію про предмет запиту на підставі архівних документів із зазначенням їх пошукових даних [34]. Або: **архівна довідка** – офіційний документ архіву, що містить відомості з архівних документів, стосовні предмета запиту, із зазначенням адреси документів [78].

Видалення або знищення персональних даних – 1. Персональні дані видаляються або знищуються в порядку, встановленому відповідно до *вимог закону*. 2. Персональні дані підлягають видаленню або знищенню у разі: 1) *закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом*; 2) *припинення правовідносин* між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом; 3) *видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого*; 4) *набрання законної сили рішенням суду щодо видалення або знищення персональних даних*. 3. Персональні дані, зібрані з *порушенням вимог цього Закону*, підлягають видаленню або знищенню у встановленому законодавством порядку. 4. Персональні дані, зібрані під час виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом, видаляються або знищуються відповідно до вимог закону [6].

Відстрочення або відмова у доступі до персональних даних – 1. Відстрочення доступу суб'єкта персональних даних *до своїх персональних даних не допускається*. 2. Відстрочення доступу до персональних даних *третіх осіб допускається у разі*, якщо необхідні дані не можуть бути надані протягом тридцяти календарних днів з дня надходження запиту. При цьому загальний термін вирішення питань, порушених у запиті, не може перевищувати сорока п'яти календарних днів. Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення. 3. Відмова у доступі до персональних даних допускається, якщо доступ до них *заборонено згідно із законом* [6].

Довідковий апарат – довідники у будь-якій формі (путівники, описи, каталоги, покажчики, бази даних, номенклатури справ тощо), призначені для пошуку архівних документів або відомостей, що містяться в них [34].

Електронний довідник – електронно-довідковий перелік прикладного характеру, в якому зібрано типові набори даних [51].

Зміни і доповнення до персональних даних – 1. Володільці чи розпорядники персональних даних зобов'язані вносити зміни до персональних даних на підставі *вмотивованої письмової вимоги* суб'єкта персональних даних. 2. Володільці чи розпорядники персональних даних зобов'язані вносити зміни до персональних даних також за зверненням інших суб'єктів відносин, пов'язаних із ПД, якщо на це є *згода суб'єкта ПД* чи відповідна зміна здійснюється згідно з *приписом* Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого чи за рішенням суду, що набрало законної сили. 3. Зміна персональних даних, які не відповідають дійсності, проводиться невідкладно з моменту встановлення невідповідності [6].

Інтерфейс прикладного програмування – набір готових функцій, що надається у вигляді сервісу для використання у зовнішніх прикладних програмах для забезпечення динамічного доступу до наборів даних [62].

Інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які *відомості чи сукупність відомостей* про фізичну особу, яка ідентифікована або може бути *конкретно ідентифікована*, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, *за винятком даних* стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є *конфіденційною* і може бути поширена тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (ч. 5 п. 3.3 Рішення Конституційного Суду № 2-рпн/2012 від 20.01.2012).

Національний інформаційний фонд України – сукупність інформаційних фондів (інформаційних ресурсів) держави: архівного, бібліотечного, стандартів, архіву друку, фонду фільмів, патентного та інших фондів [37].

Національні електронні інформаційні ресурси – *систематизовані електронні інформаційні ресурси*, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під *електронними інформаційними ресурсами* розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів [15].

Національні ресурси – ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, призначені для задоволення потреб громадянина, суспільства, держави. Національні ресурси включають державні, комунальні та приватні ресурси [59].

Національні ресурси не повинні містити – 1) закликів до захоплення державної влади, насильницької зміни конституційного ладу, порушення територіальної цілісності і недоторканності України; 2) інформації, що містить пропаганду тероризму, війни, геноциду, або культу насильства і жорстокості; 3) інформації, що дискримінує особу за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, етнічного чи соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками; 4) інформації, що може зашкодити честі, гідності, або діловій репутації окремих осіб; 5) інформації, яка містить ненормативну лексику; 6) інформації порнографічного характеру. Забороняється використання національних ресурсів для розповсюдження забороненої, недостовірної та спотвореної інформації [59].

Недержавні ресурси – значна частина ресурсів формується у недержавному секторі і використовується для надання комерційних послуг з використанням національних ресурсів [59].

Несанкціоновані дії – доступ або спроба такого доступу до державних інформаційних ресурсів в інформаційних та телекомунікаційних системах без відповідно оформленого власником або уповноваженою ним особою дозволу, вірусне ураження, вчинення інших дій, які можуть призвести до порушення цілісності, доступності та конфіденційності цих ресурсів [65].

Несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, встановленого відповідно до законодавства [5].

Поширення персональних даних – 1) передбачає дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних; 2) без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини; 3) виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані; 4) сторона, якій передаються персональні дані, повинна попередньо вжити заходів щодо забезпечення вимог Закону України «Про захист персональних даних» [6].

Приватні ресурси – ресурси, які є об'єктом права приватної власності [59].

Реєстр ресурсів – сукупність даних, упорядкованих з метою обліку і реєстрації ресурсів [59].

Система національних ресурсів – організована за єдиною технологією сукупність національних ресурсів, необхідних для розв’язання завдань соціально-економічного розвитку держави та внесених до Національного реєстру електронних інформаційних ресурсів [59].

Суб’єкти відносин, пов’язаних із персональними даними – є: суб’єкт персональних даних; володілець персональних даних; розпорядник персональних даних; третя особа; Уповноважений Верховної Ради України з прав людини. *Володільцем чи розпорядником* персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи-підприємці, які обробляють персональні дані відповідно до закону. Розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить до сфери управління цього органу. Володілець персональних даних може доручити обробку персональних даних розпоряднику персональних даних відповідно до *договору, укладеного в письмовій формі*. Розпорядник персональних даних може обробляти персональні дані лише з метою і в обсязі, визначених у договорі [6].

Централізована бібліотечна система – об’єднання бібліотек в єдине структурно-цілісне утворення, куди входить центральна бібліотека [18].

Формати для оприлюднення наборів даних:

<i>Тип даних</i>	<i>Формат даних</i>
Текстові дані	TXT, RTF, ODT*, DOC(X), PDF (з текстовим змістом, нескановане зображення), (X)HTML*
Структуровані дані	RDF*, XML*, JSON*, CSV*, XLS(X), ODS*, YAML*
Графічні дані	GIF*, TIFF, JPG (JPEG)*, PNG*
Відеодані	MPEG, MKV, AVI, FLV, MKS, MK3D
Аудіодані	MP3, WAV, MKA
Дані, розроблені з використанням програми Macromedia Flash	SWF, FLV
Архів даних	ZIP*, 7z*, Gzip*, Bzip2*
Геопросторові дані	GeoTIFF, SHP, DMF, MID/MIF, DXF, XML, GeoJSON, GPX, LOC, ARINC, AIXM.

Під час створення нових наборів даних забезпечується використання відкритих форматів даних (формати з позначкою “*” в таблиці) та структурованих даних (формати RDF, XML, JSON, CSV) [62].

ТЕМА III. ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ «ІНФОРМАЦІЙНИЙ ПОРТАЛ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ» У БОРОТБІ ЗІ ЗЛОЧИННІСТЮ

Автоматизований облік адміністративних правопорушень – призначений для здійснення *перевірки особи*, яка вчинила адміністративне правопорушення, на наявність (відсутність) даних про *повторне протягом року* вчинення однорідного правопорушення, за яке особу притягнуто до адміністративного стягнення, *аналізу стану* застосування адміністративного законодавства органами поліції та формування статистичної звітності, у тому числі у сфері безпеки дорожнього руху. Автоматизований облік адміністративних правопорушень здійснюється в *інтегрованій інформаційно-пошуковій системі* на підставі протоколів (постанов), складених (винесених) уповноваженими на те посадовими особами Національної поліції. Відомості про виявлене адміністративне правопорушення вносяться до електронної картки про адміністративне правопорушення, що заповнюється уповноваженим працівником органу Національної поліції, який є авторизованим користувачем та має доступ до ІПС для введення і коригування даних. Начальники органів Національної поліції визначають *уповноважених працівників* органів Національної поліції, яким у зв'язку з виконанням ними службових обов'язків необхідно надати доступ до ІПС для формування автоматизованого обліку адміністративних правопорушень. Надання доступу до ІПС здійснюється на підставі *заявки*, підписаної начальниками органів Національної поліції або особами, які виконують їх обов'язки, та надісланої до Управління інформаційно-аналітичної підтримки Головного управління Національної поліції України [89].

Автоматизовані робочі місця користувачів системи «Інформаційний портал Національної поліції України» – це робочі місця поліцейських та інших працівників поліції, обладнані комп'ютерною технікою, у тому числі планшетними комп'ютерами, що підключені до телекомунікаційної мережі доступу системи «Інформаційний портал Національної поліції України» (далі – ІПНП) і призначені для автоматизації службової діяльності, реалізації повноважень обробляти інформацію відповідно до наданого рівня доступу в системі ІПНП [87].

Адміністратор ІПС – це керівник структурного підрозділу Департаменту інформаційних технологій (станом на сьогодні – Департаменту інформатизації МВС), відповідальний за експлуатацію ІПС. Повноваження адміністратора ІПС на регіональному рівні надаються керівникові структурного підрозділу управління (відділу) інформаційних технологій, відповідальному за експлуатацію регіонального вузла ІПС. Адміністратору ІПС підпорядковуються адміністратори регіональних вузлів ІПС. Адміністратор ІПС відповідає за: 1) *цілодобове функціонування ІПС*; 2) *супроводження типових програмних засобів інформаційних підсистем ІПС, технологічне забезпечення обміну інформаційними ресурсами між ІПС відповідних рівнів*; 3) *здійснення контролю за формуванням та підтриманням в актуальному стані інформаційних ресурсів ІПС*; 4) *здійснення контролю за дотриманням правил, процедур, технології обробки інформації користувачами* [86].

Адміністратор системи Інтернет в НПУ – посадова особа Департаменту зв'язку та телекомунікацій Національної поліції України (далі – ДЗТ), який згідно з функціональними (посадовими) обов'язками здійснює програмно-апаратне супроводження центрального вузла доступу системи Інтернет, *адмініструє, координує та налаштовує* роботу користувачів системи Інтернет та *підтримує його працездатність*, а також *керує та спрямовує діяльність відповідальних осіб органів і підрозділів Національної поліції України*. Адміністратор системи Інтернет **має право**: 1) *самостійно блокувати доступ* до системи Інтернет у випадку передачі користувачем у системі Інтернет інформації, що становить державну таємницю та іншу інформацію з обмеженим доступом; 2) *скасовувати доступ* користувачам у наступних випадках: а) у зв'язку із зміною структури та штатних розписів підрозділів НПУ; б) у зв'язку з кадровими змінами (прийняття, звільнення, переміщення працівників, які мали доступ до системи Інтернет); в) у зв'язку із відсутністю подальшої службової необхідності у використанні доступу до системи Інтернет. Процедура скасування передбачає призупинення доступу протягом 1 місяця та знищення відповідних ним облікових записів із системи Інтернет після закінчення цього терміну. Рішення про скасування доступу до системи Інтернет приймає керівник ДЗТ; 3) *припинити доступ* до Інтернет за *запитом керівника підрозділу* даного користувача;

4) звернутися до відповідальної особи з пропозицією скасування доступу до системи Інтернет, у разі відсутності її використання протягом півріччя. Адміністратор системи Інтернет **зобов'язаний**: 1) у термін до 10 робочих днів (з дня надходження погодженої заявки до ДЗТ) та за наявності технічної можливості, *надати доступ* до системи Інтернет; 2) *реєструвати нових користувачів* у центральному реєстрі обліку користувачів; 3) *надавати послуги* системи Інтернет в Національній поліції України; 4) *підтримувати працездатність* центрального вузла доступу до системи Інтернет, *виконувати регламентні та профілактичні роботи* на ньому і *забезпечувати* його програмно-апаратну підтримку; 5) *надавати практичну допомогу* користувачам системи Інтернет у разі виникнення нетипових ситуацій, пов'язаних з роботою системи Інтернет; 6) *надавати користувачам необхідну консультативну допомогу* по роботі з системою Інтернет; 7) *забезпечити налаштування спеціалізованого програмного забезпечення* центрального вузла доступу системи Інтернет; 8) *забезпечити налаштування доступу до сервісів системи Інтернет*; 9) *проводити резервне копіювання та архівування налаштувань* центрального вузла доступу системи Інтернет після кожної суттєвої зміни конфігурації; 10) *проводити відновлення налаштувань* центрального вузла доступу системи Інтернет у випадках незадовільної роботи системи Інтернет; 11) *відключати користувачів у разі невиконання ними своїх обов'язків*, пов'язаних із використанням системи Інтернет та *обов'язково доповідати* про такі факти керівництву ДЗТ; 12) *блокувати доступ до сервісу системи Інтернет на центральному вузлі доступу* у разі незадовільної роботи сервісу [101].

Адміністратор системи ІППП – є уповноважений структурний підрозділ апарату центрального органу управління Національної поліції України [87]. Адміністратор системи ІППП забезпечує: 1) вирішення організаційних питань щодо забезпечення функціонування системи; 2) ведення обліку користувачів та надання їм доступу до інформації, що в ній обробляється; 3) захист інформації від несанкціонованого доступу, знищення, модифікації та блокування доступу до неї шляхом здійснення організаційних і технічних заходів, впровадження засобів та методів технічного захисту інформації; 4) вжиття заходів стосовно розвитку і вдосконалення системи; 5) координацію функціонування складових системи.

Бази даних поліції, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, містять відомості – зокрема, стосовно: 1) *повідомлень* про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, що надійшли технічними каналами зв'язку; 2) *щодобових переліків та складу* нарядів поліції та слідчо-оперативних груп, що заступають на чергування; 3) *завдань та орієнтувань*, що доводились до нарядів поліції для реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події; 4) *звітування нарядів поліції* за результатами реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, виявлення додаткових обставин на місці пригоди; 5) *пересувань нарядів поліції*, які отримані із планшетних комп'ютерів (мобільних терміналів) та засобами GPS [87]. Поліція може створювати *інші бази даних*, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, відповідно до ст. 25 Закону України «Про Національну поліцію» [8].

Використання інформаційних ресурсів ІПС – МВС забезпечує використання інформації, що зберігається в банках даних ІПС, виключно зі *службовою метою* згідно з чинним законодавством. *Строки зберігання інформації* в ІПС визначаються відповідно до чинного законодавства. МВС забезпечує реалізацію *права кожної особи знайомитися* з інформацією про себе, яка зберігається в банках даних ІПС, відповідно до чинного законодавства. Інформація з банків даних ІПС надається у *формі витягів безкоштовно на письмову вимогу* суду, органів прокуратури, дізнання і слідства, інших органів державної влади (посадових осіб) у зв'язку зі здійсненням ними повноважень, визначених чинним законодавством [86].

Вимоги до створення та використання паролю: 1) пароль визначається, використовується та змінюється користувачем особисто і розголошенню не підлягає (конфіденційність); 2) довжина паролю повинна бути не менше 8 (12) символів; 3) необхідно використовувати у паролі поєднання літер та цифр; 4) пароль повинен містити літери верхнього та нижнього регістру; 5) пароль повинен містити окремі спецсимволи (!@#\$%^&*()_+?!); 6) пароль не повинен починатись або закінчуватися символом «пробілу»; 7) для створення паролю необхідно вибрати бажану мову клавіатури;

8) рекомендується використовувати для пароля перемикання мов; 9) бажано використовувати випадкову (безглузду) комбінацію символів (наприклад, набирати пароль кирилицею в латинській розкладці); 10) необхідно використовувати заміну окремих символів в паролі на символи, які схожі за написанням (наприклад, І ~ 1; О ~ 0; Ч ~ 4; А ~ @; С ~ \$; Л ~ / \; В ~ 8; 3 ~ 3; Б ~ 5); 11) пароль не повинен містити персональні дані користувача; 12) не бажано використовувати паролі зі сфери своєї діяльності; 13) бажано використовувати заміну пробілів між словами в паролі на дефіси чи нижні підкреслення; 14) не бажано використовувати повторення символів; 15) пароль не повинен співпадати з логіном; 16) пароль не повинен складатися з цілого слова та не з словика; 17) забороняється використовувати стандартні паролі, засновані на повторенні, словникових словах, літерних або числових послідовностях; 18) можна використовувати для складання паролю генератори паролів; 19) можна використовувати можливості візуального ключа; 20) можна використовувати можливість оцінки паролю за ступенем надійності (наприклад, програма Password Meter); 21) для кожної програми та системи необхідно мати свій пароль; 22) складні паролі необхідно створювати для важливих програм; 23) для легкого запам'ятовування складних паролів бажано визначити правила їх формування (наприклад, перетворення віршів, пісень тощо); 24) для відновлення доступу до інформаційних ресурсів у разі забуття паролю не використовуйте можливість підказки у вигляді «ключового слова»; 25) для відновлення доступу до інформаційних ресурсів у разі забуття паролю можна використовувати номер мобільного телефону або адресу E-mail (як у випадку двохетапної аутентифікації); 26) під час створення та використання паролю необхідно встановити режим «невидимий при наборі»; 27) не використовуйте запропоновану системою можливість запам'ятати пароль під час його використання; 28) необхідна періодична зміна паролю (термін зміни паролю визначається адміністратором системи, але не рідше одного разу в 60-90 днів); 29) зміна паролю повинна бути не за графіком, а випадковим чином; 30) новий пароль повинен значно відрізнятися від попереднього паролю; 31) створений пароль необхідно запам'ятати (забороняється записувати та залишати пароль на видному місці); 32) необхідно негайно змінювати пароль у разі підозрі про його розкриття; 33) інші (укладач: Кудінов В.А.).

Відповідальна особа за актуалізацію та працездатність користувачів системи Інтернет в НПУ – відповідна посадова особа підрозділу зв'язку та телекомунікацій *зобов'язана*: 1) приймати заявки від посадових осіб НПУ на заведення, зміну або ліквідацію доступу до Інтернет; 2) надавати користувачам НПУ необхідну консультативну допомогу по роботі в Інтернет; 3) проводити один раз на рік (до 25 грудня) облік діючих користувачів, інформацію про яких уносити в Журнал обліку користувачів; 4) забезпечувати налаштування програмного забезпечення на робочому місці користувача системи Інтернет [101].

Держатель (власник) ІПС – є МВС України [86].

Джерела формування інформаційних ресурсів ІПС – є: 1) зареєстровані в органах НПУ заяви і повідомлення про злочини та адміністративні правопорушення, кримінальні справи; 2) повідомлення працівників органів НПУ у разі звернення до них громадян або службових осіб із заявою чи повідомленням про події, які загрожують особистій чи громадській безпеці, або у разі безпосереднього виявлення таких; 3) повідомлення про аварії, пожежі, катастрофи, стихійні лиха та інші надзвичайні події, які підлягають реєстрації в органах НПУ; 4) повідомлення засобів масової інформації, публічні виступи; 5) рішення органів (посадових осіб), виконання яких покладено на органи НПУ; 6) видані на ім'я особи документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень; 7) інформація, отримана під час проведення гласних оперативно-розшукових заходів від громадян і посадових осіб, про вчинені злочини (правопорушення); 8) інформація, отримана від правоохоронних органів іноземних держав на підставі міжнародних договорів України, угод про співробітництво між МВС і відповідними органами іноземних держав у сфері боротьби із злочинністю. Інформація, що обробляється в ІПС, є власністю держави і підлягає захисту відповідно до чинного законодавства [86].

Доступ до інформаційних ресурсів ІПС – авторизований доступ до них здійснюється безпосередньо з АРМ. Факт внесення, обробки, отримання інформації, виконання запиту користувачем стосовно об'єкта обліку ІПС фіксується в системному журналі реєстрації роботи користувачів ІПС [86].

Завдання ІПС – відповідно до свого призначення ІПС вирішує такі завдання: 1) *автоматизація процесів* обліку отриманої інформації, обробки інформаційних запитів, *пошук та відбір* необхідної інформації; 2) виконання *інформаційно-пошукових заходів*, проведення *аналітичних досліджень*; 3) *обмін інформацією* між інтегрованими банками даних ІПС відповідних рівнів та забезпечення постійного зв'язку між ними, уніфікація технологічних процедур опрацювання документів, збирання, реєстрації, накопичення та обробки інформації, що надходить до кожного з банків даних; 4) *постійне формування, оновлення та адміністрування банків даних* ІПС, забезпечення *достовірності, оперативного доступу та збереження інформаційного ресурсу*; 5) *формалізація технологічних процесів* обробки інформації, визначення типових маршрутних технологічних схем для їх виконання; 6) забезпечення *надійного зберігання* інформаційних обліків, максимально зручна їх систематизація; 7) забезпечення *комплексного захисту інформації та розмежування доступу до інформації*, що зберігається в ІПС; 8) *автоматизація збирання даних про результати виконання технологічних процесів* щодо інформаційних обліків, *формування аналітичних і статистичних звітів* (довідок); 9) *інформаційне забезпечення управлінської діяльності*, підготовка аналітично-довідкових матеріалів; 10) *наскрізний контроль* (підрозділ контролю, керівник органу НПУ, безпосередній виконавець) за своєчасністю і повнотою надання первинних облікових та інформаційно-пошукових документів, проведення *аналізу їх повноти, сумісності та об'єктивності* [86].

Інтегрована інформаційно-пошукова система МВС України – це сукупність різних довідково-інформаційних та оперативно-розшукових обліків, які інтегровані в одну єдину систему. Інтеграція відомостей здійснюється за установчими даними на особу (прізвище, ім'я, по батькові, дата та місце народження) [86]. *Або: Інтегрована інформаційно-пошукова система МВС України* – це сукупність організаційно-розпорядчих заходів, програмно-технічних та інформаційно-телекомунікаційних засобів, що забезпечують формування та ведення довідково-інформаційних, оперативно-розшукових обліків, авторизований доступ до інформаційних ресурсів ІПС [86].

Інформаційне забезпечення ІПС базується – на цілісності та непротивіччі інформації в єдиному інформаційному просторі організаційної інфраструктури обліків ІПС, що забезпечується використанням типового програмного забезпечення, єдиної технології обробки та обміну даними, типовою структурою даних та правилами їх інтеграції, уніфікованою системою класифікації, кодування та контролю інформації [86].

Інформаційні ресурси (об'єкти обліку) ІПС – є об'єктивно поєднаний набір відомостей, що безпосередньо стосується осіб, подій (злочинів, адміністративних правопорушень), надзвичайних подій, який накопичується в процесі службової діяльності органів НПУ в обсязі, структурі й порядку, що визначаються завданнями, покладеними на органи НПУ, відповідно до чинного законодавства [86].

Інформаційні ресурси системи «Інформаційний портал Національної поліції України» – є інформація, що утворена в процесі діяльності поліції та використовується для формування: 1) *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»; 2) *баз даних у сфері управлінських відносин*, необхідних для виконання покладених на поліцію повноважень; 3) *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 [87].

Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» – сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення. Система ІПНП є складовою частиною ЄІС МВС. *Складовими системи ІПНП є:* 1) центральний програмно-технічний комплекс; 2) автоматизовані робочі місця користувачів; 3) телекомунікаційна мережа доступу; 4) комплексна система захисту інформації [87].

Комплексна система захисту інформації системи ІПП з підтвердженою відповідністю – взаємопов’язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації. Завданням комплексної системи захисту інформації є забезпечення *конфіденційності* (у разі обробки інформації з обмеженим доступом), *цілісності*, *доступності інформації* в системі ІПП шляхом здійснення заходів, спрямованих на захист інформації від несанкціонованих дій (у тому числі з використанням комп’ютерних вірусів), які можуть призвести до її випадкової або умисної модифікації чи знищення. Контроль за дотриманням вимог законодавства України в сфері захисту інформації під час використання ІПП здійснює керівник підрозділу, де експлуатується центральний програмно-технічний комплекс системи [87].

Користувач системи Інтернет в НПУ – посадова особа НПУ, якому надано доступ до системи Інтернет у телекомунікацій мережі НПУ. Користувачам *забороняється* передавати в системі Інтернет інформацію, що становить державну таємницю, та іншу інформацію з обмеженим доступом. *Відповідальність за порушення цих вимог* несе посадова особа НПУ, зареєстрована як користувач. Користувач *має право*: 1) *користуватися* системою Інтернет для виконання своїх службових обов’язків; 2) *отримувати послуги*, що надаються системою Інтернет; 3) *звертатись за консультацією* щодо користування системою Інтернет до відповідальної особи або адміністратора системи Інтернет. Користувач *зобов’язаний*: 1) при роботі в системі Інтернет *виконувати вказівки* відповідальної особи або адміністратора системи Інтернет; 2) використовувати послуги системи Інтернет тільки *в межах службових повноважень*; 3) *забезпечити виконання вимог законодавства України* щодо роботи в глобальній мережі Інтернет. Користувачу системи Інтернет *забороняється*: 1) *надавати доступ* до системи Інтернет *іншим особам*; 2) *розповсюджувати в системі Інтернет відомості, що містять*: а) інформацію з обмеженим доступом; б) недостовірну інформацію, а також інформацію, що ображає честь і гідність інших осіб; в) віруси або інші комп’ютерні коди, файли, програми, призначені для порушення, знищення або обмеження функціональності будь-якого телекомунікаційного обладнання, програми для здійснення несанкціонованого доступу [101].

Користувачі ІПС – це працівники правоохоронних органів, яким розпорядником ІПС відповідно до вимог чинного законодавства надано право доступу до інформації в ІПС [86].

Користувачі системи ІПНП – є посадові особи органів (підрозділів) поліції, яким в установленому порядку надано право доступу до інформації в цій системі. *Ідентифікація користувача та підтвердження цілісності даних*, що обробляються в системі ІПНП, забезпечуються застосуванням електронного цифрового підпису або інших програмно-технічних засобів авторизації користувачів та забезпечення цілісності даних. Кожна дія користувача щодо отримання інформації з інформаційних ресурсів системи ІПНП фіксується у *спеціальному електронному архіві*. Користувачі системи ІПНП зобов'язані *не розголошувати* у будь-який спосіб інформацію, яка їм стала відома у зв'язку з виконанням посадових обов'язків, крім випадків, передбачених законом, *відповідають за достовірність інформації*, що вводиться ними до відповідних інформаційних ресурсів системи ІПНП, та зобов'язані дотримуватися законодавства у сфері захисту інформації [87].

Мета створення ІПС – є об'єднання існуючих в МВС України інформаційних ресурсів в єдиний інформаційно-аналітичний комплекс із використанням сучасних інформаційних технологій, комп'ютерного та телекомунікаційного обладнання для підтримки оперативно-службової діяльності органів і підрозділів поліції, суттєвого зміцнення їх спроможності протидії та профілактики злочинності [86].

Основні завдання системи «Інформаційний портал Національної поліції України» – це: 1) інформаційно-аналітичне забезпечення діяльності Національної поліції України; 2) забезпечення наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до ЄІС МВС; 3) забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу; 4) забезпечення електронної взаємодії з МВС та іншими органами державної влади [87].

Перелік баз даних Інтегрованої інформаційно-пошукової системи МВС України – це: 1) БД «Єдиний облік». 2) БД «Злочин». 3) БД «Доставлені». 4) БД «Контур». 5) БД «Особа». 6) БД «Розшук». 7) БД «Адміністративне правопорушення». 8) БД «Корупційне правопорушення». 9) БД «Мігрант». 10) БД «Угон». 11) БД «Річ». 12) БД «Втрачені документи». 13) БД «Кримінальна зброя». 14) БД «Зареєстрована зброя». 15) БД «Електронний рапорт». 16) БД «Пізнання». 17) БД «Антикваріат». 18) БД «Кримінальна статистика». 19) БД «ЄДРПОУ». 20) БД «Домашній арешт».

Положення про систему Інтернет у телекомунікаційній мережі Національної поліції України – визначає порядок функціонування системи Інтернет у телекомунікаційній мережі Національної поліції України, права і обов'язки адміністратора, відповідальних осіб та користувачів системи Інтернет, регулює взаємовідносини між ними і є обов'язковим для виконання в телекомунікаційній мережі передачі даних Національної поліції України. Розвиток системи Інтернет у телекомунікаційній мережі Національної поліції України, його супроводження, технічне обслуговування та підключення користувачів здійснюються виключно підрозділами зв'язку та телекомунікацій Національної поліції України [101].

Порядок отримання доступу до системи Інтернет в НПУ – для надання можливості користування послугами системи Інтернет, керівником підрозділу готується *заявка* на підключення користувачів або надання необхідних інтернет-сервісів за відповідною формою та після погодження підрозділами режиму та технічного захисту інформації Національної поліції України, направляється для опрацювання в ДЗТ на реалізацію в межах технічної можливості. Листи, заявки або інші повідомлення щодо незадовільної роботи системи Інтернет приймаються та реєструються підрозділами зв'язку та телекомунікацій Національної поліції України. Рішення про відновлення працездатності приймається керівниками підрозділів зв'язку та телекомунікацій Національної поліції України. Забезпечення функціонування системи Інтернет покладається на адміністратора та відповідальних осіб [101].

Порядок складання та подання запитів на отримання публічної інформації, розпорядником якої є Національна поліція України – розроблено відповідно до Закону України «Про доступ до публічної інформації» [4] з метою врегулювання механізму складання та подання запитів на публічну інформацію, розпорядником якої є Національна поліція України, до центрального органу управління поліцією, міжрегіональних територіальних органів Національної поліції, їх відокремлених підрозділів, територіальних органів поліції, їх структурних та відокремлених підрозділів, закладів та установ, що належать до сфери управління НПУ. Право на доступ до публічної інформації гарантується *максимальним спрощенням процедури подання запиту* на отримання публічної інформації. *Запитувач має право* звернутися до органів та підрозділів поліції із запитом незалежно від того, стосується ця інформація його особисто чи ні, без пояснення причини подання запиту. Запит може бути *індивідуальним або колективним*. Запит подається до органів та підрозділів поліції в усній чи письмовій формі особисто або шляхом надсилання поштовим зв'язком, факсимільним зв'язком, електронною поштою або телефоном на вибір запитувача. *Письмовий запит* подається в довільній формі. *Запит повинен містити:* 1) прізвище, ім'я, по батькові (найменування) запитувача, його поштову адресу або адресу електронної пошти, а також номер засобу зв'язку, якщо такий є; 2) загальний опис інформації або вид, назву, реквізити чи зміст документа, щодо якого зроблено запит, якщо запитувачу це відомо; 3) підпис і дату за умови подання письмового запиту. Для оформлення письмового запиту запитувач може використати *форму запиту на отримання публічної інформації*, яку можна отримати в розпорядника інформації та на офіційних веб-сайтах центрального органу управління поліцією, територіальних органів НПУ. У разі якщо особа з поважних причин (інвалідність, обмежені фізичні можливості тощо) *не може подати письмовий запит особисто*, його оформлює працівник підрозділу документального забезпечення, відповідальна особа із зазначенням у ньому своїх прізвища, імені, по батькові, контактного телефону та надає копію запиту особі, якій надано допомогу в його оформленні. *На вимогу запитувача на першому аркуші копії запиту ставиться штамп із зазначенням найменування органу чи підрозділу поліції, дати надходження та вхідного номера запиту*. Така копія повертається запитувачу [107].

Послуги системи Інтернет в НПУ – надання доступу користувачам НПУ до різноманітних сервісів глобальної мережі Інтернет або створення Інтернет-серверів НПУ у глобальній мережі Інтернет. *До основних послуг системи Інтернет належить:* 1) забезпечення доступу користувачів до інформації у мережі Інтернет; 2) реєстрація/перереєстрація користувачів; 3) забезпечення доступу до сервісів системи Інтернет із глобальної мережі Інтернет; 4) організація контролю за доступом до сервісів системи Інтернет із глобальної мережі; 5) централізоване ведення та оновлення списків користувачів. ДЗТ може розширювати або змінювати перелік послуг залежно від технічних можливостей та відповідного програмного забезпечення в межах своєї компетенції [101].

Призначення системи ІПП – для: 1) формування інформаційних ресурсів ЄІС МВС; 2) обробки інформації, яка утворена в процесі діяльності поліції; 3) надання безпосереднього оперативного доступу до інформаційних ресурсів ЄІС МВС; 4) 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; 5) здійснення пошукових та аналітичних функцій для використання інформації з інформаційних ресурсів (баз даних) поліції, МВС та інших органів державної влади; 6) 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; 7) забезпечення автоматизації процесів управління силами та засобами поліції; 8) забезпечення електронного документообігу в органах (підрозділах) поліції, обміну електронними документами з МВС; 9) комплексного захисту інформації та розмежування доступу до інформації, що зберігається в базах даних системи ІПП [87].

Розпорядник ІПС – є Департамент інформатизації МВС. Завдання розпорядника – управління ІПС та відповідними складовими системи, контроль за формуванням та підтриманням в актуальному стані інформаційних ресурсів ІПС, надання користувачам прав доступу до ІПС, ведення їх обліку, вживання заходів щодо розвитку і вдосконалення ІПС [86].

Розпорядник системи ІППП – є Національна поліція України. Розпорядник системи ІППП вживає заходів із організації матеріально-технічного та кадрового забезпечення, що необхідні для ефективного функціонування системи [87].

Система Інтернет в НПУ – відомча система сервісів глобальної мережі Інтернет у НПУ, з центральним вузлом доступу. Використання системи Інтернет є складовою частиною телекомунікаційного забезпечення НПУ і надає можливість організувати обмін інформацією між сервісами, користувачами системи Інтернет НПУ та глобальною мережею Інтернет. Система Інтернет у телекомунікаційній мережі НПУ побудована за *ієрархічним принципом на не комутованих (виділених) цифрових каналах зв'язку* за технологією IP VPN та є складовою частиною телекомунікаційної мережі НПУ. Зв'язок із зовнішнім сегментом глобальної мережі Інтернет здійснюється *через центральний вузол доступу системи Інтернет*. Для функціонування системи Інтернет у НПУ, на центральному вузлі доступу системи Інтернет для кожного користувача або сервісу (інтернет-серверу) налаштовується доступ до глобальної мережі Інтернет. Функціонування системи Інтернет для користувачів побудовано *на принципі клієнт-сервер* – програмне забезпечення користувача системи Інтернет (веб-браузер) *не має безпосередній доступ до глобальної мережі Інтернет*, а обмін інформацією з глобальною мережею Інтернет проходить *через транзитний сервер* центрального вузла доступу системи Інтернет. Функціонування системи Інтернет для сервісів побудовано на принципі переправлення сервісних портів – сервіс системи Інтернет, який не має безпосереднього доступу до глобальної мережі Інтернет, а обмін інформацією з мережею Інтернет проходить через транзитний сервер центрального вузла доступу системи Інтернет [101].

Склад інформаційних ресурсів (об'єктів обліку) ІПС – належать відомості щодо: 1) осіб, яких затримано за підозрою в учиненні злочину, які звинувачуються в учиненні злочину, узяті під варту або піддані адміністративному арешту, у тому числі їх фотографії та дактилоскопічні дані; 2) розшукуваних осіб, які переховуються від органів слідства і суду, ухиляються від виконання кримінального покарання, пропали безвісти, та в інших випадках, передбачених Законами України; 3) осіб, щодо яких здійснюється профілактична робота працівниками органами поліції;

4) осіб, які скоїли адміністративні правопорушення, щодо яких уповноваженими на те працівниками поліції згідно зі статтями 254, 255 Кодексу України про адміністративні правопорушення (далі – КУпАП) складено протоколи про адміністративні правопорушення, а органами (посадовими особами), які розглядали ці справи, було винесено постанови, передбачені статтею 284 КУпАП; 5) осіб, яких було виявлено уповноваженими на те працівниками поліції у сфері протидії корупції за скоєння корупційних правопорушень і рішеннями судів притягнуто до відповідальності за вчинення цих правопорушень; 6) іноземців та осіб без громадянства, які порушили встановлені законодавством правила в'їзду, виїзду, перебування в Україні і транзитного проїзду через її територію, виявлених працівниками поліції; 7) зареєстрованих в поліції злочинів, адміністративних правопорушень, подій, які загрожують особистій чи громадській безпеці, надзвичайних подій; 8) викрадених речей, документів, цінностей та іншого майна; 9) знайдених, вилучених у затриманих (заарештованих) осіб і зданих до поліції речей, документів, цінностей та іншого майна; 10) вилучених у громадян і службових осіб предметів і речей, заборонених або обмежених в обороті, а також документів з ознаками підробки; 11) зброї, що перебуває у користуванні громадян, підприємств, установ, організацій, господарських об'єднань, яким надано відповідно до законодавства дозвіл на її придбання, зберігання, носіння, перевезення, та яка обліковується підрозділами дозвільної системи поліції. Як допоміжний засіб документування та попередження протиправних дій, розкриття правопорушень проводиться фотофіксація осіб (речей, цінностей), фотозображення яких входять до структури об'єктів обліку ІПС [86].

Структура ІПС – побудована за трирівневою ієрархічною структурою: *перший рівень* – центральний вузол (банк даних) ІПС – розташовано в спеціально виділених службових приміщеннях Департаменту інформатизації МВС; *другий рівень* – регіональні (обласні) вузли (банки даних) ІПС; *третій рівень* – територіальний вузол ІПС [86].

Структура системи ІПП – це: 1) центральний програмно-технічний комплекс; 2) автоматизовані робочі місця користувачів; 3) телекомунікаційна мережа доступу; 4) комплексна система захисту інформації [87].

Суб'єкти правових відносин ІПС – є: 1) держатель (власник) ІПС; 2) розпорядник ІПС; 3) користувачі ІПС; 4) адміністратор ІПС; 5) адміністратор безпеки ІПС [86].

Суб'єкти системи ІПП – це: 1) розпорядник системи; 2) адміністратор системи; 3) користувачі системи [87].

Телекомунікаційна мережа доступу системи ІПП – це сукупність технічних і програмних засобів, призначених для обміну інформацією між складовими системи. Для захисту інформації, що обробляється органами (підрозділами) поліції в системі ІПП, використовуються канали єдиної цифрової відомчої телекомунікаційної мережі Міністерства внутрішніх справ України, а при використанні відкритих каналів – засоби захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації [87].

Центральний вузол доступу системи Інтернет в ІПУ – програмно-технічний комплекс з відповідним технічним та програмним забезпеченням системи Інтернет для підключення та обслуговування користувачів Національної поліції України, а також надання доступу до Інтернет сервісів Національної поліції України, який територіально розташований в серверній залі ДЗТ [101].

Центральний програмно-технічний комплекс системи ІПП – це сукупність технічних і програмних засобів, призначених для обробки інформації, які забезпечують: 1) введення, записування, зберігання, видалення, знищення, приймання та передавання інформації та формування баз даних у системи ІПП; 2) формування тимчасових наборів даних для наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних ЄІС МВС; 3) моніторинг стану інформаційного обміну між складовими системи ІПП, а також системних журналів аудиту роботи користувачів, технічних і програмних засобів; 4) захист інформації під час її обробки [87].

ДОДАТКОВА ІНФОРМАЦІЯ ДО ТЕМИ III

Адміністратор безпеки ІПС – це керівник підрозділу Департаменту інформаційних технологій (станом на сьогодні – Департаменту інформатизації МВС), відповідальний за дотримання політики безпеки в ІПС. Адміністратору безпеки ІПС підпорядковуються адміністратори безпеки регіональних вузлів ІПС. Адміністратор безпеки ІПС відповідає за: 1) цілодобовий та безперервний захист інформаційних ресурсів ІПС; 2) розмежування доступу до інформаційних ресурсів ІПС, реєстрацію та авторизацію користувачів; 3) забезпечення захисту відомостей інформаційних ресурсів ІПС від блокування, порушення цілісності та несанкціонованого доступу; 4) здійснення контролю за дотриманням правил і процедур обробки інформації користувачами; 5) збереження інформаційних масивів шляхом створення резервного банку даних [86].

АПС «Канцелярія» – автоматизована інформаційно-пошукова система «Канцелярія», що використовується для автоматизації процесів діловодства (облік документів шляхом створення електронних реєстраційних карток та накопичення інформації про рух і виконання документів) за допомогою комп'ютерної техніки [76].

Захист інформаційних ресурсів ІПС – здійснюється шляхом створення та забезпечення функціонування комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, визначеному вимогами Положення про державну експертизу в сфері технічного захисту інформації, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93, зареєстрованого в Міністерстві юстиції України 16.07.2007 за № 820/14087. КСЗІ забезпечує захист інформаційних ресурсів (банків даних) ІПС шляхом упровадження комплексу технічних, криптографічних, організаційних та інших заходів і засобів захисту інформації, спрямованих на недопущення блокування інформації, несанкціонованого ознайомлення з нею та/або її модифікації. Завданням КСЗІ ІПС відповідно до нормативних документів з технічного захисту інформації є забезпечення встановленої політики безпеки та реалізація необхідних організаційних, інженерно-технічних заходів і програмно-технічних засобів захисту, ефективне протистояння ймовірним загрозам інформаційним ресурсам ІПС з надання основних функціональних послуг безпеки: конфіденційності, цілісності, доступності, спостережливості [86].

Опитувана особа на поліграфі – особа, яка досягла 18-річного віку та є працівником Національної поліції України або кандидатом для прийняття на службу в поліцію, визначена в завданні на проведення опитування, та надала добровільну згоду на проходження процедури опитування з використанням поліграфа [94].

Опитування з використанням поліграфа – спеціально організований і науково-обґрунтований комплекс прийомів отримання, порівняння та інтерпретації психофізіологічних реакцій людини у відповідь на психологічні подразники. Метою проведення опитування є перевірка наданої інформації. Результати опитування не мають будь-якої доказової сили, несуть вірогідний та орієнтовний характер, є одним із джерел інформації, що підлягає оцінці разом з іншою сукупністю зібраних даних. Результати опитування не можуть бути підставою для застосування заходів, які обмежують законні права та свободи опитуваної особи [94].

Основні принципи використання поліграфа – 1) *принцип добровільної згоди* (спеціаліст проводить опитування лише за умови отримання письмової згоди опитуваної особи); відмова від опитування не може тягти за собою утиск особи, порушення її законних прав та свобод; 2) *принцип правомірності опитування*, відповідно до якого проводиться тільки за наявності відповідного завдання та в межах визначеного кола питань, про що спеціаліст повідомляє опитувану особу; 3) *принцип комплексності* – під час проведення опитування використовують всі наявні матеріально-технічні та методичні можливості з метою забезпечення повної та всебічної обґрунтованості висновків щодо опитуваної особи; спеціаліст повинен забезпечити опитуваній особі психологічний комфорт; 4) *принцип конфіденційності* – інформація, отримана спеціалістом під час проведення опитування, а також та, що міститься в довідці про результати опитування з використанням поліграфа, не підлягає розголошенню, крім випадків, передбачених законодавством України; 5) *принцип забезпечення прав і свобод людини під час проведення опитування* – спеціаліст повинен дотримуватись основоположних прав і свобод людини, гарантованих Конституцією України, Конвенцією про захист прав людини і основоположних свобод, а також міжнародними договорами. Опитувана особа повинна знати, щодо якої події проводиться опитування, бути ознайомлена з тематикою запитань, має право відмовитися від опитування на будь-якому етапі, не надавати пояснень щодо виникнення у нього тих чи інших психофізіологічних реакцій; 6) *принцип законності* – спеціаліст діє виключно на підставі, у межах повноважень та у спосіб, що передбачені Конституцією України та законами України. Після закінчення роботи спеціаліст готує довідку про результати опитування з використанням поліграфа у двох примірниках [94].

Поліграф – різновид спеціального психофізіологічного технічного засобу, який здійснює реєстрацію динаміки протікання не менше п'яти незалежних психофізіологічних процесів людини (грудного і діафрагмального дихання, серцево-судинної активності, електропровідності шкіри, рухової активності) у відповідь на пред'явлення за спеціальною методикою певних психологічних стимулів (запитань, зображень, предметів), не завдаючи шкоди життю, здоров'ю людини та навколишньому середовищу [94].

Склад регіонального вузла ІПРС – належать: 1) *регіональний сервер баз даних*, що складається з основного та резервного серверів баз даних регіонального банку даних, системи керування базами даних, програмного забезпечення, призначених для зберігання та обробки інформаційних ресурсів, системних журналів реєстрації роботи користувачів, програмних та технічних засобів; 2) *регіональний сервер обміну інформацією*, що складається з технологічного сервера, спеціального програмного забезпечення, призначеного для виконання операцій, що забезпечують обмін інформацією (актуалізацію інформаційних ресурсів) між регіональним та центральним вузлами ІПРС; 3) *регіональний програмно-технічний комплекс архівування інформації*, що складається із спеціалізованого сервера, програмного забезпечення та технічно відокремлених пристроїв архівного зберігання інформації, призначених для регламентного архівування (зберігання) інформації, розміщеної на регіональному сервері баз даних, та її аварійного відновлення. Регіональний програмно-технічний комплекс архівування інформації може бути реалізований у складі регіонального сервера баз даних, який додатково обладнується технічними пристроями архівування інформації; 4) *регіональний комутаційний центр*, що призначений для виконання централізованої функції комутації та маршрутизації потоків інформації ІПРС у регіональному сегменті єдиної цифрової телекомунікаційної мережі МВС та локальних обчислювальних мережах; 5) *автоматизоване робоче місце адміністратора регіонального вузла ІПРС*, що є складовою КСЗІ регіонального вузла, призначене для моніторингу системних журналів реєстрації роботи програмних та технічних засобів, аналізу порушень у роботі системи, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів регіонального вузла; 6) *автоматизоване робоче місце адміністратора безпеки*, що є складовою КСЗІ регіонального вузла, призначене для реалізації технології надання доступу користувачам до інформації в ІПРС відповідно до наданих розпорядником ІПРС прав доступу, моніторингу системних журналів реєстрації роботи користувачів та програмних засобів; 7) *автоматизоване робоче місце криптографічного захисту*, що є складовою КСЗІ регіонального вузла системи, призначене для реалізації технології електронного цифрового підпису в ІПРС; 8) *автоматизовані робочі місця*, які забезпечують авторизований доступ користувачів ІПРС до інформаційних ресурсів (баз даних) регіонального вузла ІПРС [86].

Склад територіального вузла ІПРС – входять: 1) автоматизовані робочі місця, які забезпечують авторизований доступ користувачів ІПРС до формування та використання інформаційних ресурсів (баз даних) регіонального вузла ІПРС; 2) територіальний сервер, що складається з технологічного сервера, спеціального програмного забезпечення, призначеного для виконання технологічних операцій, що забезпечують функціонування, відновлення, архівне збереження автоматизованих робочих місць територіального вузла ІПРС. Обмін інформацією між вузлами та доступ користувачів до ІПРС забезпечується засобами ЄЦВТМ МВС тощо [86].

Склад центрального вузла ІПС – належать: 1) *центральный сервер баз даних*, що складається з основного та резервного серверів баз даних центрального банку даних, системи керування базами даних, програмного забезпечення, призначених для зберігання та обробки інформаційних ресурсів, системних журналів реєстрації роботи користувачів, програмних та технічних засобів; 2) *центральный сервер обміну інформацією*, що складається з основного та резервного технологічних серверів, спеціального програмного забезпечення, призначеного для виконання операцій, що забезпечують обмін інформацією (актуалізацію інформаційних ресурсів) між центральним та регіональними вузлами ІПС; 3) *центральный програмно-технічний комплекс архівування інформації*, що складається із спеціалізованого сервера, програмного забезпечення та технічно відокремлених пристроїв архівного зберігання інформації, призначених для регламентного архівування (зберігання) інформації, розміщеної на центральному сервері баз даних, та її аварійного відновлення; 4) *центральный комутаційний центр*, що призначений для виконання централізованої функції комутації та маршрутизації потоків інформації ІПС в єдиній цифровій телекомунікаційній мережі МВС та локальних обчислювальних мережах. Управління центральним комутаційним центром здійснюється визначеним підрозділом Департаменту інформатизації МВС; 5) *автоматизоване робоче місце адміністратора центрального вузла ІПС*, що є складовою КСЗІ центрального вузла, призначене для моніторингу системних журналів реєстрації роботи програмних та технічних засобів, аналізу порушень у роботі системи, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів центрального вузла; 6) *автоматизоване робоче місце адміністратора безпеки*, що є складовою КСЗІ центрального вузла, призначене для реалізації технології надання доступу користувачам до інформації в ІПС відповідно до наданих розпорядником ІПС прав доступу, моніторингу системних журналів реєстрації роботи користувачів та програмних засобів; 7) *автоматизоване робоче місце криптографічного захисту*, що є складовою КСЗІ центрального та регіональних вузлів системи, призначене для реалізації технології електронного цифрового підпису в ІПС; 8) *автоматизовані робочі місця*, які забезпечують авторизований доступ користувачів ІПС до інформаційних ресурсів (баз даних) центрального вузла ІПС [86].

Склад центрального програмно-технічного комплексу системи ІПНП – входять: 1) *центральне сховище даних* – програмно-технічний комплекс, який складається із серверів, систем керування базами даних та іншого програмного забезпечення, призначених для безперервного виконання операцій, записування, зберігання, знищення, приймання та передавання інформації, зберігання системних журналів аудиту роботи користувачів та системних журналів реєстрації роботи програмних засобів; 2) *сервери додатків* – програмно-технічний комплекс, який складається із серверів та програмного забезпечення, призначених для безперервного виконання операцій з інформаційного обміну між складовими системи ІПНП,

функціонування програмних засобів генерації інтерфейсів користувачів для оброблення інформації, записування та зберігання системних журналів аудиту приймання та передавання інформації, реєстрації роботи програмних засобів; 3) *шлюзові сервери* – програмно-технічний комплекс, який складається із серверів, призначених для забезпечення захисту інформації під час здійснення обміну інформацією між підсистемами, взаємодії з інформаційними системами МВС та інших центральних органів виконавчої влади; 4) *автоматизоване робоче місце адміністратора безпеки* – складова комплексної системи захисту інформації в системі ПНП, обладнана технічними засобами та програмним забезпеченням, призначеними для моніторингу системних журналів реєстрації роботи програмних та технічних засобів, аналізу порушень в роботі системи ПНП, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів, визначення повноважень користувачів системи ПНП. Центральний програмно-технічний комплекс системи ПНП розміщується в спеціалізованих службових приміщеннях Національної поліції України [87].

Телекомунікації (електрозв'язок) – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах [10].

Телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням [10].

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [5, 65].

Транспортна мережа передачі даних – це універсальна мережа, що реалізує функції транспортування/комутації та об'єднує окремі мережі доступу із забезпеченням транзиту трафіку між ними високошвидкісними каналами [52].

Транспортна телекомунікаційна мережа – мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу [10].

Трафік – сукупність інформаційних сигналів, що передаються за допомогою технічних засобів операторів, провайдерів телекомунікацій за визначений інтервал часу, включаючи інформаційні дані споживача та/або службу інформацію [10].

ТЕМА IV. ПРОВЕДЕННЯ НАВЧАЛЬНО-ДІЛОВОЇ ГРИ «ЛІНІЯ-102»

Автомобільна система технічних приладів і технічних засобів фото- і кінозйомки, відео-, аудіозапису – технічний комплекс, що встановлюється на службових транспортних засобах НПУ, а саме автомобілях ситуаційних центрів, командно-штабних автомобілях, спеціальному автотранспорті для перевезення затриманих та взятих під варту осіб [79].

АРМ диспетчера ЧЧ Головного управління системи «ЦУНАМІ» – 1) відображає перелік подій, прийнятих оператором «102», які були вчинені в районі обслуговування; 2) в разі визначення телефонного номера заявника відображає накопичені дані по цьому номеру (за якою адресою встановлено, кількість та зміст попередніх звернень); 3) надає можливість зв'язатись з оператором «102», який прийняв виклик; 4) надає можливість зв'язатись з заявником для уточнення даних по події; 5) в разі отримання П.І.Б. заявника, надає всю наявну інформацію про особу з ІПС МВС України; 6) надає повну інформацію на адресу з ІПС МВС України; 7) інформує про повторність надходження інформації про подію; 8) відображає дислокацію та стан роботи патрульних нарядів; 9) забезпечує керування нарядами для реагування на прийняті кримінальні правопорушення та події; 10) відслідковує послідовність реагування на подію з остаточною реєстрацію в «Єдиному обліку».

Група реагування патрульної поліції – наряд патрульної поліції у складі не менше 2 працівників, які в зоні оперативного реагування виконують завдання із забезпечення публічного (громадського) порядку, взаємодії з населенням, безпеки дорожнього руху, попередження правопорушень або подій, оперативного реагування на них [77].

Диспетчер – старший інспектор, інспектор-черговий ЧЧ Головного управління Національної поліції (далі – ГУНП), уповноважений на здійснення керування нарядами поліції за допомогою АРМ «Диспетчер» в інформаційно-телекомунікаційному порталі «ЦУНАМІ» з метою оперативного реагування на заяви та повідомлення про правопорушення та інші події [96].

Диспетчерський центр управління системи «ЦУНАМІ» – 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 ГУНП в м. Києві диспетчерського центру. 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: 1) отримання інформації з служби «102» та відстеження на електронній карті місць учинення кримінальних правопорушень; 2) 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; 3) управління нарядами поліції під час проведення пошукових заходів; 4) здійснення моніторингу відеоінформації з камер відеоспостереження, встановлених у районі його обслуговування; 5) відстеження результатів реагування на заяви та повідомлення громадян про кримінальні правопорушення, прийняті рішення тощо [108].

Зал оперативного управління чергової служби – спеціально визначене приміщення чергової служби, обладнане необхідними засобами зв'язку та оргтехнікою, призначене для здійснення дистанційного управління всіма силами та засобами органу (підрозділу) поліції з метою протидії злочинності, забезпечення публічної безпеки і порядку, охорони прав і свобод людини, а також інтересів суспільства і держави, надання в межах, визначених законодавством України, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги [91].

Зона оперативного реагування наряду поліції – умовний поділ території обслуговування на окремі сектори, які закріплені в системі ПНП за конкретними нарядами поліції. Зони визначаються керівництвом територіальних органів (підрозділів) поліції та затверджуються наказом [77].

Мета застосування працівниками поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису – здійснюється з метою: 1) попередження, виявлення або фіксування правопорушення; 2) охорони громадської безпеки та власності; 3) забезпечення безпеки осіб; 4) забезпечення публічної безпеки і порядку [79].

Мета створення системи «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; 2) *скороченню часу реагування на повідомлення громадян* про кримінальні правопорушення та події, припинення правопорушень та затримання злочинців по «гарячих слідах»; 3) *покращенню контролю за своєчасністю та якістю реагування нарядів поліції* на кримінальні та інші правопорушення, дотриманням законності під час виконання службових обов’язків працівників поліції. Впровадження централізованого управління нарядами патрульної служби поліції (далі – «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 [108].

Обов’язки працівника поліції, пов’язані із застосуванням технічних приладів і технічних засобів фото- і кінозйомки, відеозапису – під час виконання своїх повноважень поліцейським *забороняються*: 1) самовільне видалення відеозаписів з носіїв відеозапису, заміна цих носіїв, зміна їх системної дати та часу; 2) примусове виключення відеореєстраторів, у тому числі на вимогу сторонніх осіб; 3) перешкоджання здійсненню фото- і кінозйомки, відеозапису; 4) використання носіїв відеозапису у випадках, не пов’язаних із здійсненням ними повноважень поліції; 5) копіювання, передання інформації з відповідних носіїв стороннім особам. *За фактами* втрати або пошкодження портативного відеореєстратора чи карти пам’яті, відеореєстраторів, установлених на службових транспортних засобах, безпілотних літальних апаратах складових стаціонарних та автомобільних систем, призначається та проводиться службове розслідування [79].

Оперативне інформування – це єдина система збирання, опрацювання та подання до чергової служби вищого рівня інформації про правопорушення або подію з метою організації контролю за встановленням і затриманням осіб, які вчинили кримінальні правопорушення, а також оперативного реагування на надзвичайні ситуації [77].

Оперативне реагування – скоординовані дії чергової служби, нарядів патрульної поліції, груп реагування патрульної поліції та інших нарядів, спрямовані на організацію невідкладного прибуття працівників поліції до заявника або на вказане місце події з метою припинення правопорушення, установлення особи та затримання ймовірного правопорушника, збереження слідів злочину, надання допомоги потерпілим особам у межах повноважень поліції [77].

Оперативний черговий – головний інспектор-черговий Департаменту організаційно-аналітичного забезпечення та оперативного реагування, старший інспектор-черговий з особливих доручень (старший інспектор – черговий) Управління організаційно-аналітичного забезпечення та оперативного реагування (далі – УОАЗОР), старший інспектор-черговий органу поліції [96].

Оператор служби «102» – посадова особа відділу «102» чергової служби ГУНП, діяльність якої спрямована на прийом телефонного дзвінка та електронного повідомлення заявника в якому міститься інформація про правопорушення та інші події та їх реєстрація за допомогою АРМ «Оператор «102»» в інформаційно-телекомунікаційному порталі «ЦУНАМІ» [96].

Під час приймання та реєстрації заяв та повідомлень про правопорушення або події, організації оперативного реагування на них працівникам підрозділу «102», диспетчерам, старшим зміни працівникам підрозділу «102» та диспетчерам, працівникам чергової служби НПУ забороняється – 1) заходити в систему ППНП не під своїм логіном та паролем; 2) надавати заявникам інформацію про місце проживання працівників поліції, інших правоохоронних органів, суду, абонентські номери їх особистих телефонів; 3) надавати наявну в системі ППНП інформацію стороннім особам, а також посадовим особам правоохоронних органів, яких працівник не може ідентифікувати; 4) без дозволу безпосереднього керівника в робочий час залишати робоче місце та розташування підрозділу [77].

Підрозділ «102» – це відділ «102» УОАЗОР, працівники якого за допомогою АРМ «Оператор «102» системи ІПНП у цілодобовому режимі здійснюють приймання екстрених викликів і реєстрацію повідомлень про правопорушення або події, що надходять телефоном за скороченим номером екстреного виклику поліції «102», а також за допомогою інших видів зв'язку [77].

Портативний відеореєстратор – це пристрій, призначений для запису, зберігання та відтворення відеоінформації, технічні характеристики та особливості конструкції якого дають змогу закріпити його на форменому одязі поліцейського [79].

Прийняття заяв і повідомлень про вчинені кримінальні правопорушення та інші події – дії службових осіб органів поліції при одержанні заяв і повідомлень про вчинені кримінальні правопорушення та інші події [80].

Реєстрація події – фіксація інформації про правопорушення або подію в системі ІПНП та/або журналах з присвоєнням записам порядкових номерів [77].

Сектор реагування патрульної поліції – підрозділ патрульної поліції, який цілодобово забезпечує оперативне реагування на повідомлення про правопорушення або події, у межах компетенції здійснює їх розгляд, а також комплекс превентивних заходів шляхом патрулювання території обслуговування, виявлення та припинення правопорушень, застосування визначених законодавством поліцейських та інших заходів [77].

Система «ЦУНАМІ» – це комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами органів НПУ. Організаційно система складається з двох рівнів: 1. До складу *міського рівня* організаційної структури входять: а) центр прийняття повідомлень – служба «102»; б) центр управління (чергові по місту, диспетчери-оператори системи); в) центр інформаційно-технічного супроводу системи. 2. До складу *районного рівня* організаційної структури входять: а) чергові частини районних управлінь; б) патрульні наряди районного управління, Департаменту патрульної поліції, Поліції охорони тощо; в) слідчо-оперативні групи; г) дільничні офіцери поліції [108].

Центр прийняття повідомлень системи «ЦУНАМІ» – 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 ГУНП України 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: 1) дані про власника телефонного номеру; 2) кількість дзвінків, які раніше були здійснені з цього номеру; 3) відслідковування повторних викликів по вже зареєстрованій події; 4) географічне місцезнаходження абонента на електронній карті міста; 5) попередження про дзвінки абонентів, які внесені до окремого списку: психічно хворі, телефонні хулігани тощо. Оператор здійснює первинну кваліфікацію події, заповнює короткий зміст повідомлення, місце та час скоєння, прикмети злочинця, напрямок його руху. 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» ІПС МВС України, що перешкоджає укриттю кримінальних правопорушень на стадії кваліфікації їх в районних управліннях. Заповнена оператором картка відразу надходить до диспетчера-чергового, відповідального за керування нарядами поліції в тому чи іншому районі столиці. Місце вчинення кримінального правопорушення (місце перебування заявника) відображається на електронній карті м. Києва. 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 [108].

ДОДАТКОВА ІНФОРМАЦІЯ ДО ТЕМИ IV

Відеореєстратор – пристрій, призначений для запису, зберігання та відтворення відеоінформації [79].

Інструкція про порядок запису та збереження в цифровому вигляді заяв і повідомлень, які надходять за телефоном «102», або за допомогою інших засобів зв'язку до Національної поліції України – встановлює порядок організації запису заяв і повідомлень про вчинені кримінальні правопорушення та інші події, які надходять за телефоном «102», або за допомогою інших засобів зв'язку уповноваженими працівниками чергової служби, ситуаційних центрів, центрального органу управління поліції, міжрегіональних територіальних органів НПУ, територіальних органів НПУ в Автономній Республіці Крим та м. Севастополі, областях та м. Києві, їх територіальних (відокремлених) підрозділах, використовується цифровий багатоканальний реєстратор мовленнєвої інформації з вмонтованим автоматичним визначником номерів телефонів та таксофонів [96].

Інформаційна довідка про правопорушення або подію – електронний або паперовий документ визначеної форми, адресований Голові НПУ, начальникам ГУНП та/або територіальних (відокремлених) підрозділів, що містить опис (стислий чи розгорнутий) правопорушення або події [77].

Карта пам'яті або флеш-карта – компактний електронний носій інформації, що використовується для зберігання цифрової інформації [79].

Кінозйомка та відеозапис – процеси фіксації динамічних властивостей об'єктів, подій, явищ за допомогою кіно- або відеокамери. Кінозйомка проводиться на фотоматеріалах, відеозапис – на цифрових носіях інформації [79].

Контроль за використанням технічних приладів і технічних засобів, що мають функцію фото- і кінозйомки, відеозапису – здійснює відповідальна особа; за інформацією, отриманою з їх допомогою, – безпосередньо керівник органу, підрозділу поліції. Дозвіл на копіювання та видачу відеозаписів надається відповідальній особі виключно за рішенням керівника цього органу, підрозділу поліції. Копіювання та видача відеозапису проводяться відповідальною особою на підставі відповідного письмового доручення керівника органу, підрозділу поліції або особи, яка виконує його обов'язки [79].

Обов'язки технічного спеціаліста щодо обслуговування реєстратора мовленнєвої інформації – 1) два рази на добу перевіряти працездатність реєстратора; 2) не допускати прослуховування записів службових розмов особами, які не призначені наказом начальника відповідного підрозділу; 3) вести журнал обліку про виявлені технічні несправності робити запис; 4) обов'язково зберігати записану інформацію протягом 90 діб на основному носії та з'ємних архівних носіях, з цифрових та аналогових реєстраторів – на жорсткому диску реєстратора та з'ємних архівних носіях [96].

Порядок видачі для прослуховування та знищення записаної мовленнєвої інформації на реєстратор – 1) записана інформація може бути надана з дотриманням законодавства України фізичним особам, органам державної влади України та судовим органам; 2) рішення щодо надання або ненадання запису з реєстратора приймає керівник відповідного органу поліції, до якого звертається заявник або надійшов запит; 3) записана інформація видається технічним спеціалістом або посадовою особою, що виконує його обов'язки і допущена до експлуатації реєстратора відповідно до вимог цієї Інструкції. При цьому, у журналі обліку, проставляється дата запису, зазначаються проміжок часу в якому була записана розмова, особа, яка одержала запис, її особистий підпис та дата видачі носіїв запису; 4) записана інформація надається не в оригіналі, а тільки в копії, на окремому носії, причому лише визначений один або кілька фрагментів; 5) основний носій та з'ємний архівний носій не видаються нікому, доступ до них повинен мати тільки відповідальна посадова особа, а також технічні спеціалісти; 6) стирання записів з носіїв (після закінчення 90 діб зберігання або з носіїв, які виробили свій ресурс чи були пошкоджені в процесі експлуатації) проводиться комісією. При цьому, в обліковій документації робиться про це відповідний запис [96].

Порядок обліку та зберігання записаної мовленнєвої інформації на реєстратор – 1) з'ємні архівні носії із записами телефонних розмов та переговорів по радіостанціях чергових працівників чергової служби (ситуаційного центру) органу поліції зберігаються у металевій опечатаній шафі (у місці встановлення реєстратора) протягом 90 діб; 2) з'ємні архівні носії маркуються (нумеруються) та реєструються в журналі обліку, що зберігається в технічного спеціаліста або посадової особи, яка виконує його обов'язки й допущена до експлуатації реєстратора; 3) один раз на рік у встановленому порядку перевіряються: технічний стан реєстратора; зберігання з'ємних архівних носіїв; ведення відповідної документації; результати перевірки доповідаються керівнику органу поліції [96].

Сервер для зберігання відеозаписів – програмно-апаратний комплекс, призначений для зберігання цифрової відеоінформації з усіх видів технічних засобів, що використовуються органами, підрозділами поліції [79].

Слідчо-оперативна група – організаційна форма взаємодії слідчих, працівників оперативних та інших підрозділів поліції, з метою виявлення, фіксації, вилучення та пакування слідів кримінального правопорушення, речових доказів, установлення свідків та потерпілих, з'ясування обставин кримінального правопорушення, що мають значення для всебічного, повного і неупередженого їх дослідження та встановлення осіб, які його вчинили [77].

Службовий документ – офіційно зареєстрований службою діловодства або відповідним чином засвідчений документ, що одержаний чи створений органом чи підрозділом поліції в процесі його діяльності та має відповідні реквізити [76].

Службовий електронний документ – офіційно зареєстрований службою діловодства або відповідним чином засвідчений електронний документ, що одержаний чи створений установою у процесі її діяльності та складається з обов’язкових реквізитів [51].

Станція для заряджання та зберігання відеозаписів портативних відеореєстраторів – програмно-апаратний комплекс, призначений для зберігання фото- і відеозаписів, а також автоматичного заряджання їх акумуляторних батарей [79].

Стаціонарна система технічних приладів і технічних засобів фото- і кінозйомки, відеозапису – технічний комплекс, установлений в органах, підрозділах поліції та призначений для здійснення фото- і кінозйомки, відеозапису з метою забезпечення публічної безпеки та порядку, також може бути використаний у деяких службових приміщеннях органів, підрозділів поліції, у тому числі спеціальних приміщеннях, призначених для утримання затриманих та взятих під варту осіб [79].

Строк зберігання відеозаписів – становить: 1) з портативних та відеореєстраторів, установлених у службових транспортних засобах тощо, – 30 діб; 2) з автомобільної або стаціонарної системи залежно від технічних характеристик – не менше 30 діб; 3) у стаціонарних системах, які використовуються під час відбору кандидатів на службу до поліції, – 60 діб; 4) під час проведення поліцейськими навчальних занять та навчальних зборів зі службової підготовки – встановлюється керівником навчань. Строк зберігання відеозаписів за рішенням керівника органу, підрозділу поліції може бути збільшено у разі використання їх у процесі здійснення оперативно-розшукової діяльності, у рамках розслідування кримінального провадження та/або в провадженнях у справах про адміністративні правопорушення, у разі фіксації надзвичайних подій за участю особового складу поліції, інших подій, якщо вони можуть бути використані в процесі службової діяльності органів, підрозділів поліції, під час проведення службових розслідувань [79].

Технічний спеціаліст – інженер, старший інженер, підрозділу зв’язку ГУНП, уповноважений на здійснення технічного обслуговування реєстратора [96].

Уповноважена особа – посадова особа, яка наділена правом вчиняти дії та відповідає згідно із законодавством за наслідки їх вчинення [51].

Управлінська інформація – сукупність необхідних даних, які сприятимуть вирішенню управлінських рішень [51].

Управлінське рішення – будь-яке завдання, визначне посадовою особою або колегіальним органом в межах повноважень та спрямоване на досягнення поставлених цілей [51].

Фонограма – звукозапис на відповідному носії (магнітній стрічці чи магнітному диску, грамофонній платівці, компакт-диску тощо) виконання або будь-яких звуків, крім звуків у формі запису, що входить до аудіовізуального твору. Фонограма є вихідним матеріалом для виготовлення її примірників (копій) [14].

Фонодокумент – документ, який містить звукову інформацію, зафіксовану будь-якою системою звукозапису [78].

Цифровий багатоканальний реєстратор мовленнєвої інформації з вмонтованим автоматичним визначником номерів телефонів та таксофонів (далі – реєстратор) – запис на реєстратор виконується цілодобово з усіх робочих місць уповноважених працівників чергової служби та ситуаційних центрів органів поліції. Реєстратор встановлюється у відокремленому від чергової служби та ситуаційного центру приміщенні органу (підрозділу) поліції. Підключення реєстратора до мережі електроживлення здійснюється через блок безперебійного живлення на окремий автоматичний пакетний вимикач розподільчого щитка, доступ до якого повинен бути обмеженим. Про початок експлуатації реєстратора видається наказ органу поліції. Цим наказом також призначається уповноважена посадова особа чергової служби, відповідальна за організацію та контроль запису розмов на реєстратор, затверджується список технічних спеціалістів (або посадових осіб, які виконують їх обов'язки), допущених до експлуатації реєстратора, список посадових осіб, яким дозволено видавати записи для прослуховування та перелік робочих місць, канатів (ліній) зв'язку, по яких здійснюється запис повідомлення про вчинені кримінальні правопорушення та інші події. Відповідальність, за безперервне цілодобовий запис телефонних розмов і переговорів за телефоном «102» та радіостанціях, технічне обслуговування, зберігання архівних носіїв записаної інформації покладається на підрозділ зв'язку органу поліції, в якому його встановлено або посадову особу, що виконує обов'язки спеціаліста зв'язку (призначається наказом начальника). Посадова особа чергової служби і технічний спеціаліст або посадова особа, яка виконує, його обов'язки, повинні ознайомитись з інструкцією по експлуатації реєстратора. Для виконання зміни параметрів роботи реєстратора використовуються паролі збіжності: 1) один пароль встановлює технічний спеціаліст або посадова особа, що виконує його обов'язки і допущена до експлуатації реєстратора; 2) другий пароль встановлює уповноважена посадова особа чергової частини, відповідальна за організацію та контроль запису розмов на реєстратор [96].

Чергова служба – чергова частина Департаменту організаційно-аналітичного забезпечення та оперативного реагування НПУ, ЧЧ (ситуаційні відділи) УОАЗОР ГУНП, ЧЧ територіальних підрозділів ГУНП, старші інспектори-чергові (інспектори-чергові) та помічники чергових секторів реагування патрульної поліції територіальних підрозділів ГУНП, які забезпечують безперервне та цілодобове виконання своїх завдань [91].

СЛОВНИК

найбільш поширених загальних термінів

Абонент – споживач телекомунікаційних послуг, який отримує телекомунікаційні послуги на умовах договору, котрий передбачає підключення кінцевого обладнання, що перебуває в його власності або користуванні, до телекомунікаційної мережі [10].

Абонентський номер – сукупність цифрових знаків для позначення кінцевого обладнання абонента в телекомунікаційній мережі [10].

Автор електронного документа – фізична або юридична особа, яка створила електронний документ [26].

Адвокат – фізична особа, яка здійснює адвокатську діяльність на підставах та в порядку, що передбачені цим Законом [16].

Адреса мережі Інтернет – визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символічний ідентифікатор доменних імен в ієрархічній системі доменних назв [10].

Адресат – фізична або юридична особа, якій адресується електронний документ [26].

Адресний простір мережі Інтернет – сукупність адрес мережі Інтернет [10].

Аналітично-синтетична обробка науково-технічної інформації – це процес обробки інформації шляхом аналізу і синтезу змісту документів з метою одержання необхідних відомостей, а також шляхом їх класифікації, оцінки, співставлення і узагальнення [32].

Архівна копія – офіційний документ архіву, що відтворює текст архівного документа або зображення архівного графічного документа із зазначенням їх адреси (справа, том, місце знаходження документа) [78].

Архівна справа – галузь життєдіяльності суспільства, що охоплює наукові, організаційні, правові, технологічні, економічні та інші питання діяльності юридичних і фізичних осіб, пов'язані із нагромадженням, обліком, зберіганням архівних документів та використанням відомостей, що в них містяться [34]. *Або: архівна справа* – галузь діяльності, що охоплює питання організації зберігання і використання архівних документів [78].

Архівна установа, архів, архівний підрозділ, архівний відділ – це відповідно установа чи структурний підрозділ, що забезпечує облік і зберігання архівних документів, використання відомостей, що в них містяться, та формування Національного архівного фонду і/або здійснює управління, науково-дослідну та інформаційну діяльність у сфері архівної справи і діловодства [34].

Архівний витяг – архівна копія, що відтворює частину тексту архівного письмового документа, завірена заведеним порядком [78].

Архівний документ – документ незалежно від його виду, виду матеріального носія інформації, місця, часу створення і місця зберігання та форми власності на нього, що припинив виконувати функції, для яких був створений, але зберігається або підлягає зберіганню з огляду на значущість для особи, суспільства чи держави або цінність для власника також як об'єкт рухомого майна [34].

Аудіовізуальна інформація – будь-які сигнали, що сприймаються зоровими і слуховими рецепторами людини та ідентифікуються як повідомлення про події, факти, явища, процеси, відомості про осіб, а також коментарі про них, що передаються за допомогою зображень та звуків [42].

Аудіовізуальний (електронний) засіб масової інформації – організація, яка надає для масового приймання споживачами аудіовізуальну інформацію, передану у вигляді електричних сигналів і прийняту за допомогою побутових електронних пристроїв [42].

Аудіовізуальний документ – документ, що містить зображувальну і звукову інформацію [78].

Аудіовізуальний твір – твір, що фіксується на певному матеріальному носії (кіноплівці, магнітній плівці чи магнітному диску, компакт-диску тощо) у вигляді серії послідовних кадрів (зображень) чи аналогових або дискретних сигналів, які відображають (закодовують) рухомі зображення (як із звуковим супроводом, так і без нього), і сприйняття якого є можливим виключно за допомогою того чи іншого виду екрана (кіноекрана, телевізійного екрана тощо), на якому рухомі зображення візуально відображаються за допомогою певних технічних засобів. *Видами* аудіовізуального твору є кінофільми, телефільми, відеофільми, діафільми, слайдофільми тощо, які можуть бути ігровими, анімаційними (мультиплікаційними), неігровими чи іншими [14]. *Або: аудіовізуальний твір* – частина телерадіопрограми, яка є об'єктом авторського права, має певну тривалість, авторську назву і власну концепцію, складається з епізодів або цілісних авторських творів, поєднаних між собою творчим задумом і зображувальними чи звуковими засобами та яка є результатом спільної діяльності авторів, виконавців та виробників [42].

Безпроводовий доступ до телекомунікаційної мережі (безпроводовий доступ) – електрозв'язок з використанням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися із збереженням унікального ідентифікаційного номера в межах пунктів закінчення телекомунікаційної мережі, які під'єднані до одного комутаційного центру [10].

Бібліотека-депозитарій – бібліотека, яка забезпечує постійне зберігання бібліотечного фонду, сформованого з документів, що рідко використовуються і мають наукову та/або художню цінність [18].

Бібліотечна система України – розгалужена мережа бібліотек різних видів, пов’язаних взаємодією і взаємовикористанням бібліотечних ресурсів [18].

Біометричні дані – дактилокартки, зразки ДНК [8].

Бланк документа – стандартний аркуш паперу з частково надрукованим текстом постійної інформації і місцем для змінної інформації документа [78].

Бланк електронного документа – уніфікована форма електронного документа установи або її структурного підрозділу з відповідними реквізитами та полями постійної і змінної інформації [51].

Бланк службового документа – уніфікована форма службового документа з надрукованою постійною інформацією і наявним місцем для фіксування змінної інформації [76].

Блокування інформації в системі – це дії, внаслідок яких унеможливується доступ до інформації в системі [5].

Веб-клієнт – програмний комплекс, що інтегрується до програмного забезпечення державного електронного інформаційного ресурсу отримувача та забезпечує формування і передавання запитів та отримання відповідей за допомогою шлюзів безпечного обміну [57].

Веб-сайт – сукупність даних, електронної (цифрової) інформації, інших об’єктів авторського права і (або) суміжних прав тощо, пов’язаних між собою і структурованих у межах адреси веб-сайту і (або) облікового запису власника цього веб-сайту, доступ до яких здійснюється через адресу мережі Інтернет, що може складатися з доменного імені, записів про каталоги або виклики і (або) числової адреси за Інтернет-протоколом [14]. *Або: веб-сайт* – 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 [25].

Веб-сервіс – програмний комплекс, що інтегрується до програмного забезпечення державного електронного інформаційного ресурсу постачальника і забезпечує отримання запитів та формування і передавання відповідей за допомогою шлюзів безпечного обміну [57].

Веб-сторінка – складова частина веб-сайту, що може містити дані, електронну (цифрову) інформацію, інші об’єкти авторського права і (або) суміжних прав тощо [14].

Види документів, віднесених до обов’язкового примірника – видання текстові, нотні, картографічні, образотворчі; видання електронні; видання, аудіопродукція та інші документи для сліпих; аудіо-, візуальна, аудіовізуальна продукція (кіно-, відео-, фото-, фонодокументи); нормативно-правові акти у сфері стандартизації, метрології та сертифікації; патентні документи [37].

Види інформації за змістом: 1) інформація про фізичну особу (ст. 11); 2) інформація довідково-енциклопедичного характеру (ст. 12); 3) інформація про стан довкілля (екологічна інформація) (ст. 13); 4) інформація про товар (роботу, послугу) (ст. 14); 5) науково-технічна інформація (ст. 15); 6) податкова інформація (ст. 16); 7) правова інформація (ст. 17); 8) статистична інформація (ст. 18); 9) соціологічна інформація (ст. 19); 10) інші види інформації [2, 30].

Використання інформації – це задоволення інформаційних потреб громадян, юридичних осіб і держави [30].

Вимоги до захисту в системі інформації від несанкціонованого блокування – визначаються розпорядником інформації, якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством [69].

Вимоги до оформлення документа на персональному комп'ютері – документи, як правило, набирають і роздруковують у текстовому редакторі Word (*шрифт Times New Roman*) з такими параметрами: формат аркуша – *A4*; розмір шрифту основного тексту – *14 кель*; абзацний відступ – *1,25 см*; міжрядковий інтервал – *одинарний*; вирівнювання тексту – *по ширині*. Опцію “Автоматична розстановка переносів” *не використовують*. Бланки документів повинні мати такі береги: лівий – *30 мм*, верхній та нижній – *20 мм*, правий – *10 мм*. Документи повинні мати такі обов'язкові реквізити: назву організації, назву виду документа, дату, реєстраційний індекс документа, заголовок до тексту документа, текст документа, відмітку про наявність додатків, підпис, гриф погодження документа, візи документа та відбиток печатки органу внутрішніх справ. Реквізити документа відокремлюються один від одного через *1,5–3 міжрядкових інтервали*. Максимальна довжина рядка багаторядкових реквізитів (крім реквізиту “Текст”) дорівнює *73 мм (28 друкованих знаків)*. Вимоги та особливості оформлення документів, що містять службову інформацію, державну таємницю та/або мають гриф обмеження доступу, визначаються відповідними НПА. *Відповідальність* за зміст, рівень підготовки та належне оформлення документів, що розробляються в системі МВС, покладається на особу, яка підготувала документ [78].

Вимоги та порядок створення системи захисту – встановлюються *Адміністрацією Держспецв'язку*. Вимоги до захисту інформації кожної окремої системи встановлюються *технічним завданням* на створення системи або системи захисту. У складі системи захисту повинні використовуватися *засоби захисту інформації з підтвердженою відповідністю*. У разі використання засобів захисту інформації, які не мають підтвердження відповідності на момент проектування системи захисту, відповідне оцінювання проводиться під час державної експертизи системи захисту. Порядок проведення державної експертизи системи захисту, державної експертизи та сертифікації засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією [69].

Висновок – документ, що містить думку, висновок установи, комісії, спеціаліста щодо якогось документа чи питання [78].

Виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї [5].

Витяг – засвідчена копія частини тексту електронного документа, який містить певний обсяг інформації або запису реєстру [51].

Витяг з документа – засвідчена копія частини тексту службового документа [76]. *Або: витяг із документа* – копія документа, що відтворює його частину, засвідчену заведеним порядком [78].

Вихідний документ – документ, відправлений із організації [78].

Відеограма – відеозапис на відповідному матеріальному носії (магнітній стрічці, магнітному диску, компакт-диску тощо) виконання або будь-яких рухомих зображень (із звуковим супроводом чи без нього), крім зображень у вигляді запису, що входить до аудіовізуального твору. Відеограма є вихідним матеріалом для виготовлення її копій [14].

Віднесення інформації до державної таємниці – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього [3].

Відносини між власниками систем – власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються *договором*, який укладається між власниками систем, якщо інше не встановлено законодавством. Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі [5].

Відносини між власником системи та користувачем – власник системи надає користувачеві відомості *про правила і режим роботи* системи та забезпечує йому *доступ* до інформації в системі відповідно до визначеного порядку доступу [5].

Відносини між володільцем інформації та власником системи – власник системи забезпечує *захист інформації* в системі в порядку та на умовах, визначених у *договорі*, який укладається ним із володільцем інформації, якщо інше не передбачено законом. Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі [5].

Відомість – перелік даних (відомостей), розташованих у певному порядку (платіжна відомість тощо) [78].

Відомчий акт – письмовий документ нормативного або індивідуального характеру, що видають міністерства, інші центральні органи державної виконавчої влади в межах своєї компетенції [78].

Відповідальність за порушення законодавства про доступ до публічної інформації несуть особи, винні у вчиненні таких порушень: 1) ненадання відповіді на запит; 2) ненадання інформації на запит; 3) безпідставна відмова у задоволенні запиту на інформацію; 4) неоприлюднення інформації відповідно до статті 15 цього Закону; 5) надання або оприлюднення недостовірної, неточної або неповної інформації; 6) несвочасне надання інформації; 7) необґрунтоване віднесення інформації до інформації з обмеженим доступом; 8) нездійснення реєстрації документів; 9) навмисне приховування або знищення інформації чи документів [4].

Відповідальність за порушення законодавства про захист інформації в системах – особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом [5].

Відповідь на запит щодо отримання інформації державного електронного інформаційного ресурсу – електронне повідомлення, автоматично сформоване веб-сервісом постачальника та передане отримувачу за допомогою шлюзів безпечного обміну через веб-клієнт, що містить дані відповідного державного електронного інформаційного ресурсу або дані про їх відсутність [57].

Відтворення – виготовлення одного або більше примірників твору, відеограми, фонограми в будь-якій матеріальній формі, а також їх запис для тимчасового чи постійного зберігання в електронній (у тому числі цифровій), оптичній або іншій формі, яку може зчитувати комп'ютер [14].

Візуалізація – процес відтворення даних у формі, що є сприйнятною людиною [51].

Візування проекту електронного документа (візування) – накладання посадовою особою електронного цифрового підпису на проект електронного документа для засвідчення факту погодження цієї особою завізованого проекту документа [51].

Вказівка – правовий акт, що видає орган державного управління, переважно з питань інформаційно-методичного характеру, а також із питань, пов'язаних із організацією виконання наказів, інструкцій, інших актів цього та вищих органів управління [78].

Власник веб-сайту – особа, яка є володільцем облікового запису та встановлює порядок і умови використання веб-сайту. За відсутності доказів іншого власником веб-сайту вважається реєстрант відповідного доменного імені, за яким здійснюється доступ до веб-сайту, і (або) отримувач послуг хостингу [14].

Власник веб-сторінки – особа, яка є володільцем облікового запису, що використовується для розміщення веб-сторінки на веб-сайті, та яка управляє і (або) розміщує електронну (цифрову) інформацію в межах такої веб-сторінки. Власник веб-сайту не є власником веб-сторінки, якщо останній володіє обліковим записом, що дозволяє йому самостійно, незалежно від власника веб-сайту, розміщувати інформацію на веб-сторінці та управляти нею [14].

Власник ресурсів – фізична або юридична особа, яка має право власності на ресурси [59].

Власник системи – фізична або юридична особа, якій належить право власності на систему [5].

Властивості інформації – 1) достовірність; 2) своєчасність; 3) повнота; 4) зрозумілість; 5) об'єктивність; 6) актуальність; 7) корисність; 8) об'ємність; 9) конфіденційність; 10) цілісність; 11) доступність; 12) захищеність; 13) якість та ін. [108].

Внутрішній документ – документ, створений у межах організації, установи і призначений для виконання цієї організації або установою [78].

Володільць інформації – фізична або юридична особа, якій належать права на інформацію [5].

Вхідний документ – документ, що надійшов до організації [78].

Гарантії права на інформацію забезпечується: 1) створенням механізму реалізації права на інформацію; 2) створенням можливостей для вільного доступу до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів; 3) обов'язком суб'єктів владних повноважень інформувати громадськість та засоби масової інформації про свою діяльність і прийняті рішення; 4) обов'язком суб'єктів владних повноважень визначити спеціальні підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації; 5) здійсненням державного і громадського контролю за додержанням законодавства про інформацію; 6) встановленням відповідальності за порушення законодавства про інформацію. Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [2].

Геоінформаційні системи – сучасні комп'ютерні технології, що дають можливість поєднати модельне зображення території (електронне відображення карт, схем, космо-, аерозображень земної поверхні) з інформацією табличного типу (різноманітні статистичні дані, списки, економічні показники тощо) [9].

Гіперпосилання – формалізований відповідно до стандартів мережі Інтернет запис адреси веб-сайту або його частини (веб-сторінки, даних). У разі якщо гіперпосилання адресує до частини веб-сайту (веб-сторінки), то, крім домену і (або) числової адреси за Інтернет-протоколом, воно може містити додаткові записи про каталоги або виклики і умови доступу до веб-сторінки, що може бути відтворена або збережена на пристроях, які можуть читувати та відтворювати електронну (цифрову) інформацію з використанням мережі Інтернет [14].

Голосова телефонія – обмін інформацією голосом у реальному часі з використанням телекомунікаційних мереж [10].

Графік – 1) графічний або текстовий документ, що відображає стан або динаміку будь-якого явища; 2) план роботи з точними показниками норм і часу виконання (наприклад, графік відпусток) [78].

Гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації [3]. *Або: гриф секретності* – штамп установленого зразка, обов'язковий реквізит кожного матеріального носія інформації, віднесеної до державної таємниці [78].

Дата документа – обов'язковий реквізит документа, що вказує на час підписання, затвердження чи узгодження документа і має три складники: день, місяць, рік [78]. *Або: дата документа* – це дата його підписання, затвердження, прийняття, реєстрації. Дата оформляється цифровим або словесно-цифровим способом. У разі оформлення дати цифровим способом число і місяць проставляються двома парами цифр, розділеними крапкою; рік – чотирма цифрами, крапка в кінці не ставиться. Елементи дати зображують арабськими цифрами в один рядок у послідовності: день, місяць, рік (08.03.2019). У текстах нормативно-правових актів та посиланнях на них і документах, що містять відомості фінансового характеру, застосовується словесно-цифровий спосіб зазначення дати з проставлянням нуля в позначенні дня місяця, якщо він містить одну цифру, наприклад: 08 березня 2019 року. Дозволяється вживати слово “рік” у скороченому варіанті “р.”, наприклад: 08 березня 2019 р. [78].

Депонування – форма збирання і розповсюдження рукописних робіт, переважно наукових [18].

Депонування документів – установлений порядок зберігання документів у довідково-інформаційному фонді [78].

Державна архівна установа – архівна установа, що здійснює свою діяльність за рахунок коштів Державного бюджету України [34].

Державна підтримка засобів масової інформації – сукупність правових, економічних, соціальних, організаційних та інших заходів державного сприяння зміцненню і розвитку інформаційної галузі, її інфраструктури [21].

Державна статистика – централізована система збирання, опрацювання, аналізу, поширення, збереження, захисту та використання статистичної інформації [22].

Державна статистична діяльність – сукупність дій, пов'язаних з проведенням державних статистичних спостережень та наданням інформаційних послуг, спрямована на збирання, опрацювання, аналіз, поширення, збереження, захист та використання статистичної інформації, забезпечення її достовірності, удосконалення статистичної методології [22].

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою [3].

Державне зберігання документів – постійне зберігання архівних документів, що здійснюють державні архіви, а також деякі інші організації відповідно до своєї компетенції [78].

Державний експерт з питань таємниць – посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування [3].

Державний засіб масової інформації: а) державна теле- і радіомовна організація; б) державне інформаційне агентство [21].

Державний реєстр банків – реєстр, що ведеться Національним банком України і містить відомості про державну реєстрацію усіх банків [17].

Державні ресурси – ресурси, які є об'єктом права державної власності [59].

Дійсний документ – документ, відомості про час і місце створення якого або про автора, які містяться в самому документі чи виявлені будь-яким шляхом, відповідають дійсності; непідробний, нефальшований [78].

Діловий лист – документ, що застосовують для зв'язку, передачі інформації на відстані між двома кореспондентами, якими можуть бути як юридичні, так і фізичні особи [78].

Діловодство – діяльність, що охоплює сукупність робіт із документування установи й організацію роботи з документами [78]. *Або: діловодство* – сукупність процесів, що забезпечують документування управлінської інформації та організацію роботи зі службовими документами [34, 76].

Діяльність інформаційних агентств – це збирання, обробка, творення, зберігання, підготовка інформації до поширення, випуск та розповсюдження інформаційної продукції [29].

Для оброблення, передавання, зберігання службової, таємної інформації, персональних даних, а також інформації єдиних та державних електронних реєстрів використовуються – комп’ютерні програми (їх оновлення), в яких немає недокументованих функцій, що підтверджується результатами державної експертизи у сфері захисту інформації, яка досліджує вихідні коди та відповідні виконувани модулі програм і компонентів, перевіряється достовірність і повнота (цілісність), ідентифікується джерело походження (авторство), з фіксуванням стану комп’ютерних програм чи їх оновлень на момент проведення перевірки. Під час вибору комп’ютерних програм, які пройшли державну експертизу у сфері захисту інформації, органи виконавчої влади віддають перевагу (за інших однакових об’єктивних технічних та якісних характеристик) комп’ютерним програмам (далі – КП), у яких реалізовано вищий рівень гарантій коректності надання функціональних послуг безпеки [67].

До інформації з обмеженим доступом не можуть бути віднесені такі відомості: 1) про стан довкілля, якість харчових продуктів і предметів побуту; 2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей; 3) про стан здоров’я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення; 4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов’язаних з політичними репресіями, Голодомором 1932-1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів; 5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб; 6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов’язковість яких надана Верховною Радою України [2].

Довгий (словесний) формат дати – це: дев’ятнадцяте листопада дві тисячі сімнадцятого року (наприклад: договір, заповіт) [108].

Довгий (словесно-цифровий) формат дати – це: 19 листопада 2017 р. або 19 листопада 2017 року (наприклад: нормативно-правові та фінансові документи) [108].

Довідка – 1) документ, що передає одна організація, установа іншій і підтверджує факти біографічного чи службового характеру; 2) документ, що містить опис (стилий чи розгорнутий) і підтвердження тих чи інших фактів і подій [78]. *Або: довідка* – документ, який містить відомості про притягнення до кримінальної відповідальності, відсутність (наявність) судимості або обмежень, передбачених кримінально-процесуальним законодавством України [108].

Дозвіл – документ, що надає право на виконання робіт з технічного захисту інформації для власних потреб [50].

Документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі [2]. *Або: документ* – матеріальна форма одержання, зберігання, використання і поширення інформації, зафіксованої на папері, магнітній, кіно-, фотоплівці, оптичному диску або іншому носіїві [18, 37]. *Або: документ* – засіб закріплення різними способами на спеціальному матеріалі інформації про факти, події, явища об'єктивної дійсності і розумової діяльності людини; таку інформацію розташовують за наперед визначеною схемою, обов'язковою для всіх укладачів [78].

Документ вторинний – документ, підготовлений у ході інформаційного аналізу на підставі вивчення і перероблення первинного документа (анотація, реферат тощо) [78].

Документаційний (документальний) фонд – сукупність службових документів, що нагромадились або зібрані в процесі діяльності органу чи підрозділу поліції, склад і процес формування якого визначають його нормативні документи [76].

Документообіг – комплекс робіт із документами, укладеними чи отриманими установою або організацією: прийняття, розподіл, реєстрація, контроль за виконанням, формування справ, зберігання й використання документації, рух документованої інформації між інстанціями [78]. *Або: документообіг* – рух службових документів з моменту їх створення або одержання до завершення виконання або відправлення [76].

Документування – сукупність процесів для утворення всіх видів документації, що відображають діяльність установи, організації або підприємства [78].

Домен – частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється [10].

Домен другого рівня – частина адресного простору мережі Інтернет, що розташовується на другому рівні ієрархії імен у цій мережі [10].

Домен.UA – домен верхнього рівня ієрархічного адресного простору мережі Інтернет, створений на основі кодування назв країн відповідно до міжнародних стандартів, для обслуговування адресного простору українського сегмента мережі Інтернет [10].

Доповідна записка – документ, адресований керівникові установи, що інформує керівника про якийсь не відомий йому факт, подію тощо (у зв'язку з означеним можливі і деякі пропозиції) [78].

Доповідь – документ, у якому викладено суть, висновки, пропозиції щодо конкретної теми (довідь призначено для усного викладу й обговорення) [78].

Допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації [3].

Доручення – документ, що уповноважує його пред'явника виконувати визначені дії від імені довірителя [78].

Доступ до державної таємниці – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень [3].

Доступ до інформації – за порядком доступу інформація поділяється на *відкриту* інформацію та інформацію з *обмеженим доступом*. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом [2].

Доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі [5].

Доступ до інформації забезпечується шляхом – 1) систематичного та оперативного оприлюднення інформації: в офіційних друкованих виданнях; на офіційних веб-сайтах в мережі Інтернет; на єдиному державному веб-порталі відкритих даних; на інформаційних стендах; будь-яким іншим способом; 2) надання інформації за запитами на інформацію [4].

Доступ до інформації про особу – кожна особа *має право*: 1) знати у період збирання інформації, але до початку її використання, які відомості про неї та з якою метою збираються, як, ким і з якою метою вони використовуються, передаються чи поширюються, крім випадків, встановлених законом; 2) доступу до інформації про неї, яка збирається та зберігається; 3) вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання якої здійснюється з порушенням вимог закону; 4) на ознайомлення за рішенням суду з інформацією про інших осіб, якщо це необхідно для реалізації та захисту прав та законних інтересів; 5) на відшкодування шкоди у разі розкриття інформації про цю особу з порушенням вимог, визначених законом. Обсяг інформації про особу, що збирається, зберігається і використовується розпорядниками інформації, має бути *максимально обмеженим* і використовуватися лише з метою та у спосіб, визначений законом. Зберігання інформації про особу *не повинно тривати довше*, ніж це необхідно для досягнення мети, задля якої ця інформація збиралася. Відмова особі в доступі до інформації про неї, приховування, незаконне збирання, використання, зберігання чи поширення інформації можуть бути *оскаржені* [4].

Доступність – властивість інформації бути захищеною від несанкціонованого блокування [50].

Досудове розслідування – стадія кримінального провадження, яка починається з моменту внесення відомостей про кримінальне правопорушення до ЄРДР і закінчується закриттям кримінального провадження або направленням до суду обвинувального акту, клопотання про застосування примусових заходів медичного або виховного характеру, клопотання про звільнення особи від кримінальної відповідальності [13].

Досудове слідство – форма досудового розслідування, в якій здійснюється розслідування злочинів [13].

Досьє – 1) сукупність документів, матеріалів, що стосуються певного питання, справи, особи; 2) тека, в якій містяться матеріали, що стосуються певного питання, справи, особи [78].

Друковані засоби масової інформації (преса) в Україні – розуміються періодичні і такі, що продовжуються, видання, які виходять під постійною назвою, з періодичністю один і більше номерів (випусків) протягом року на підставі свідоцтва про державну реєстрацію [24].

Дублікат – примірник документа, укладений і виданий замість втраченого оригіналу, який має однакову юридичну силу з оригіналом і обов'язкову позначку “ДУБЛІКАТ” [78].

Електронна (цифрова) інформація – аудіовізуальні твори, музичні твори (з текстом або без тексту), комп'ютерні програми, фонограми, відеограми, програми (передачі) організацій мовлення, що знаходяться в електронній (цифровій) формі, придатній для зчитування і відтворення комп'ютером, які можуть існувати і (або) зберігатися у вигляді одного або декількох файлів (частин файлів), записів у базі даних на зберігаючих пристроях комп'ютерів, серверів тощо у мережі Інтернет, а також програми (передачі) організацій мовлення, що ретранслюються з використанням мережі Інтернет [14].

Електронна ідентифікація – процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи [25].

Електронна копія електронного документа – візуальне подання електронного документа в електронній формі без електронних цифрових підписів, якими його було завізовано та/або підписано, відповідність та правовий статус якої засвідчено електронною печаткою [51].

Електронна копія оригіналу паперового документа (фотокопія) – візуальне подання паперового документа в електронній формі, отримане шляхом сканування (фотографування) паперового документа, відповідність оригіналу та правовий статус якого засвідчено електронною печаткою установи [51].

Електронна печатка – електронні дані, які додаються створювачем електронної печатки до інших електронних даних або логічно з ними пов'язуються і використовуються для визначення походження та перевірки цілісності пов'язаних електронних даних [25].

Електронна послуга – будь-яка послуга, що надається через інформаційно-телекомунікаційну систему [25].

Електронна резолюція – накладена посадовою особою на електронний документ вказівка керівника виконавцю, яка зазначає стислий зміст прийнятого нею рішення щодо організації виконання електронного документа, на яку накладено ЕЦП зазначеної особи. Електронна резолюція є єдиною допустимою формою реалізації доручень, виданих у електронній формі [51].

Електронна справа – електронна папка з електронними документами, з яких сформовано цю справу, та електронним внутрішнім описом, що включені до справи [51].

Електронне повідомлення – автоматично або у разі необхідності автоматизовано створена та передана в електронній формі інформація про доставку/ отримання/ відмову в реєстрації/ реєстрацію електронного документа адресатом та інше [51].

Електронне повідомлення – інформація, надана споживачу через телекомунікаційні мережі, яка може бути у будь-який спосіб відтворена або збережена споживачем в електронному вигляді [28].

Електронне урядування – форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян [55].

Електронний аудіовізуальний документ – електронний документ, зміст якого представлено у вигляді відеоряду, зображення і/або запису звуку, для фіксування і/або відтворення яких застосовують відповідну апаратуру, на який накладено електронний цифровий підпис [51].

Електронний внутрішній опис документів справи – окремий обліковий електронний документ, що містить перелік заголовків до текстів електронних документів справи із зазначенням порядкових номерів, їх реєстраційних індексів, дат та найменування файлів відповідних електронних документів [51].

Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [2, 26, 76]. *Або: електронний документ* – документ, інформацію в якому подано в електронній формі, що включає необхідні реквізити, у тому числі ЕЦП. Формат і структура даних електронного документа, його обов'язкові реквізити, а також візуальна форма його подання визначаються законодавством [78].

Або: електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. *Візуальною формою* подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною. Для ідентифікації автора електронного документа може використовуватися *електронний підпис*. Накладанням електронного підпису завершується створення електронного документа. Юридична сила електронного документа *не може бути заперечена* виключно через те, що він має електронну форму. Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму. Перевірка цілісності електронного документа проводиться шляхом перевірки електронного цифрового підпису [26].

Електронний документообіг (обіг електронних документів) – одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів [2, 26]. *Або: електронний документообіг (обіг електронних документів)* – сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів. В інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах, які забезпечують обмін електронними документами, що містять державні інформаційні ресурси, або інформацію з обмеженим доступом, повинен забезпечуватися захист цієї інформації відповідно до законодавства [26, 76].

Електронний документообіг установи – обіг службових електронних документів з моменту їх створення або одержання до завершення виконання, відправлення, знищення або передавання до архіву [51].

Електронний журнал – окремий реєстр системи електронного документообігу установи, що містить записи про зареєстровані документи, об'єднані за певною ознакою або групою ознак [51].

Електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис [25].

Електронний підручник (посібник) – електронне навчальне видання із систематизованим викладом навчального матеріалу, що відповідає освітній програмі, містить цифрові об'єкти різних форматів та забезпечує інтерактивну взаємодію [39].

ЕОТ – електронна обчислювальна техніка [76].

Етапи функціонування ІПС – 1) збір та зберігання інформації; 2) пошук та видача інформації користувачу [108].

ЄДРПОУ – Єдиний державний реєстр підприємств та організацій України (введення до ЄДРПОУ здійснює Державний комітет статистики України) [78].

Журнал – документ, що укладається за певною формою і містить систематичні записи відомостей, подій, операцій, рішень тощо [78].

За порядком доступу інформація поділяється – на: 1) відкриту інформацію; 2) інформацію з обмеженим доступом [2].

Забезпечення захисту інформації в системі – відповідальність за забезпечення захисту інформації в системі покладається на *власника системи*. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює *службу захисту інформації* або призначає *осіб*, на яких покладається забезпечення захисту інформації та контролю за ним. Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи *повідомляє* відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган [5].

Забезпечення інформаційної безпеки національних ресурсів – здійснюється їх *власниками* шляхом створення комплексної системи захисту інформації щодо запобігання несанкціонованому доступу та дотримання належного рівня захисту національних ресурсів [59].

Завдання ОРД – є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави [38].

Запис – процес фіксування інформації в документі або будь-якому запам'ятовуючому пристрої [78].

Запис (звукозапис, відеозапис) – фіксація за допомогою спеціальних технічних засобів (у тому числі й за допомогою числового представлення) на відповідному матеріальному носії звуків і (або) рухомих зображень, яка дозволяє здійснювати їх сприйняття, відтворення або сповіщення за допомогою відповідного пристрою [14].

Записка – стислий виклад питання або пояснення змісту документа, факту, події (наприклад, службова записка, доповідна записка, пояснювальна записка тощо) [78].

Запит щодо отримання інформації державного електронного інформаційного ресурсу – електронне повідомлення, сформоване веб-клієнтом отримувача та передане постачальнику за допомогою шлюзів безпечного обміну через веб-сервіс з метою отримання даних відповідного державного електронного інформаційного ресурсу [57].

Засекречування матеріальних носіїв інформації – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації [3].

Засіб електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які використовуються для створення та/або перевірки електронного підпису чи печатки [25].

Засіб електронної ідентифікації – носій інформації, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг [25].

Засоби дистанційного зв'язку – телекомунікаційні мережі, поштовий зв'язок, телебачення, інформаційні мережі, зокрема Інтернет, які можуть використовуватися для укладення договорів на відстані [28].

Засоби інформатизації – електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв'язку, що використовуються для реалізації інформаційних технологій [9].

Засоби комунікації – засоби розповсюдження продукції інформаційних агентств, такі як: друковані та екранні видання, радіо, телебачення (кабельне, супутникове, глобальне), електричний та електронний зв'язок (телеграф, телефон, телекс, телефакс), комп'ютерні мережі та інші телекомунікації [29].

Засоби масової інформації – засоби, призначені для публічного поширення друкованої або аудіовізуальної інформації [2].

Захист відкритої інформації – відкрита інформація під час обробки в системі повинна зберігати *цілісність*, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до *ознайомлення* з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише *ідентифіковані та автентифіковані користувачі*, яким надано відповідні повноваження. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні *блокуватися* [69].

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [2].

Захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [5].

Захист особи, яка оприлюднює інформацію – посадові та службові особи не підлягають юридичній відповідальності, незважаючи на порушення своїх обов'язків, за розголошення інформації про правопорушення або відомостей, що стосуються серйозної загрози здоров'ю чи безпеці громадян, довкіллю, якщо особа при цьому керувалася добрими намірами та мала обґрунтоване переконання, що інформація є достовірною, а також містить докази правопорушення або стосується істотної загрози здоров'ю чи безпеці громадян, довкіллю [4].

Захист службової і таємної інформації – під час обробки службової і таємної інформації повинен забезпечуватися її захист від *несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення*. Доступ до службової інформації надається *тільки ідентифікованим та автентифікованим* користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні *блокуватися*. Забезпечення захисту в системі таємної інформації, яка не становить державну таємницю, та конфіденційної інформації здійснюється згідно з вимогами до захисту службової інформації, якщо інше не передбачено законом [69].

Захисту в системі підлягає – 1) відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами); 2) конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації» [4]; 3) службова інформація; 4) інформація, яка становить державну або іншу передбачену законом таємницю; 5) інформація, вимога щодо захисту якої встановлена законом [69].

Захищений носій особистих ключів – засіб кваліфікованого електронного підпису чи печатки, що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на ньому даних від несанкціонованого доступу, безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання [66].

Заява – документ, що містить прохання або пропозицію особи (осіб) до установи чи посадової особи (наприклад, заява про прийняття на роботу, про надання відпустки тощо) [78].

Зберігання інформації – це забезпечення належного стану інформації та її матеріальних носіїв [30].

Зведення – документ, що є узагальненням відомостей із одного питання (наприклад, зведення пропозицій, зауважень, вимог тощо) і укладається на вимогу вищих органів або посадової особи [78].

Звернення громадян – слід розуміти викладені в письмовій або усній формі пропозиції (зауваження), заяви (клопотання) і скарги [7].

Звід відомостей, що становлять державну таємницю – акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених цим Законом сферах [3].

Звіт – документ, що містить відомості про виконану роботу (план, завдання, підготовка і проведення заходів, доручень) [78].

Здійснення заходів з легалізації комп'ютерних програм – координує міжвідомча робоча група з питань легалізації комп'ютерних програм. Організаційно-технічне забезпечення діяльності міжвідомчої робочої групи здійснює Мінекономрозвитку. З метою забезпечення прозорості діяльності міжвідомчої робочої групи її рішення оприлюднюються на офіційному веб-сайті Мінекономрозвитку до 01 травня. Комп'ютерні програми, які не підлягають легалізації через моральну застарілість, невідповідність функціональним завданням органів виконавчої влади, вимогам захисту інформації тощо, виводяться з експлуатації до кінця року, в якому проводилася інвентаризація. Здійснення заходів з легалізації комп'ютерних програм є напрямом використання бюджетних коштів, що відображається в паспортах відповідних бюджетних програм. Органи виконавчої влади подають до 1 грудня Мінекономрозвитку перелік комп'ютерних програм, щодо яких здійснені заходи з легалізації, із зазначенням кількісних показників та обсягів коштів, спрямованих на здійснення заходів з легалізації у звітному періоді [68].

Злочин – є передбачене Кримінальним кодексом України суспільно небезпечне винне діяння (дія або бездіяльність), вчинене суб'єктом злочину. Залежно від ступеня тяжкості злочини поділяються на злочини невеликої тяжкості, середньої тяжкості, тяжкі та особливо тяжкі [12].

Знищення інформації в системі – дії, внаслідок яких інформація в системі зникає [5].

Зобов'язання працівників органів виконавчої влади, що використовують у своїй діяльності комп'ютерні програми – надавати доступ до них працівникам підрозділу ІТ для встановлення (переустановлення) комп'ютерних програм або проведення їх інвентаризації [67].

Ідентифікаційні дані особи – унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи [25].

Інвентаризація комп'ютерних програм – проводиться працівниками підрозділу ІТ або комісією, призначеною розпорядженням керівника органу. Мінекономрозвитку подає щороку до 01 червня КМУ узагальнену інформацію про результати інвентаризації комп'ютерних програм [67].

Інструкція – правовий акт, що видає або затверджує орган державного управління для встановлення певних правил, які регулюють організаційні, науково-технічні, фінансові, технологічні, інші спеціальні види діяльності установ, організацій, підприємств, їх підрозділів і служб, посадових осіб, громадян (наприклад, інструкція з діловодства) [78].

Інтернет – всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами [10].

Інтероперабельність – технологічна сумісність технічних рішень, що використовуються під час надання електронних послуг, та їх здатність взаємодіяти між собою [25].

Інформатизація – сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та ІТ, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки [9, 31].

Інформаційна безпека телекомунікаційних мереж – здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації [10].

Інформаційна послуга – дії суб'єктів щодо забезпечення споживачів інформаційними продуктами [9]. *Або: інформаційною послугою* – є діяльність з надання інформаційної продукції споживачам з метою задоволення їхніх потреб [2, 30]

Інформаційна продукція – матеріалізований результат інформаційної діяльності, призначений для задоволення потреб суб'єктів інформаційних відносин [2].

Інформаційна система органів державної статистики – сукупність технічних, програмних, комунікаційних та інших засобів, які забезпечують процес збирання, накопичення, опрацювання, поширення, збереження, захисту та використання статистичної інформації [22].

Інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування [9].

Інформаційний обмін – відправлення, отримання та передача електронних документів, що здійснюється користувачем кваліфікованих електронних довірчих послуг в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано документ [66].

Інформаційний продукт (продукція) – документована інформація, яка підготовлена і призначена для задоволення потреб користувачів [9].

Інформаційний ринок – це система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг [32].

Інформаційний суверенітет держави – здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави [9].

Інформаційні агентства – є зареєстровані як юридичні особи суб'єкти інформаційної діяльності, що діють з метою надання інформаційних послуг [29].

Інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле [5].

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [2]. *Або: інформація* – відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [10].

Інформація довідково-енциклопедичного характеру – систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище. *Основними джерелами* інформації довідково-енциклопедичного характеру є: енциклопедії, словники, довідники, рекламні повідомлення та оголошення, путівники, картографічні матеріали, електронні бази та банки даних, архіви різноманітних довідкових інформаційних служб, мереж та систем, а також довідки, що видаються уповноваженими на те органами державної влади та органами місцевого самоврядування, об'єднаннями громадян, організаціями, їх працівниками та автоматизованими інформаційно-телекомунікаційними системами. *Правовий режим* інформації довідково-енциклопедичного характеру визначається законодавством та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України [2].

Інформація з обмеженим доступом – є: 1) конфіденційна інформація; 2) таємна інформація; 3) службова інформація [2, 4].

Інформація письмова – відомості та повідомлення, висловлені за допомогою знаків письма [78].

Інформація про стан довкілля (екологічна інформація) – відомості та/або дані про: 1) стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими; 2) фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми); 3) стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля; 4) інші відомості та/або дані. *Правовий режим* інформації про стан довкілля (екологічної інформації) визначається законами України та міжнародними договорами України, згода на обов'язковість яких надана ВРУ. Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, *не може бути віднесена* до інформації з обмеженим доступом [2].

Інформація про товар (роботу, послугу) – відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги). Інформація про вплив товару (роботи, послуги) на життя та здоров'я людини *не може бути віднесена* до інформації з обмеженим доступом. *Правовий режим* інформації про товар (роботу, послугу) визначається законами України про захист прав споживачів, про рекламу, іншими законами та міжнародними договорами України, згода на обов'язковість яких надана ВРУ [2].

Інформація, що вводить в оману – є, зокрема, відомості, які: 1) містять неповні, неточні або неправдиві дані про походження товару, виробника, продавця, спосіб виготовлення, джерела та спосіб придбання, реалізації, кількість, споживчі властивості, якість, комплектність, придатність до застосування, стандарти, характеристики, особливості реалізації товарів, робіт, послуг, ціну і знижки на них, а також про істотні умови договору; 2) містять неповні, неточні або неправдиві дані про фінансовий стан чи господарську діяльність суб'єкта господарювання; 3) приписують повноваження та права, яких не мають, або відносини, в яких не перебувають; 4) містять посилення на обсяги виробництва, придбання, продажу чи поставки товарів, виконання робіт, надання послуг, яких фактично не було на день поширення інформації [27].

Інцидент кібербезпеки – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів [15].

Канал електрозв'язку – сукупність технічних засобів, призначених для перенесення електричних сигналів між двома пунктами телекомунікаційної мережі, і який характеризується смугою частот та/або швидкістю передачі [10].

Картка обліку комп'ютерної програми – повинна містити відомості про працівника, за яким закріплена ліцензія на використання КП, та/або залежно від принципу ліцензування – відомості про комп'ютер, на якому вона використовується, назву, вид КП, дату її встановлення, найменування виробника чи розповсюджувача, за необхідності – реквізити ліцензії. Картка обліку може також містити інформацію про обмеження щодо використання КП залежно від кількості ядер процесора на комп'ютерному обладнанні, кількості користувачів на одну ліцензію, кількості пристроїв, на яких користувач може використовувати КП, строку використання КП за наявності таких обмежень у ліцензії на використання КП. Картка обліку зберігається у підрозділі протягом строку дії ліцензії. У разі закріплення комп'ютера або ліцензії на використання КП за іншим працівником, установлення або вилучення комп'ютерних програм до картки обліку вноситься відповідний запис [67].

Категорія режиму секретності – категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях [3].

Кваліфіковані електронні довірчі послуги – електронні довірчі послуги, що надаються кваліфікованим надавачем електронних довірчих послуг відповідно до Закону України “Про електронні довірчі послуги” [66].

Кегль – розмір літер у друкарській системі мір (у пунктах) [78].

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [15].

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 [15].

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів [15].

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [15].

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [15].

Кіберзлочинність – сукупність кіберзлочинів [15].

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 [15].

Кіберрозвідка – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням [15].

Кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням [15].

Кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням [15].

Кінцеве обладнання – обладнання, призначене для з'єднання з пунктом закінчення телекомунікаційної мережі з метою забезпечення доступу до телекомунікаційних послуг [10].

Ключові слова – слова, необхідні і достатні для відтворення основного змісту документа [78].

Кодекс – єдиний законодавчий акт, у якому систематизовано норм окремої галузі права (наприклад, цивільного, кримінального) чи законодавства [78].

Комп'ютерна програма – набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах) [14].

Комплекс технічного захисту інформації – сукупність заходів та засобів, призначених для реалізації ТЗІ в ІС або на об'єкті [50].

Комплексна система захисту інформації – взаємопов’язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [5]. *Або: комплексна система захисту інформації* – сукупність організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації [65]. *Або: комплексна система захисту інформації* – створюється для забезпечення захисту інформації в системі та призначається для захисту інформації від: 1) витoku технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій; 2) несанкціонованих дій з інформацією, у тому числі з використанням комп’ютерних вірусів; 3) спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування. Захист інформації від витoku технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником інформації. Захист інформації від несанкціонованих дій, у тому числі від комп’ютерних вірусів, забезпечується в усіх системах. Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято розпорядником інформації [69].

Контрафактний примірник твору, фонограми, відеограми – примірник твору, фонограми чи відеограми, відтворений, опублікований і (або) розповсюджуваний з порушенням авторського права і (або) суміжних прав, у тому числі примірники захищених в Україні творів, фонограм і відеограм, що ввозяться на митну територію України без згоди автора чи іншого суб’єкта авторського права і (або) суміжних прав, зокрема з країн, в яких ці твори, фонограми і відеограми ніколи не охоронялися або перестали охоронятися [14].

Конфіденційна інформація – інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Відносини, пов’язані з правовим режимом конфіденційної інформації, регулюються законом [2]. *Або: конфіденційна інформація* – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [4]. *Або: конфіденційна інформація* – статистична інформація, яка належить до інформації з обмеженим доступом і знаходиться у володінні, користуванні або розпорядженні окремого респондента та поширюється виключно за його згодою відповідно до погоджених з ним умов [22].

Конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення [50].

Копія документа – документ, що відтворює інформацію оригіналу й усі його зовнішні ознаки або їх частину і засвідчується заведеним порядком (рівнозначна з оригіналом) [78]. *Або: копія документа* – документ, що містить точне знакове відтворення змісту чи документної інформації іншого документа і в окремих випадках деяких його зовнішніх ознак [76].

Користувач архівними документами – фізична або юридична особа, яка відповідно до законодавства ознайомлюється з архівними документами [34].

Користувач бібліотеки – фізична чи юридична особа, яка звернулася до послуг бібліотеки [18].

Користувачі електронних довірчих послуг – підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують електронні довірчі послуги у надавачів таких послуг відповідно до вимог цього Закону [25].

Короткий (цифровий) формат дати – це: 1) 19.11.2017 (Україна, Німеччина, Норвегія, Сербія, Франція, Швейцарія); 2) 19/11/2017 (Англія, Бельгія, Італія, Іспанія, Бразилія, Латинська Америка); 3) 19-11-2017 (Данія, Нідерланди, Португалія); 4) 2017-11-19 (Угорщина, Польща, Словаччина, Словенія, Чехія, Швеція); 5) 11-19-2017 США (примітка до всіх форматів дати: якщо день, місяць – одинарні числа, то додаємо «0») [108].

Кримінальне провадження – досудове розслідування і судове провадження, процесуальні дії у зв'язку із вчиненням діяння, передбаченого законом України про кримінальну відповідальність [13].

Криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо [3, 5].

Критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури [15].

Критично важливі об'єкти інфраструктури – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може сприяти негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей [15].

Легалізація комп'ютерних програм в органах виконавчої влади – приведення використання комп'ютерних програм у відповідність з вимогами законодавства про авторське право шляхом заміни неліцензійних комп'ютерних програм ліцензійними [68].

Легенда – 1) пояснювальний текст, що додається до карти, схеми й інших матеріалів і містить узагальнення й висновки; 2) пояснення умовних способів зображення на картах, діаграмах, схемах тощо; 3) відомості про виданий документ, що містять пошукові дані, вказівку на справжність, спосіб відтворення, зовнішні особливості, попередні видання документа [78].

Лист – узагальнена назва різних за змістом службових документів, що є засобом спілкування між установами, організаціями, приватними особами, повідомлення й оповіщення про що-небудь [78].

Ліцензійна комп'ютерна програма – комп'ютерна програма, яка використовується на умовах, визначених у ліцензії [67].

Ліцензія – документ, що засвідчує право суб'єкта господарювання на здійснення зазначеного в ньому виду діяльності у сфері телекомунікацій протягом визначеного строку на конкретних територіях з виконанням ліцензійних умов [10].

Ліцензія на використання комп'ютерної програми – дозвіл на використання комп'ютерної програми на умовах, визначених ліцензією, наданий правовласником [67].

Ліцензування – видача, переоформлення, продовження терміну дії, визнання недійсними, анулювання ліцензій, видача копій та дублікатів ліцензій, ведення ліцензійних справ та ліцензійних реєстрів, контроль за додержанням ліцензійних умов, видача розпоряджень про усунення порушень ліцензійних умов [10].

Локалізація програмних продуктів – приведення програмних продуктів, які використовуються в Україні, у відповідність із законами України та іншими нормативно-правовими актами, стандартами, нормами і правилами, що діють в Україні [9].

Макет документа – попередня чи остаточна схема розміщення інформації на документі [78].

Масова інформація – інформація, що поширюється з метою її доведення до необмеженого кола осіб [2].

Матеріальні носії секретної інформації – матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо [3].

Мета Концепції розвитку електронного урядування в Україні – є визначення напрямів, механізмів і строків формування ефективної системи електронного урядування в Україні для задоволення інтересів та потреб фізичних та юридичних осіб, вдосконалення системи державного управління, підвищення конкурентоспроможності та стимулювання соціально-економічного розвитку країни. Реалізація Концепції передбачена на період до 2020 року та покликана підтримати координацію та співпрацю органів державної влади та органів місцевого самоврядування для досягнення необхідного рівня ефективності та результативності розвитку електронного урядування, просування ідеї реформування державного управління та децентралізації на базі широкого використання сучасних інформаційно-комунікаційних технологій в усій країні, а також сприяти реалізації першочергових пріоритетів, визначених Стратегією сталого розвитку “Україна-2020” [55].

Мова діловодства в системі Національної поліції України – ведеться українською мовою, крім випадків, передбачених законодавством про мови в Україні. Документи, які надсилаються іноземним адресатам, оформлюються українською мовою або мовою держави-адресата, або однією з мов міжнародного спілкування. Діловодство в Робочому апараті Укрбюро Інтерполу ведеться українською мовою з використанням на бланках символіки Інтерполу відповідно до вимог цієї Інструкції з урахуванням рекомендацій Генерального секретаріату Інтерполу [76].

Мова інформації – визначається законом про мови, іншими актами законодавства в цій сфері, міжнародними договорами та угодами, згода на обов’язковість яких надана Верховною Радою України [2].

Монопольний (домінуючий) оператор телекомунікацій – оператор, який відповідно до законодавства України займає монопольне (домінуюче) становище на ринку певних телекомунікаційних послуг на території держави чи певного регіону [10].

Найбільш відомі на українському ринку правові ІПС – це: «Законодавство України», «Єдиний державний реєстр нормативно-правових актів», «Ліга: Закон», «Нормативні акти України» [108].

Найбільш поширені в Україні автоматизовані системи документообігу – це: e-Docs (www.elgnc.com.ua); Megapolis.DocNet (www.inbase.com.ua); MasterDoc (www.bkc.com.ua); ДІЛО (www.eos.com.ua); FossDoc (www.fossdoc.com.ua); АСКОД (www.infoplus.ua); SX-Government (www.sx-ua.com); Optima-WorkFlow-Стандарт (www.iisd.com.ua).

Наказ – основний розпорядчий документ, що видає керівник підприємства, установи, організації на основі єдиначальності і містить індивідуальні приписи або правові норми з питань внутрішньо-організаційної діяльності, адресовані підпорядкованим органам і працівникам [78].

Наукова (науково-технічна) продукція – науковий та (або) науково-технічний (прикладний) результат, призначений для реалізації [33].

Науковий (науково-технічний) проект – комплекс заходів, пов’язаних із забезпеченням виконання та безпосереднім проведенням наукових досліджень та (або) науково-технічних розробок з метою досягнення конкретного наукового або науково-технічного (прикладного) результату [33].

Науково-інформаційна діяльність – це сукупність дій, спрямованих на задоволення потреб громадян, юридичних осіб і держави у науково-технічній інформації, що полягає в її збиранні, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні [32].

Науково-технічна діяльність – наукова діяльність, спрямована на одержання і використання нових знань для розв’язання технологічних, інженерних, економічних, соціальних та гуманітарних проблем, основними видами якої є прикладні наукові дослідження та науково-технічні (експериментальні) розробки [33].

Науково-технічна інформація – будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України [2, 32].

Національна система конфіденційного зв’язку – сукупність спеціальних телекомунікаційних систем (мереж) подвійного призначення, які за допомогою криптографічних та/або технічних засобів забезпечують обмін інформацією з обмеженим доступом, крім інформації, що становить державну таємницю в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану [35].

Національна телекомунікаційна мережа – сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв’язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам [15].

Національний архівний фонд – сукупність архівних документів, що відображають історію духовного і матеріального життя Українського народу та інших народів, мають культурну цінність і є надбанням української нації [34].

Національний аудіовізуальний продукт – програми, фільми, аудіовізуальні твори, вироблені фізичними або юридичними особами України [42].

Неліцензійна комп'ютерна програма – комп'ютерна програма, яка використовується з порушенням умов, визначених у ліцензії, або не має чинної ліцензії на її використання. Використання КП, створених (розроблених), розповсюджених, а також забезпечених технічною підтримкою суб'єктів господарювання, які перебувають під контролем іноземної держави, до якої застосовано спеціальні економічні та інші обмежувальні заходи відповідно до Закону України «Про санкції», дозволяється до закінчення строку дії ліцензії без отримання технічної підтримки (оновлень, виправлень тощо) від зазначених суб'єктів господарювання. Не дозволяється продовження строку дії ліцензії або легалізація таких неліцензійних КП. Зазначені неліцензійні програми виводяться з експлуатації до кінця року, в якому проводилася інвентаризація КП. У разі необхідності ліцензійні КП після закінчення строку дії ліцензії та/або неліцензійні КП повинні бути замінені ліцензійними КП з аналогічними функціями, які створені (розроблені), розповсюджені, а також забезпечені технічною підтримкою суб'єктів господарювання, які не перебувають під контролем іноземної держави, до якої застосовано спеціальні економічні та інші обмежувальні заходи відповідно до Закону України «Про санкції» [68].

Неправомірне збирання комерційної таємниці – вважається добування протиправним способом відомостей, що відповідно до законодавства України становлять комерційну таємницю, якщо це завдало чи могло завдати шкоди суб'єкту господарювання [27].

Номенклатура справ – обов'язковий для кожної юридичної особи систематизований перелік назв справ, що формуються в її діловодстві, із зазначенням строків зберігання справ [34]. *Або: номенклатура справ* – обов'язковий для кожного органу чи підрозділу поліції систематизований перелік назв справ, що формуються в його діловодстві, із зазначенням строків їх зберігання [76]. *Або: номенклатура справ* – систематизований перелік чи список назв справ, заведених у діловодстві установи [78].

Нормативний документ – документ, в якому подано визначені правила, норми і т.ін. [78].

Нотаріус – це уповноважена державою фізична особа, яка здійснює нотаріальну діяльність у державній нотаріальній конторі, державному нотаріальному архіві або незалежну професійну нотаріальну діяльність, зокрема посвідчує права, а також факти, що мають юридичне значення, та вчиняє інші нотаріальні дії, передбачені законом, з метою надання їм юридичної вірогідності [36].

Об'єкт інформаційних відносин – є інформація [2].

Об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [15].

Об'єкти захисту в системі – є *інформація*, що обробляється в ній, та *програмне забезпечення*, яке призначено для обробки цієї інформації [5].

Обліковий запис – формалізований згідно зі стандартами мережі Інтернет запис на комп'ютерному обладнанні (комп'ютерах, серверах), підключеному до мережі Інтернет, що ідентифікує користувача (наприклад, власника веб-сайту) на такому обладнанні, включає в себе дані про доступ до частини каталогів і програмного забезпечення комп'ютерного обладнання, а також визначає права такого доступу, що надають можливість володільцю облікового запису додавати, видаляти, змінювати електронну (цифрову) інформацію і дані веб-сайту, надавати доступ до веб-сайту або його частин, окремих даних іншим особам, припиняти функціонування такого веб-сайту або його частини в межах облікового запису [14].

Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог: 1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; 2) розголошення інформації може завдати істотної шкоди цим інтересам; 3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні. *Обмеженню доступу підлягає інформація, а не документ.* Якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений [4].

Обов'язковий примірник документів – примірник різних видів тиражованих документів, який передає його виробник на безоплатній або платній основі юридичним особам, визначеним цим Законом [37].

Обов'язковий реквізит електронного документа – обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили [26].

Обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів [5].

Обсяг документообігу – кількість документів, що надійшли до організації чи укладені в ній за відповідний період [78].

Огляд – документ, що укладено з метою інформування підвідомчих та інших організацій про роботу в будь-якій галузі або про діяльність групи установ протягом визначеного періоду [78].

Оголошення – 1) інформація про масовий захід; 2) документ із такою інформацією [78].

Одержання інформації – це набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошеної інформації громадянами, юридичними особами або державою [30].

Одержувач обов'язкового примірника документів – юридична особа України, яка одержує обов'язковий примірник документів на безоплатній або платній основі та забезпечує його зберігання і використання [37].

Оновлення комп'ютерної програми – стала версія комп'ютерної програми (протестована розробником та/або користувачами щодо коректності її роботи), яка забезпечує виконання не менше однієї з таких умов: 1) *суттєво оптимізує роботу* комп'ютерної програми; 2) виконує *необхідні додаткові функції*; 3) виконує *нові функції захисту*, яких немає у попередній версії комп'ютерної програми [67].

Оперативно-розшукова діяльність – це система гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів [38].

Оператор телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж [10].

Оператор, провайдер телекомунікацій з істотною ринковою перевагою на ринку телекомунікаційних послуг – оператор, провайдер телекомунікацій, частка доходу якого на визначеному національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, ринку певних телекомунікаційних послуг протягом року, що передуює проведенню аналізу ринку, перевищує 25 відсотків сумарного доходу всіх операторів, провайдерів телекомунікацій, отриманого на цьому ринку за той самий період часу, або якщо внаслідок технологічного процесу надання послуги іншому оператору, провайдеру телекомунікацій її може бути надано тільки в мережі певного оператора, провайдера телекомунікацій [10].

Опис – юридично оформлений перелік документів [78].

Опис документів – виклад відомостей про склад і зміст документів в архівних довідниках і на титулах справ [78].

Опис справ в електронній формі – довідник в електронній формі, призначений для обліку та розкриття змісту одиниць зберігання, одиниць обліку, закріплення їх систематизації в межах архівного фонду [51].

Організаційна структура системи національних ресурсів – її утворюють: 1) спеціально уповноважений центральний орган виконавчої влади у галузі зв'язку та сфері інформатизації, відповідальний за ведення Національного реєстру електронних інформаційних ресурсів; 2) структурні підрозділи з питань інформаційних технологій, взаємодії із засобами масової інформації та зв'язків з громадськістю органів державної влади та органів місцевого самоврядування; 3) інформаційні підрозділи підприємств, установ та організацій, а також засоби масової інформації. *Інфраструктуру* системи національних ресурсів становлять органи державної влади та суб'єкти господарювання, що забезпечують формування, використання та захист, а також взаємодію виробників і користувачів національних ресурсів [59].

Організаційно-розпорядча документація – уніфікована підсистема управлінської документації, що забезпечує організацію процесів управління та управлінської праці [76].

Організація роботи зі службовими документами – організація здійснення документообігу, формування справ, зберігання службових документів та користування ними в процесі діяльності установи [76].

Оригінал документа – 1) перший примірник документа; 2) примірник документа, що є вихідним матеріалом для копіювання [78].

Оригінал електронного документа – вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги» [25]. У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Якщо автором створюються ідентичні за документарною інформацією та реквізитами *електронний документ та документ на папері*, кожен з документів є *оригіналом і має однакову юридичну силу*. Оригінал електронного документа повинен давати змогу довести його *цілісність та справжність* у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, в тому числі у паперовій копії. Електронна копія електронного документа засвідчується у порядку, встановленому законом. Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством [26].

Оригінал службового документа – примірник службового документа, що має оригінальний підпис посадової (службової) особи установи [76].

Основні види інформаційної діяльності: створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації [2]. *Або: основні види інформаційної діяльності* – є одержання, використання, поширення та зберігання інформації [30].

Основні види продукції інформаційних агентств – це електронна, друкована, фото-, кіно-, аудіо- та відеопродукція [29].

Основні завдання «Національної суспільної телерадіокомпанії України» – є: 1) *об'єктивне, повне, своєчасне і неупереджене* інформування про суспільно значущі події в Україні та за кордоном; 2) *сприяння консолідації* українського суспільства; 3) розвиток і зміцнення статусу *української мови та культури*, сприяння розвитку мов і культур національних меншин; 4) сприяння якнайповнішому задоволенню інформаційних, культурних та освітніх потреб населення України, у тому числі шляхом створення та поширення економічних, історично-документальних, культурно-мистецьких, навчально-пізнавальних, розважальних, спортивних програм, програм для дітей та молоді, людей з обмеженими фізичними можливостями, національних меншин, інших соціальних груп; 5) *оперативне інформування населення про надзвичайні ситуації, що становлять загрозу життю чи здоров'ю людей*; 6) надання громадянам України *затребуваних інформаційних продуктів*, відсутніх на комерційному ринку; 7) сприяння *зміцненню міжнародного авторитету* України [41].

Основні завдання для забезпечення формування системи національних ресурсів – 1) забезпечення широкого доступу до ресурсів, у тому числі іноземних, через глобальні інформаційні мережі; 2) правове врегулювання суспільних відносин, пов'язаних з формуванням, використанням та захистом національних ресурсів; 3) вироблення рекомендацій щодо приведення національних ресурсів до єдиних стандартів на базі новітніх інформаційних технологій, міжнародних стандартів, уніфікованих систем класифікації і кодування інформації; 4) створення ефективних національних пошукових, геоінформаційних та навігаційних систем; 5) забезпечення розвитку національної освіти, науки, культури через використання новітніх інформаційних технологій; 6) залучення до формування системи національних ресурсів недержавних структур; 7) створення умов для забезпечення захисту національних ресурсів незалежно від форми власності; 8) сприяння наповненню інформаційного ринку національними ресурсами [59].

Основні напрями державної інформаційної політики – є: 1) забезпечення доступу кожного до інформації; 2) забезпечення *рівних можливостей* щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; 3) створення умов для формування в Україні *інформаційного суспільства*; 4) забезпечення *відкритості та прозорості* діяльності суб'єктів владних повноважень; 5) *створення* інформаційних систем і мереж інформації, розвиток електронного урядування; 6) постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; 7) забезпечення *інформаційної безпеки* України; 8) сприяння *міжнародній співпраці в інформаційній сфері* та входженню України до світового інформаційного простору [2].

Основні принципи електронного документообігу – це: 1) *однократна реєстрація документа*, що дозволяє однозначно ідентифікувати документ; 2) *можливість паралельного виконання операцій*, що дозволяє скоротити час руху документів і підвищення оперативності їх виконання; 3) *безперервність руху документа*, що дозволяє ідентифікувати відповідального за виконання документа (завдання) в кожен момент часу життя документа (процесу); 4) *єдина база документів*, що дозволяє унеможливити дублювання документів; 5) *ефективно організована система пошуку документа*, що дозволяє знаходити документ, володіючи мінімальною інформацією про нього; 6) *розвинена система звітності* по різних статусах і атрибутах документів, що дозволяє контролювати рух документів по процесах документообігу і приймати управлінські рішення, ґрунтуючись на даних із звітів [108].

Основні принципи інформаційних відносин – є: 1) гарантованість права на інформацію; 2) відкритість, доступність інформації, свобода обміну інформацією; 3) достовірність і повнота інформації; 4) свобода вираження поглядів і переконань; 5) правомірність одержання, використання, поширення, зберігання та захисту інформації; 6) захищеність особи від втручання в її особисте та сімейне життя [2].

Особиста картка – документ, що служить для обліку й аналізу руху кадрів [78].

Особистий архівний документ – архівний документ, що створений фізичною особою або безпосередньо її стосується [34].

Особистий документ – офіційний документ, що посвідчує особу людини або її права, обов'язки, службовий чи суспільний стан (може містити і біографічні відомості) [78].

Особливий формат дати – це: 02.XII.2018 (лікарі); залізнична техніка.

Особливо цінний документ – документ, що має не скороминуче значення і є незамінним у разі його втрати [78].

Особова справа – справа, що містить документи про особу [78].

Отримувач – суб'єкт владних повноважень, що має право на отримання даних державного електронного інформаційного ресурсу, держателем якого є інший суб'єкт владних повноважень, під час надання адміністративних послуг і здійснення інших повноважень відповідно до покладених на нього завдань [57].

Офіційний документ – документ, створений організацією або посадовою особою й оформлений заведеним порядком [78].

Офіційні веб-портали вищих державних органів України:

Верховна рада України – <https://rada.gov.ua/>

Державна судова адміністрація України – <https://dsa.court.gov.ua/dsa/>

Кабінет Міністрів України – <https://www.kmu.gov.ua/ua>

Конституційний суд України – <http://www.ccu.gov.ua/>

Президент України – <https://www.president.gov.ua/>

Офіційні веб-портали вищих навчальних закладів МВС України:

Дніпропетровський державний університет внутрішніх справ – <http://dduvs.in.ua>

Донецький юридичний інститут МВС України – <http://www.dli.donetsk.ua/>

Луганський державний університет внутрішніх справ імені Е.О. Дідоренка – <http://www.lduvs.edu.ua/>

Львівський державний університет безпеки життєдіяльності – <https://ldubgd.edu.ua/>

Львівський державний університет внутрішніх справ – <http://www2.lvduvs.edu.ua/>

Національна академія внутрішніх справ – <https://www.naiu.kiev.ua/>

Національна академія державної прикордонної служби України імені Б. Хмельницького – <https://nadpsu.edu.ua/abiturientam/pravy-la-pryjomu/>

Національна академія національної гвардії України – <http://nangu.edu.ua/>

Національний університет цивільного захисту України – <http://nuczu.edu.ua/ukr/>

Одеський державний університет внутрішніх справ – <http://oduvs.edu.ua>

Харківський національний університет внутрішніх справ – <http://univd.edu.ua>

Офіційні веб-портали міністерств України:

Міністерство аграрної політики та продовольства України – <http://www.minagro.gov.ua/>

Міністерство внутрішніх справ України – <https://mvs.gov.ua/>

Міністерство екології та природних ресурсів України – <http://www.menr.gov.ua>

Міністерство економічного розвитку і торгівлі України – <http://www.me.gov.ua/?lang=uk-UA>

Міністерство енергетики та вугільної промисловості України – <http://mpe.kmu.gov.ua/>

Міністерство з питань ТОТ та ВПО України – <http://mtot.gov.ua/>

Міністерство закордонних справ України – <https://mfa.gov.ua/ua>

Міністерство інформаційної політики України – <http://mip.gov.ua/>

Міністерство інфраструктури України – <http://mtu.gov.ua/>

Міністерство культури України – <http://mincult.kmu.gov.ua>

Міністерство молоді та спорту – <http://dsmsu.gov.ua>

Міністерство оборони України – <http://www.mil.gov.ua/>

Міністерство освіти і науки України – <https://mon.gov.ua/>

Міністерство охорони здоров'я України – <http://moz.gov.ua/>

Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України – <http://www.minregion.gov.ua>

Міністерство соціальної політики України – <http://www.msp.gov.ua>

Міністерство у справах ветеранів України – <https://mva.gov.ua/>

Міністерство фінансів України – <http://www.minfin.gov.ua>

Міністерство юстиції України – <https://minjust.gov.ua>

Офіційні веб-портали підпорядкованих органів МВС України:

Державна міграційна служба України – <https://dmsu.gov.ua/>

Державна прикордонна служба України – <https://dpsu.gov.ua/>

Державна служба України з надзвичайних ситуацій –
<https://www.dsns.gov.ua/>

Національна гвардія України – <http://ngu.gov.ua/ua>

Національна поліція України – <https://www.npu.gov.ua/>

Офіційні веб-портали різних інших органів України:

Антимонопольний комітет України –
<http://www.amc.gov.ua/amku/control/main/uk/index>

Генеральна прокуратура України – <https://www.gp.gov.ua/>

Державна архівна служба України – <https://archives.gov.ua/>

Державна аудиторська служба України –
<http://www.dkrs.gov.ua/kru/uk/index>

Державна екологічна інспекція України – <https://www.dei.gov.ua/>

Державна регуляторна служба України – <http://www.drs.gov.ua/>

Державна служба спеціального зв'язку та захисту інформації України –
<http://www.dsszzi.gov.ua/dsszzi/control/uk/index>

Державна служба статистики України – <http://www.ukrstat.gov.ua/>

Державна служба фінансового моніторингу України –
<http://www.sdfm.gov.ua/>

Державна служба якості освіти України – <http://sqe.gov.ua/index.php/uk-ua/>

Державна фіскальна служба України – <http://sfs.gov.ua/>

Державне агентство з питань електронного урядування України –
<https://www.e.gov.ua/ua>

Державне бюро розслідувань – <https://dbr.gov.ua/>

Державний комітет телебачення і радіомовлення України –
<http://comin.kmu.gov.ua/>

Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів –
<https://arma.gov.ua/>

Національне агентство України з питань державної служби –
<https://nads.gov.ua/>

Національне агентство України з питань запобігання корупції –
<https://nazk.gov.ua/>

Національне антикорупційне бюро України – <https://nabu.gov.ua/>

Патрульна поліція України – <http://patrol.police.gov.ua/>

Пенсійний фонд України – <https://www.pfu.gov.ua/>

Рада національної безпеки і оборони України <http://www.rnbo.gov.ua/>

Служба безпеки України – <https://ssu.gov.ua/>

Фонд державного майна України – <http://www.spfu.gov.ua/>

Центральна виборча комісія – <https://www.cvk.gov.ua/>

Оформлення офіційного документа – процес творення документа з використанням необхідних (визначених) реквізитів [78].

Охорона державної таємниці – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв [3].

Охорона права на інформацію: 1) право на інформацію охороняється законом; держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації; 2) ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом; суб'єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію; 3) забороняється вилучення і знищення друкованих видань, експонатів, інформаційних банків, документів з архівних, бібліотечних, музейних фондів, крім встановлених законом випадків або на підставі рішення суду; 4) право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному законом [2].

Паперова копія оригіналу електронного документа – візуальне подання електронного документа у паперовій формі, яке засвідчене в порядку, встановленому цією Інструкцією [51].

Патентні документи – описи до патентів на винаходи (корисні моделі) та методичні документи до них [37].

ПЕОМ – персональна електронно-обчислювальна машина [76].

Первинний документ – документ, що містить вихідну інформацію [78].

Перевірка стану документів – установлення відповідності фактичної наявності одиниць зберігання документів записам в обліках архіву, виявлення документів, які вимагають консервації, реставрації, дезінфекції [78].

Передавання даних – передавання інформації у вигляді даних з використанням телекомунікаційних мереж [10].

Перенесення абонентського номера – телекомунікаційна послуга, що надається абоненту за його заявою, яка полягає у збереженні за абонентом наданого йому оператором телекомунікацій абонентського номера з метою використання цього номера для отримання телекомунікаційних послуг у мережі іншого оператора телекомунікацій, що надає телекомунікаційні послуги на території України [10].

Персональний номер – абонентський номер, що присвоюється зареєстрованому абоненту за його заявою у порядку, встановленому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, централізовано адмініструється і може використовуватися цим абонентом для отримання відповідно до договору телекомунікаційних послуг незалежно від географічного регіону України і типу цих послуг [10].

Першочергові проблеми розвитку електронного урядування в Україні: 1) недостатній рівень єдиної координації, контролю та взаємодії замовників завдань і проектів у сфері інформатизації та розвитку електронного урядування; 2) економічна криза, що призвела до зменшення обсягу фінансування завдань та проектів у сфері розвитку електронного урядування; 3) низька якість, ефективність та результативність реалізації проектів і завдань у зазначеній сфері; 4) несформованість та недосконалість нормативно-правової бази, що регулює сферу розвитку електронного урядування; 5) низька якість управління розробленням, впровадженням, підтримкою функціонування та розвитком інформаційно-телекомунікаційних систем (бази даних, реєстри тощо) та ресурсів (центри обробки даних, телекомунікаційні мережі тощо) органів влади; 6) несформованість базової інформаційно-телекомунікаційної інфраструктури електронного урядування як техніко-технологічної основи для реалізації всіх проектів і завдань у зазначеній сфері; 7) відсутність автоматизованого обміну даними та інтероперабельності між інформаційно-телекомунікаційними системами органів влади; 8) недостатній рівень інформаційної безпеки та захисту інформації в інформаційно-телекомунікаційних системах органів влади; 9) низькі темпи запровадження електронних форм взаємодії між органами влади і фізичними та юридичними особами, зокрема надання електронних послуг та доступу до відкритих даних; 10) неврегульованість питання електронної ідентифікації та автентифікації фізичних та юридичних осіб під час взаємодії з органами влади; 11) низькі темпи розвитку внутрішніх систем електронного документообігу та сучасних інформаційно-аналітичних інструментів підтримки прийняття управлінських рішень; 12) недостатній рівень готовності державних службовців та працівників органів місцевого самоврядування, фізичних та юридичних осіб до запровадження і використання інструментів електронного урядування; 13) цифрова нерівність у використанні інформаційно-комунікаційних технологій між органами влади на центральному та місцевому рівні; 14) недостатній рівень участі громадян та контролю у зазначеній сфері [55].

Письмовий документ – текстовий документ, в якому інформацію зафіксовано (записано) графічними знаками письма [78].

Підзаконний акт – правовий акт органу державної влади, що прийнято на основі закону з метою його виконання [78].

Підписання проекту електронного документа – накладання уповноваженою особою (уповноваженими особами), зазначеною (зазначеними) у реквізитах підписувача такого документа, електронного цифрового підпису (підписів) на проект електронного документа для засвідчення факту його затвердження [51].

Підрозділи документального забезпечення – Департамент документального забезпечення, управління, відділи, сектори документального забезпечення, канцелярії органів та підрозділів поліції [76].

План – документ, в якому викладено точний перелік робіт або заходів, призначених до виконання, їх послідовність, обсяг, тимчасові координати, керівників і конкретних виконавців, терміни проведення (плани можуть бути перспективні, розраховані на декілька років, річні, квартальні, місячні, тижневі тощо) [78].

План захисту інформації в системі – захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого службою захисту інформації плану захисту інформації в системі, який містить: 1) завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації; 2) визначення моделі загроз для інформації в системі; 3) основні вимоги щодо захисту інформації та правила доступу до неї в системі; 4) перелік документів, згідно з якими здійснюється захист інформації в системі; 5) перелік і строки виконання робіт службою захисту інформації [69].

Планова інвентаризація комп'ютерних програм – проводиться щороку з метою здійснення контролю за станом дотримання законодавства з питань їх правової охорони та визначення потреби у нових програмах. Інформацію про результати планової інвентаризації, що проводиться згідно з методикою проведення інвентаризації, встановленою Мінекономрозвитку, органи виконавчої влади подають щороку до 01 березня Мінекономрозвитку [67].

Повідомлення – документ, що інформує про майбутні заходи (наприклад, засідання, збори, конференція) і пропонує взяти в них участь [78].

Повний формат дати – це: 19.11.2017 08:15:20 (наприклад: фіскальний чек, відеореєстратор, журнал дзвінків, sms, створення файлу, протокол слідчої дії) [108].

Повноваження державних органів у сфері захисту інформації в системах – вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України. Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації: 1) розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції; 2) визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом; 3) організовує проведення державної експертизи КСЗІ, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації; 4) здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом; 5) здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання таких загрозі [5].

Погоджувач – посадова особа, що здійснює візування (погодження) проекту документа [51].

Подання – документ, що містить пропозиції про призначення, переміщення або заохочення особового складу, а також рекомендації щодо визначених дій і заходів із питань діяльності установ [78].

Податкова інформація – сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України. Правовий режим податкової інформації визначається Податковим кодексом України та іншими законами [2].

Позапланова інвентаризація комп'ютерних програм – проводиться за рішенням керівника органу виконавчої влади або Мінекономрозвитку з метою здійснення контролю за станом дотримання законодавства з питань правової охорони КІ та упорядкування їх використання в органах виконавчої влади [67].

Положення – нормативний акт, що визначає порядок створення, права, обов'язки й організацію роботи установи, структурних підрозділів на тривалий час [78].

Порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст [5].

Порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації [5].

Послуга – діяльність виконавця з надання (передачі) споживачеві певного визначеного договором матеріального чи нематеріального блага, що здійснюється за індивідуальним замовленням споживача для задоволення його особистих потреб [28].

Постанова – нормативний акт, що приймають вищі й деякі центральні органи колегіального управління для розв'язання найбільш важливих і принципових питань, встановлення стабільних норм, правил поведінки [78].

Постачальник – суб'єкт владних повноважень, що є держателем (розпорядником) державного електронного інформаційного ресурсу [57].

Постачальник послуг хостингу – особа, яка надає власникам веб-сайтів послуги і (або) ресурси для розміщення веб-сайтів або їх частин у мережі Інтернет та із забезпечення доступу до них через мережу Інтернет. Власник веб-сайту, який розміщує свій веб-сайт або його частину в мережі Інтернет на власних ресурсах і (або) самостійно забезпечує доступ до нього з використанням Інтернет, одночасно є постачальником послуг хостингу [14].

Постійний реквізит документа – реквізит документа, обов'язково застосовуваний під час виготовлення бланка документа [78].

Потреба органів виконавчої влади в комп'ютерних програмах – визначається виходячи з необхідності забезпечення виконання існуючих і нових завдань, покладених на ці органи, створення або модернізації інформаційних чи телекомунікаційних систем, заміни старих версій програм або компонентів комп'ютерів та/або їх периферійного обладнання, а також у разі висунення додаткових вимог до КП, що вже використовуються. Придбання ліцензійних КП або ліцензій на їх використання та інсталяція КП органами виконавчої влади здійснюється з урахуванням потреби. При цьому здійснюється придбання і використання виключно ліцензійних КП, які повинні мати відповідну ліцензію в паперовій та/або електронній формі та у разі наявності іншу документацію в паперовій та/або електронній формі, яка подається правовласником користувачам ліцензійних КП [67].

Поширення інформації – це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошеної інформації [30].

Пошукові реквізити документа – відомості про місце зберігання документа: архівний шифр і посилання на номер аркуша (або сторінки) документа [78].

Пояснювальна записка – 1) документ особистого характеру, в якому автор пояснює певні дії, факти, вчинки (найчастіше – порушення дисципліни, невиконання роботи, доручення тощо); 2) документ, який пояснює зміст окремих положень основного документа (наприклад, плану, звіту, проекту) [78].

Права керівника підрозділу інформаційних технологій щодо використання комп'ютерних програм – 1) подає керівникові органу виконавчої влади пропозиції про необхідність придбання нових КП (чи комп'ютерів з попередньо встановленими програмами), забезпечує отримання необхідних КП, що розповсюджуються на безоплатній основі, та проведення їх інвентаризації; 2) організовує роботу із створення архівів КП та збереження супровідної документації; 3) організовує проведення планових та позапланових перевірок дотримання вимог цього Порядку; 4) перевіряє у разі потреби наявність та справжність ліцензії; 5) організовує подання методичної допомоги працівникам з питань правомірного використання КП; 6) здійснює заходи з метою запобігання неправомірному використанню КП [67].

Права підрозділу інформаційних технологій щодо обліку комп'ютерних програм – 1) складає інвентарний список комп'ютерних програм; 2) оформляє на кожну ліцензію на використання комп'ютерної програми картку обліку в електронній або паперовій формі із зазначенням комп'ютера, на якому використовується ліцензія, або із зазначенням працівника, за яким вона закріплена, якщо умови ліцензії на використання комп'ютерної програми передбачають закріплення її за користувачем, а не за комп'ютером, на який вона встановлюється [67].

Права працівників органів виконавчої влади, що використовують у своїй діяльності комп'ютерні програми – зобов'язані дотримуватися законодавства з питань правової охорони комп'ютерних програм та виконувати умови їх використання. При цьому зазначені працівники *не мають право*: 1) установлювати комп'ютерні програми та використовувати їх без дозволу працівника підрозділу інформаційних технологій; 2) відтворювати і розповсюджувати комп'ютерні програми та надавати доступ до них третім особам без дозволу особи, що має виключне право видавати дозвіл на використання комп'ютерних програм; 3) використовувати на робочому місці комп'ютерні програми, не зазначені в картці обліку. Встановлення комп'ютерних програм чи їх переустановлення здійснюється працівником підрозділу інформаційних технологій або відповідальною особою, визначеною наказом органу виконавчої влади [67].

Правила – службові документи організаційного характеру, у яких викладено обов'язкові для виконання вимоги, норми, настанови, що регламентують визначений порядок дій або поведінки [78].

Право на інформацію: 1) кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів; 2) реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб [2].

Правова інформація – будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо. Джерелами правової інформації є Конституція України, інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань. З метою забезпечення доступу до законодавчих та інших нормативних актів фізичним та юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття [2].

Правовий статус – набрання електронними даними юридичної сили [51].

Правовласник – особа, якій відповідно до закону чи договору належать майнові права інтелектуальної власності на комп'ютерну програму, або особа, яка діє від імені такої особи в межах наданих повноважень [67].

Предметний каталог – каталог документальних матеріалів, що містить відомості про предмети, факти, події, географічні назви й осіб, згаданих у документах (розташовано в алфавітному порядку) [78].

Предметний покажчик – покажчик основних предметних (або тематичних) позначень, розташованих в алфавітному порядку [78].

Примірник відеограми – копія відеограми на відповідному матеріальному носії, яка виконана безпосередньо чи опосередковано із цієї відеограми і містить усі зафіксовані на ній рухомі зображення чи їх частину (як із звуковим супроводом, так і без нього) [14].

Примірник електронного документа – файл, який містить набір даних, тотожний оригіналу електронного документа [51].

Примірник твору – копія твору, виконана у будь-якій матеріальній формі [14].

Примірник фонограми – копія фонограми на відповідному матеріальному носії, яка виконана безпосередньо чи опосередковано із цієї фонограми і містить усі зафіксовані на ній звуки чи їх частину [14].

Принципи формування та вимоги до змісту національних ресурсів – під час формування системи національних ресурсів повинні використовуватися технології і засоби, спроможні забезпечити їх необхідний рівень та доступність через глобальні інформаційні мережі. Власники національних ресурсів, фізичні та юридичні особи, що надають послуги із використанням національних ресурсів, зобов'язані дотримуватися принципів законності, достовірності, загальнодоступності, забезпечення захисту ресурсів та прав користувачів [59].

Притягнення до кримінальної відповідальності – стадія кримінального провадження, яка починається з моменту повідомлення особі про підозру у вчиненні кримінального правопорушення [13].

Прихована реклама – інформація про особу чи товар у програмі, передачі, публікації, якщо така інформація слугує рекламним цілям і може вводити в оману осіб щодо дійсної мети таких програм, передач, публікацій [40].

Пріоритетні напрями формування системи національних ресурсів – є: 1) правове врегулювання відносин, що виникають під час формування, використання і захисту національних ресурсів; 2) гармонізація нормативно-правової бази у сфері національних ресурсів з міжнародними правовими нормами; 3) визначення та вдосконалення структури і складу національних ресурсів; 4) управління національними ресурсами [59].

Провайдер телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку [10].

Проводовий електрозв'язок – передавання і приймання інформації із застосуванням проводових ліній з металевими або волоконнооптичними жилами [10].

Програма – документ, в якому викладено основні напрями роботи установи чи підприємства на певний період або етап і строки їх здійснення [78].

Програмно-технічний комплекс, що використовується під час надання електронних довірчих послуг – апаратні, апаратно-програмні та програмні засоби, що забезпечують виконання функцій, пов'язаних з наданням електронних довірчих послуг [25].

Продукція інформаційного агентства – це матеріалізований результат його діяльності, призначений для розповсюдження з метою задоволення інформаційних потреб громадян, юридичних осіб, держави [29].

Проект документа – попередній текст документа, призначений для розгляду [78].

Проект електронного документа – документ в електронній формі до накладення електронного цифрового підпису уповноваженою особою (уповноваженими особами), зазначеною (зазначеними) у реквізитах підписувача такого документа [51].

Пропозиція – різновид доповідної записки, у якому є перелік конкретних пропозицій із певного питання [78].

Протокол – 1) документ, який фіксує хід обговорення питань і прийняття рішень на зборах, засіданнях, нарадах, судовому процесі, конференціях колегіальних органів; 2) один із видів процесуально-правових актів [78].

Публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом. Публічна інформація є *відкритою*, крім випадків, встановлених законом [4].

Публічна інформація у формі відкритих даних – це публічна інформація у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання. Розпорядники інформації зобов'язані надавати публічну інформацію у формі відкритих даних на запит, оприлюднювати і регулярно оновлювати її на єдиному державному веб-порталі відкритих даних та на своїх веб-сайтах. Публічна інформація у формі відкритих даних є дозволеною для її подальшого вільного використання та поширення. Будь-яка особа може вільно копіювати, публікувати, поширювати, використовувати, у тому числі в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до складу власного продукту, публічну інформацію у формі відкритих даних з обов'язковим посиланням на джерело отримання такої інформації [4].

Рапорт – письмове звернення працівника до вищої посадової особи з викладом питань службового чи особистого характеру і проханням у зв'язку з цим [78].

Реалізація державної політики у сфері державних ресурсів полягає у **розв'язанні таких завдань** – 1) створення та ведення Національного реєстру електронних інформаційних ресурсів, зокрема реєстрація та облік державних ресурсів, формування і забезпечення доступності інформації про склад, розміщення і умови використання ресурсів; 2) систематизація, забезпечення доступу до наявних державних ресурсів та їх актуалізація; 3) формування та забезпечення ефективного використання державних ресурсів органами державної влади; 4) вдосконалення нормативно-правової бази, зокрема визначення порядку і умов користування, оплати робіт, пов'язаних з формуванням, використанням, та захистом державних ресурсів; 5) координація діяльності органів державної влади і недержавних структур у сфері формування, використання та захисту державних ресурсів. Слід сприяти залученню недержавних структур для надання інформаційних послуг з використанням державних ресурсів [59].

Реалізація державної політики у сфері недержавних ресурсів полягає у **розв'язанні таких завдань** – 1) розвиток конкурентного середовища, підвищення асортименту і якості інформаційних послуг з використанням національних ресурсів; 2) сприяння заснуванню і підтримка суб'єктів інформаційного ринку недержавної форми власності, які надаватимуть послуги з використанням національних ресурсів; 3) сприяння наповненню інформаційного ринку національними ресурсами; 4) розроблення та реалізація заходів, спрямованих на захист прав користувачів; 5) гармонізація з міжнародними правовими нормами нормативно-правової бази, пов'язаної з ресурсами; 6) забезпечення сертифікації національних ресурсів; 7) сприяння проведенню незалежних експертиз, конкурсів, рейтингових досліджень [59].

Реалізація Концепції розвитку електронного урядування в Україні здійснюється за такими основними принципами – 1) *цифровий за замовчуванням* – забезпечення будь-якої діяльності органів влади (у тому числі надання публічних послуг, забезпечення міжвідомчої взаємодії, взаємодії з фізичними та юридичними особами, інформаційно-аналітичної діяльності) передбачає електронну форму реалізації як пріоритетну, а планування та реалізацію будь-якої реформи, проекту чи завдання – із застосуванням інформаційно-комунікаційних технологій; 2) *одноразове введення інформації* – реалізація підходу, за якого фізичні та юридичні особи лише один раз подають інформацію до органів влади, а у подальшому ця інформація повторно використовується органами влади для надання публічних послуг та виконання інших владних повноважень з дотриманням вимог захисту інформації та персональних даних; 3) *сумісність за замовчуванням* – здійснення проектування та функціонування інформаційно-телекомунікаційних систем в органах влади відповідно до єдиних відкритих вимог та стандартів для забезпечення їх подальшої сумісності та електронної взаємодії та повторного використання; 4) *доступність та залучення громадян*; 5) *відкритість та прозорість*; 6) *довіра та безпека* [55].

Редакційна правка – будь-яке редагування проекту електронного документа, виконуване автором, погоджувачем або підписувачем [51].

Реєстр – перелік, що застосовують у бухгалтерському обліку чи діловодстві [78].

Реєстратор – працівник служби діловодства установи, уповноважений на здійснення реєстрації вхідної та/або вихідної кореспонденції установи [51].

Реєстраційна картка – картка, призначена для обліку документів у діловодстві установи [78].

Реєстраційно-моніторингова картка – картка в електронній формі, що містить вичерпну інформацію про створення, одержання, проходження, виконання, відправлення, зберігання та знищення в установі документа незалежно від форми його створення [51].

Реєстрація документів – запис в облікових формах (журналах, картках тощо) стислих відомостей про документ і проставлення на документі індексу й дати реєстрації [78].

Режим секретності – встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці [3].

Результати навчання – знання, уміння, навички, способи мислення, погляди, цінності, інші особисті якості, які можна ідентифікувати, спланувати, оцінити і виміряти та які особа здатна продемонструвати після завершення освітньої програми або окремих освітніх компонентів [20]. *Або: **результати навчання*** – знання, уміння, навички, способи мислення, погляди, цінності, інші особисті якості, набуті у процесі навчання, виховання та розвитку, які можна ідентифікувати, спланувати, оцінити і виміряти та які особа здатна продемонструвати після завершення освітньої програми або окремих освітніх компонентів [39].

Реквізит документа – обов’язковий складник офіційного документа, відсутність якого позбавляє документ юридичної сили (наприклад, назва, дата, підпис, печатка і т. ін.); кожен документ має йому властивий набір реквізитів і порядок їх розташування [78].

Реквізит електронного документа – інформація, зафіксована в електронному документі та реєстраційно-моніторинговій картці для його ідентифікації, організації обігу та надання йому юридичної сили [51].

Реквізит службового документа – обов’язковий елемент, зафіксований у документі для його ідентифікації, організації обліку та надання йому юридичної сили [76].

Реклама – інформація про особу чи товар, розповсюджена в будь-якій формі та в будь-який спосіб і призначена сформулювати або підтримати обізнаність споживачів реклами та їх інтерес щодо таких особи чи товару [40].

Репродукція документа – факсимільна копія документа, виконана поліграфічними й іншими технічними засобами, в якій зберігаються лінійні співвідношення і тональність оригіналу [78].

Рішення – підзаконний правовий акт (вирок суду, постанова) [78].

Розголошення комерційної таємниці – є ознайомлення іншої особи без дозволу особи, уповноваженої на те, з відомостями, що відповідно до законодавства України становлять комерційну таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням відповідних обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання [27].

Розмноження документів – процес відтворення документів через різні способи разового й тиражного копіювання [78].

Розпорядження – правовий акт, що видає одноосібно керівник організації, установи, а також керівник колегіального органу державного управління для виконання оперативних завдань [78].

Розсекречування матеріальних носіїв секретної інформації – зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації [3].

Роумінг національний – телекомунікаційна послуга, яка забезпечує можливість абонентам одного оператора телекомунікацій, що надає послуги рухомого (мобільного) зв'язку на території України, отримувати телекомунікаційні послуги в телекомунікаційній мережі іншого оператора (операторів) у межах України [10].

РСО – режимно-секретний орган [76].

Рухомий (мобільний) зв'язок – електрозв'язок із застосуванням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах усіх пунктів закінчення телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції [10].

Свідцтво – офіційний документ, що засвідчує той чи інший факт і має юридичне значення (наприклад, свідоцтво про народження, свідоцтво про закінчення навчального закладу, свідоцтво про укладення шлюбу, свідоцтво про винахід) [78].

Середній формат дати – це: 19-лис-2017 (наприклад: бази даних) [108].

Система електронного документообігу установи – сукупність програмно-технічних засобів, призначених для автоматизованого виконання завдань щодо організації роботи з електронними документами у діловодстві установи [51].

Система моніторингу – комплексна автоматизована система безперервного збору, обробки, систематизації та аналізу інформації про стан виконання управлінських рішень (електронних документів) в установі [51].

Система обов'язкового примірника документів – сукупність видів обов'язкових примірників документів, а також порядок їх доставляння, зберігання та використання [37].

Системи «Ліга: Закон» – найповніше джерело систематизованої та достовірної правової інформації зі зручними інструментами для пошуку. Дають змогу швидко знайти й проаналізувати правову інформацію на будь-який момент часу, оцінити ситуацію та прийняти правильне рішення [108].

Системи електронних комунікацій – системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних [15].

Скарга – звернення з вимогою про поновлення прав і захист законних інтересів громадян, порушених діями (бездіяльністю), рішеннями державних органів, органів місцевого самоврядування, підприємств, установ, організацій, об'єднань громадян, посадових осіб [7].

Склад Національної системи конфіденційного зв'язку – складовими Національної системи конфіденційного зв'язку є спеціальні телекомунікаційні системи (мережі), їх фіксовані і мобільні компоненти, централізовані системи захисту інформації та оперативно-технічного управління. Структура побудови Національної системи конфіденційного зв'язку повинна забезпечувати відокремлення інформації з обмеженим доступом, крім інформації, що становить державну таємницю, органів державної влади та органів місцевого самоврядування, інших юридичних та фізичних осіб з використанням криптографічних та/або технічних засобів [35].

Служба діловодства – Департамент документального забезпечення Національної поліції України, підрозділи документального забезпечення та уповноважені особи, що забезпечують реєстрацію, облік, організацію документообігу службових документів, зберігання документаційного фонду або його частини до передачі на архівне зберігання [76]. *Або: служба діловодства* – структурний підрозділ або відповідальна особа установи, що забезпечує реєстрацію, облік, організацію документообігу службових документів, зберігання документаційного фонду або його частини до передавання на зберігання до архіву установи [51].

Служба захисту інформації – здійснює організацію та проведення робіт із захисту інформації в системі, забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації. Утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи. У разі коли обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою. Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту – покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи [69].

Службова електронна пошта – електронна пошта (поштова скринька) працівника установи, сформована з використанням доменного імені у домені gov.ua для обміну управлінською інформацією, яка не має юридичної сили [51].

Службова записка – документ про виконання роботи, що надсилає посадова особа іншій посадовій особі (як правило, керівникові) [78].

Службова інформація – відповідно до вимог частини другої статті 6 Закону України «Про державну таємницю» до службової може належати така інформація: 1) що міститься в документах суб'єктів владних повноважень, які становлять внутрішньому службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; 2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф “для службового користування” [4].

Службовий документ – офіційно зареєстрований службою діловодства або відповідним чином засвідчений документ, що одержаний чи створений органом чи підрозділом поліції в процесі його діяльності та має відповідні реквізити [76].

Службовий електронний документ – офіційно зареєстрований службою діловодства або відповідним чином засвідчений електронний документ, що одержаний чи створений установою у процесі її діяльності та складається з обов'язкових реквізитів [51].

Службовий твір – твір, створений автором у порядку виконання службових обов'язків відповідно до службового завдання чи трудового договору (контракту) між ним і роботодавцем [14].

Соціологічна інформація – будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо. *Правовий режим* соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана ВРУ [2].

Спеціальна телекомунікаційна система (мережа) – телекомунікаційна система (мережа), призначена для обміну інформацією з обмеженим доступом [35].

Спеціальна телекомунікаційна система (мережа) подвійного призначення – спеціальна телекомунікаційна система (мережа), призначена для забезпечення телекомунікацій (електрозв'язку) в інтересах органів державної влади та органів місцевого самоврядування, з використанням частини її ресурсу для надання послуг іншим споживачам [35].

Список – документ, що містить перелік осіб або предметів у певному порядку, укладений для інформації чи реєстрації [78].

Споживач телекомунікаційних послуг (споживач) – юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб [10].

Справа – документ або сукупність документів, що стосуються одного питання або ділянки роботи [78].

Сталість телекомунікаційної мережі – властивості телекомунікаційної мережі зберігати повністю або частково свої функції за умови впливу на неї дестабілізуючих чинників [10].

Статистична інформація – документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства [2, 22]. Офіційна державна статистична інформація підлягає систематичному оприлюдненню. Держава гарантує суб'єктам інформаційних відносин відкритий доступ до офіційної державної статистичної інформації, за винятком інформації, доступ до якої обмежений згідно із законом. Правовий режим державної статистичної інформації визначається Законом України «Про державну статистику» [22], іншими законами та міжнародними договорами України, згода на обов'язковість яких надана ВРУ [2].

Статистична методологія – сукупність науково обґрунтованих способів, правил і методів статистичного вивчення масових соціально-економічних явищ та процесів, які встановлюють порядок збирання, опрацювання і аналізу статистичної інформації [22].

Статистичне спостереження – планомірний, науково організований процес збирання даних щодо масових явищ та процесів, які відбуваються в економічній, соціальній та інших сферах життя України та її регіонів, шляхом їх реєстрації за спеціальною програмою, розробленою на основі статистичної методології [22].

Стенограма – дослівний запис виступів, реплік, запитань і відповідей у ході певної наради, зборів, конференцій тощо методом стенографії або звукозапису, який потім розшифровують і друкують [78].

Стратегія формування системи ресурсів органів державної влади – полягає в систематизації та інтеграції зазначених ресурсів з метою забезпечення прозорості, відкритості, підвищення, оперативності та ефективності роботи органів державної влади та забезпечення широкого доступу громадян до державних ресурсів [59].

Страхова копія документа – копія особливо цінного документа, виготовлена на випадок його втрати або пошкодження [78].

Страховий фонд копій документів – сукупність страхових копій документів [78].

Строк (термін) придатності – строк (термін), визначений НПА, нормативними документами, умовами договору, протягом якого у разі додержання відповідних умов зберігання та/або експлуатації чи споживання продукції її якісні показники і показники безпеки повинні відповідати вимогам НПА, нормативних документів та умовам договору [28].

Строк зберігання документа – період обов'язкового зберігання службового документа, визначений законодавством унаслідок проведення експертизи його цінності [76].

Строк зберігання електронного документа – період часу обов'язкового зберігання службового електронного документа, визначений номенклатурою справ установи на підставі нормативно-правових актів [51].

Строк розгляду запитів на інформацію – розпорядник інформації має надати відповідь на запит на інформацію *не пізніше п'яти робочих днів* з дня отримання запиту. У разі якщо запит на інформацію стосується інформації, необхідної для захисту життя чи свободи особи, щодо стану довкілля, якості харчових продуктів і предметів побуту, аварій, катастроф, небезпечних природних явищ та інших надзвичайних подій, що сталися або можуть статись і загрожують безпеці громадян, відповідь має бути надана *не пізніше 48 годин* з дня отримання запиту. Клопотання про термінове опрацювання запиту має бути обґрунтованим. У разі якщо запит стосується надання великого обсягу інформації або потребує пошуку інформації серед значної кількості даних, розпорядник інформації може продовжити строк розгляду запиту до *20 робочих днів* з обґрунтуванням такого продовження. Про продовження строку розпорядник інформації повідомляє запитувача в письмовій формі *не пізніше п'яти робочих днів* з дня отримання запиту. Інформація на запит надається *безкоштовно*. У разі якщо задоволення запиту на інформацію передбачає виготовлення копій документів обсягом *більш як 10 сторінок*, запитувач зобов'язаний відшкодувати фактичні витрати на копіювання та друк. При наданні особі інформації про себе та інформації, що становить суспільний інтерес, плата за копіювання та друк *не стягується* [4].

Строк служби – календарний строк використання продукції за призначенням, починаючи від введення в обіг чи після ремонту, протягом якого виробник (виконавець) гарантує її безпеку та несе відповідальність за істотні недоліки, що виникли з його вини [28].

Ступінь секретності («особливої важливості», «цілком таємно», «таємно») – це категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою. Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, не може перевищувати для інформації із ступенем секретності *«особливої важливості»* – 30 років, для інформації *«цілком таємно»* – 10 років, для інформації *«таємно»* – 5 років [3].

Суб'єкт владних повноважень – орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень [2].

Суб'єкти відносин, пов'язаних із захистом інформації в системах – є: 1) володільці інформації; 2) власники системи; 3) користувачі; 4) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи. На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі – розпоряднику системи [5].

Суб'єкти електронного документообігу – автор, підписувач, адресат та посередник, які набувають передбачених законом або договором прав і обов'язків у процесі електронного документообігу [26].

Суб'єкти інформаційних відносин – є: 1) фізичні особи; 2) юридичні особи; 3) об'єднання громадян; 4) суб'єкти владних повноважень [2].

Суб'єкти Національної системи конфіденційного зв'язку – органи державної влади та органи місцевого самоврядування, юридичні та фізичні особи, що беруть участь у створенні, функціонуванні, розвитку та використанні цієї системи [35].

Суб'єкти ринку телекомунікацій – оператори, провайдери телекомунікацій, споживачі телекомунікаційних послуг, виробники та/або постачальники технічних засобів телекомунікацій [10].

Судове рішення – процесуальний документ, ухвалений судом (у тому числі слідчим суддею під час досудового розслідування) під час розгляду справи (матеріалів кримінального провадження) на будь-якій стадії судового провадження (ухвала, окрема ухвала, рішення, вирок, постанова, судовий наказ) [64].

Суспільно необхідні видання – пріоритетні види видань для забезпечення загальнодержавних потреб [19].

Схема електронної ідентифікації – система електронної ідентифікації, в якій засоби електронної ідентифікації видаються фізичним, юридичним особам та представникам юридичних осіб [25].

Схиленням до розголошення комерційної таємниці – є спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням відповідних обов'язків відомості, що відповідно до законодавства України становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання [27].

Табель – документ, в якому є перелік показників, складений у певному порядку [78].

Таблиця – 1) тип тексту документа, у якому інформацію подано в цифровій чи словесній формі і викладено в рубриках вертикальних і горизонтальних площин; 2) документ із таким текстом [78].

Таємна інформація – інформація, доступ до якої обмежується відповідно до частини другої статті 6 Закону України «Про державну таємницю» [3], розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю [4].

Таємний архів – архівна установа, про існування якої не заявлено публічно [34].

Тезаурус – словник-довідник, в якому перераховано всі лексичні одиниці інформаційно-пошукової мови (дескриптори) із їх зв'язками, а також синонімічні дескриптори та ключові слова й словосполучення природної мови [78].

Тези – стислий виклад основних думок тексту документа чи виступу [78].

Телебачення (телемовлення) – виробництво аудіовізуальних програм та передач або комплектування (пакування) придбаних аудіовізуальних програм та передач і їх поширення незалежно від технічних засобів розповсюдження, які приймаються необмеженою кількістю осіб [42].

Телеграма – узагальнена назва різних за складом службових документів, переданих телеграфом [78].

Телекомунікаційна мережа доступу – частина телекомунікаційної мережі між пунктом закінчення телекомунікаційної мережі та найближчим вузлом (центром) комутації включно [10].

Телекомунікаційна мережа загального користування – телекомунікаційна мережа, доступ до якої відкрито для всіх споживачів [10, 88].

Телекомунікаційна послуга – продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері телекомунікацій [10].

Телекс – телеграма, яку посилають телетайпом [78].

Телемережі – телекомунікаційні мережі загального користування, що призначаються для передавання програм радіо- та телебачення, а також інших телекомунікаційних і мультимедійних послуг і можуть інтегруватися з іншими телекомунікаційними мережами загального користування [10].

Телетайпограма – загальна назва різних за складом документів, переданих телетайпом [78].

Телефонограма – узагальнена назва різних за складом документів, що передають телефоном і записує адресат [78].

Технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації [3]. *Або: **технічний захист секретної інформації*** – діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (або) витоку секретної інформації технічними каналами [88].

Технічний канал витоку інформації – сукупність джерела інформації, середовища її поширення та технічних засобів розвідки [99].

Технічні засоби захисту – технічні пристрої і (або) технологічні розробки, призначені для створення технологічної перешкоди порушенню авторського права і (або) суміжних прав при сприйнятті і (або) копіюванні захищених (закодованих) записів у фонограмах (відеограмах) і передачах організацій мовлення чи для контролю доступу до використання об'єктів авторського права і суміжних прав [14].

Технічні засоби телекомунікацій – обладнання, станційні та лінійні споруди, призначені для утворення телекомунікаційних мереж [10].

Типовий документ – 1) документ, що відображає однорідні питання й укладають за визначеними зразками; 2) нормативний чи розпорядчий документ, що визначає порядок роботи установ або окремих сторін їх діяльності, є зразком для укладання однойменних документів установами з урахуванням специфіки їх діяльності; 3) документ, створений в установі під час виконання функцій, властивих більшості установ, незалежно від їх відомчої належності [78].

Трафарет – тип уніфікованого тексту, що містить постійну інформацію і пропуски, призначені для подальшого заповнення їх змінною інформацією [78].

Указ – акт, що видає чи затверджує найвищий орган влади або Президент держави [78].

Унікальний документ – документ особливої цінності, що не має аналогів за змістом і оформленням [78].

Уповноважена особа – посадова особа, яка наділена правом вчиняти дії та відповідає згідно із законодавством за наслідки їх вчинення [51].

Управлінський документ – службовий документ, спрямований на виконання установою функцій, що забезпечують її діяльність. До управлінських документів належать організаційно-розпорядчі, первинно-облікові, банківські, фінансові, звітно-статистичні, планові, ресурсні тощо [76].

Ухвала – 1) нормативний акт, що приймає місцевий орган виконавчої влади в колегіальному порядку для вирішення найбільш важливих питань його компетенції; 2) спільні акти, що видає декілька неоднорідних органів – колегіальні й такі, що діють на основі єдиноначальності, а також державні органи, громадські організації тощо [78].

Факс – узагальнена назва різноманітних за змістом документів, що за допомогою телекомунікаційного зв'язку та принтера безпосередньо надходять до організації, установи, підприємства [78].

Фальсифікація – підроблення, зміна вигляду або властивостей предмета і надання йому такого зовнішнього вигляду, який не відповідає його справжній суті. Підроблення документів у кримінальному праві – підроблення справжніх або укладання фальшивих документів [78].

Фальсифікована продукція – продукція, виготовлена з порушенням технології або неправомірним використанням знаку для товарів та послуг, чи копіюванням форми, упаковки, зовнішнього оформлення, а так само неправомірним відтворенням товару іншої особи [28].

Фонограма – звукозапис на відповідному носії (магнітній стрічці чи магнітному диску, грамофонній платівці, компакт-диску тощо) виконання або будь-яких звуків, крім звуків у формі запису, що входить до аудіовізуального твору [14].

Фонодокумент – документ, який містить звукову інформацію, зафіксовану будь-якою системою звукозапису [78].

Формати дати – це: 1) короткий; 2) середній; 3) довгий (словесно-цифровий); 4) довгий (словесний); 5) повний; 6) особливий [108].

Формування електронних справ – групування виконаних електронних документів у справи відповідно до номенклатури справ установи [51].

Формуляр – сукупність розміщених у встановленій послідовності реквізитів документа [78].

Фотодокумент – документ, створений фотографічним способом [78].

Характеристика – офіційний документ, в якому дано оцінку ділових і моральних якостей працівника і висновки у зв'язку з цим [78].

Цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення [50].

Юридична особа – установа, організація чи підприємство, що виступають як самостійні носії цивільних прав і обов'язків [78].

ПРЕДМЕТНИЙ ПОКАЖЧИК

- Абонент, 136
Абонентський номер, 136
Автентифікація, 88
Автоматизація оперативно-довідкового обліку, 79
Автоматизована інформаційна система оперативного призначення єдиної інформаційної системи МВС, 11
Автоматизована система документообігу суду, 79
Автоматизоване робоче місце ЄЦВТМ, 79
Автоматизований облік адміністративних правопорушень, 105
Автоматизовані робочі місця користувачів системи «Інформаційний портал Національної поліції України», 105
Автоматизовані робочі місця на веб-порталі Національної академії внутрішніх справ, 11
Автомобільна система технічних приладів і технічних засобів фото- і кінозйомки, відео-, аудіозапису, 126
Автор електронного документа, 136
Авторизація користувача, 79
Авторизація на проведення операцій внесення до безконтактного електронного носія, 79
Адвокат, 136
Адміністратор бази даних центрального вузла АІС ОП, 11
Адміністратор бази даних, 88
Адміністратор безпеки ІПС, 121
Адміністратор безпеки центрального вузла АІС ОП, 12
Адміністратор Єдиного державного реєстру судових рішень, 80
Адміністратор єдиної інформаційної системи МВС, 12
Адміністратор ІПС, 106
Адміністратор Національного реєстру електронних інформаційних ресурсів, 80
Адміністратор системи Інтернет в НПУ, 106
Адміністратор системи ІПНП, 107
Адміністрація Державної служби спеціального зв'язку та захисту інформації України (Адміністрація Держспецзв'язку), 80
Адреса мережі Інтернет, 136
Адресат, 136
Адресний простір мережі Інтернет, 136
АІПС «Канцелярія», 121
АІС ОП, 11
Аналітично-синтетична обробка науково-технічної інформації, 136
АРМ диспетчера ЧЧ Головного управління системи «ЦУНАМІ», 126
АРМ, 11
Архів, 101
Архівна довідка, 101
Архівна копія, 136
Архівна справа, 136
Архівна установа, архів, архівний підрозділ, архівний відділ, 136
Архівний витяг, 137
Архівний документ, 137
Аудіовізуальна інформація, 137
Аудіовізуальний (електронний) засіб масової інформації, 137
Аудіовізуальний документ, 137
Аудіовізуальний твір, 137
АЦСК, 41

База даних, 88
База знань, 88
База персональних даних, 88

Бази даних поліції, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, 13
Бази даних поліції, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, містять відомості, 108
Банк даних, 88
Банки даних інформаційної системи Міжнародної організації кримінальної поліції – Інтерполу, 13
БД, 11
Безконтактний електронний носій, 80
Безпроводовий доступ до телекомунікаційної мережі (безпроводовий доступ), 137
БЕН, 80
Бібліотека, 89
Бібліотека-депозитарій, 137
Бібліотечна система України, 138
Бібліотечний фонд, 89
Бібліотечні ресурси, 89
Біометричні дані, 138
Бланк документа, 138
Бланк електронного документа, 138
Бланк службового документа, 138
Блокування інформації в системі, 138

Веб-клієнт, 138
Веб-сайт, 138
Веб-сервіс, 138
Веб-сторінка, 138
Видалення або знищення персональних даних, 101
Види документів, віднесених до обов'язкового примірника, 138
Види інформації за змістом, 139
Використання інформації, 139
Використання інформаційних ресурсів ІПС, 108
Використання персональних даних, 89

Використання поліцією інформаційних ресурсів, 13
Використання правових інформаційно-пошукових систем в юридичній діяльності дозволяє одержати наступні результати, 14
Вилучення облікових документів з оперативно-довідкових картотек, 81
Вимога, 14
Вимоги (рекомендації) щодо забезпечення захисту секретної інформації, 81
Вимоги до баз даних, 89
Вимоги до запитів до Національного центрального бюро Інтерполу в Україні, 14
Вимоги до захисту в системі інформації від несанкціонованого блокування, 139
Вимоги до оформлення документу на персональному комп'ютері, 139
Вимоги до створення та використання паролю, 108
Вимоги та порядок створення системи захисту, 139
Висновок, 140
Виток інформації, 140
Витяг з документа, 140
Витяг з ЄРДР, 81
Витяг з переліку відомостей, що становлять службову інформацію в системі МВС України, 230
Витяг з переліку відомостей, що становлять службову інформацію в системі Національної поліції України, 232
Витяг, 140
Вихідний документ, 140
Відеограма, 140
Відеореєстратор, 132
Відкритий формат, 89
Віднесення інформації до державної таємниці, 140
Відносини між власниками систем, 140

Відносини між власником системи та користувачем, 140
Відносини між володільцем інформації та власником системи, 140
Відомість, 140
Відомості з Єдиного реєстру досудових розслідувань, 14
Відомості, що не можуть бути розголошені в текстах судових рішень, відкритих для загального доступу, 15
Відомчий акт, 141
Відповідальна особа за актуалізацію та працездатність користувачів системи Інтернет в НПУ, 110
Відповідальність за внесення інформації до ЄРДР, 15
Відповідальність за порушення законодавства про доступ до публічної інформації несуть особи, винні у вчиненні таких порушень, 141
Відповідальність за порушення законодавства про захист інформації в системах, 141
Відповідь на запит щодо отримання інформації державного електронного інформаційного ресурсу, 141
Відстрочення або відмова у доступі до персональних даних, 101
Відтворення, 141
Візуалізація, 141
Візування проекту електронного документа (візування), 141
Вказівка, 141
Власник веб-сайту, 141
Власник веб-сторінки, 142
Власник і розпорядник ЄІС МВС України, 15
Власник ресурсів, 142
Власник системи, 142
Властивості інформації, 142

Властивості полів бази даних системи управління базами даних Microsoft Access, 90
Внесення відомостей до ЄРДР, 15
Внесення інформації в банки даних Генерального секретаріату Інтерполу, 16
Внутрішні користувачі інформаційної системи (бази даних), 90
Внутрішній документ, 142
Володілець інформації Єдиного державного реєстру судових рішень, 16
Володілець інформації, 142
Володілець інформації, що обробляється в центральній підсистемі ЄІС МВС, 16
Володілець персональних даних, 91
Володільцями інформації, що обробляється у функціональних підсистемах ЄІС МВС, 16
ВРУ, 30
Вузол зв'язку єдиної цифрової відомчої телекомунікаційної мережі, 16
Вузол мережі ЄЦВТМ, 16
Вхідний документ, 142

Гарантії права на інформацію забезпечується, 142
Геоінформаційні системи, 142
Гіперпосилання, 143
Голосова телефонія, 143
Графік, 143
Гриф секретності, 143
Група реагування патрульної поліції, 126
ГУНП, 125

Дані, 91
Дата документа, 143
Департамент інформатизації МВС України, 16

Департамент міжнародного поліцейського співробітництва Національної поліції України, 17
Депонування документів, 143
Депонування, 143
Державна архівна установа, 143
Державна підтримка засобів масової інформації, 143
Державна статистика, 144
Державна статистична діяльність, 144
Державна таємниця, 144
Державне зберігання документів, 144
Державний експерт з питань таємниць, 144
Державний засіб масової інформації, 144
Державний реєстр банків, 144
Державні ресурси, 144
Держатель (власник) ІПС, 110
Держатель ЄРДР, 17
Джерела накопичення інформації в НЦБ Інтерполу в Україні, 17
Джерела формування інформаційних ресурсів ІПС, 110
ДЗТ, 106
Диспетчер, 126
Диспетчерський центр управління системи «ЦУНАМІ», 127
ДІАП, 11
Дійсний документ, 144
Діловий лист, 144
Діловодство, 144
Діяльність інформаційних агентств, 144
Для оброблення, передавання, зберігання службової, таємної інформації, персональних даних, а також інформації єдиних та державних електронних реєстрів використовуються, 145
До інформації з обмеженим доступом не можуть бути віднесені такі відомості, 145

Довгий (словесний) формат дати, 145
Довгий (словесно-цифровий) формат дати, 145
Довідка з персонально-довідкового обліку, 18
Довідка, 145
Довідковий апарат, 101
Довідково-інформаційний фонд, 91
Довідково-пошуковий апарат, 91
Дозвіл, 145
Документ вторинний, 146
Документ, 146
Документаційний (документальний) фонд, 146
Документообіг, 146
Документування, 146
Домен другого рівня, 146
Домен, 146
Домен.UA, 146
Доповідна записка, 146
Доповідь, 146
Допуск до державної таємниці, 146
Доручення, 147
Доступ до відкритої інформації ЄІС МВС, 18
Доступ до відомостей, внесених до ЄРДР, 18
Доступ до державної таємниці, 147
Доступ до інформації в системі, 147
Доступ до інформації забезпечується шляхом, 147
Доступ до інформації про особу, 147
Доступ до інформації, 147
Доступ до інформаційних ресурсів ІПС, 110
Доступ уповноважених працівників до сервісів ЄІС МВС, 18
Доступ фізичної особи до інформації про себе, що обробляється в ЄІС МВС, 19
Доступність, 147
Досудове розслідування, 148
Досудове слідство, 148
Досьє, 148

Друковані засоби масової інформації (преса) в Україні, 148
ДСА, 16
Дублікат, 148

Електронна (цифрова) інформація, 148
Електронна адреса суб'єкта владних повноважень, 19
Електронна ідентифікація, 148
Електронна копія електронного документа, 148
Електронна копія оригіналу паперового документа (фотокопія), 148
Електронна печатка, 149
Електронна послуга, 149
Електронна резолюція, 149
Електронна справа, 149
Електронне повідомлення, 149
Електронне повідомлення, 149
Електронне урядування, 149
Електронний аудіовізуальний документ, 149
Електронний внутрішній опис документів справи, 149
Електронний довідник, 101
Електронний документ, 149
Електронний документообіг (обіг електронних документів), 150
Електронний документообіг установи, 150
Електронний журнал, 150
Електронний кабінет, 19
Електронний підпис, 150
Електронний підручник (посібник), 150
Електронний примірник судового рішення, 19
Електронний цифровий підпис, 19
Електронні дані, 91
ЕОТ, 150
Етапи проектування бази даних в СУБД Microsoft Access, 91
Етапи функціонування ІПС, 151

Ефективне функціонування ЄІС МВС, 19
Ефективність технічного захисту секретної інформації, 82
ЕЦП, 19

Єдина база даних електронних адрес, номерів факсів (телефаксів) суб'єктів владних повноважень, 20
Єдина звітність про кримінальні правопорушення, осіб, які їх учинили, та рух кримінальних проваджень відповідно до ЄРДР, 20
Єдина інформаційна система МВС, 20
Єдиний державний веб-портал відкритих даних, 21
Єдиний державний реєстр судових рішень, 21
Єдиний облік, 22
Єдиний реєстр досудових розслідувань, 22
ЄДР, 81
ЄДРПОУ, 151
ЄДРСР, 16
ЄІС, 11
ЄРДР, 14
ЄЦВТМ, 16
ЄЦВТМ, 22

Журнал, 151

За порядком доступу інформація поділяється, 151
Забезпечення захисту інформації в системі, 151
Забезпечення інформаційної безпеки національних ресурсів, 151
Завдання ЄІС МВС, 23
Завдання ІПС, 111
Завдання ОРД, 151
Завдання системи інформаційного забезпечення органів Національної поліції, 23

Загальна характеристика банків даних Генерального секретаріату Інтерполу, 24
Загальний доступ до судових рішень, 24
Загальні вимоги до обробки персональних даних, 91
Загроза для секретної інформації, 82
Зал оперативного управління чергової служби, 127
Замовник і утримувач Національного реєстру електронних інформаційних ресурсів, 25
Запис (звукозапис, відеозапис), 151
Запис, 151
Записка, 151
Запит щодо отримання інформації державного електронного інформаційного ресурсу, 152
Засекречування матеріальних носіїв інформації, 152
Засіб електронного підпису чи печатки, 152
Засіб електронної ідентифікації, 152
Засоби дистанційного зв'язку, 152
Засоби інформатизації, 152
Засоби комунікації, 152
Засоби криптографічного захисту інформації, 82
Засоби масової інформації, 152
Засоби передавання інформації в ЄЦВТМ, 25
Захист відкритої інформації, 152
Захист відомостей, внесених до ЄРДР, 25
Захист інформації в НЦБ Інтерполу в Україні, 25
Захист інформації в системі, 153
Захист інформації, 153
Захист інформації, внесеної до Єдиного державного реєстру судових рішень, 26
Захист інформаційних ресурсів ІПС, 121

Захист особи, яка оприлюднює інформацію, 153
Захист службової і таємної інформації, 153
Захисту в системі підлягає, 153
Захищений носій особистих ключів, 153
Заява, 153
Заявникові відмовляється в наданні відомостей з персонально-довідкового обліку в разі, якщо, 26
Зберігання інформації, 154
Зберігання інформаційних ресурсів ЄІС МВС, що створені в системі МВС, 26
Зберігання інформаційних ресурсів інших суб'єктів ЄІС МВС, 26
Зберігання персональних даних, 92
Збирання персональних даних, 92
Зведення, 154
Звернення громадян, 154
Звід відомостей, що становлять державну таємницю, 154
Звіт, 154
Згода суб'єкта персональних даних, 92
Здійснення заходів з легалізації комп'ютерних програм, 154
Злочин, 154
Зміни і доповнення до персональних даних, 102
Зміст Національного реєстру електронних інформаційних ресурсів, 27
Знеособлення персональних даних, 92
Знеособлення, 27
Знищення інформації в системі, 154
Зобов'язання користувачів ЄІС МВС, 27
Зобов'язання працівників органів виконавчої влади, що використовують у своїй діяльності комп'ютерні програми, 154

Зона оперативного реагування
наряду поліції, 127

Ідентифікаційні дані особи, 154

Ідентифікація особи, 93

Ідентифікація, 93

Ієрархічна модель даних, 93

ІПС, 55

Інвентаризація комп'ютерних
програм, 155

Інструкція про порядок
використання правоохоронними
органами можливостей НЦБ

Інтерполу в Україні у попередженні,
розкритті та розслідуванні злочинів,
27

Інструкція про порядок запису та
збереження в цифровому вигляді
заяв і повідомлень, які надходять за
телефоном «102», або за допомогою
інших засобів зв'язку до
Національної поліції України, 132

Інструкція, 155

Інтеграція інформаційних ресурсів

ЄІС МВС, 27

Інтегрована інформаційно-пошукова
система МВС України, 111

Інтернет, 155

Інтероперабельність, 155

Інтерфейс прикладного
програмування відкритих даних, 28

Інтерфейс прикладного
програмування, 102

Інформатизація, 155

Інформаційна (автоматизована)
система, 93

Інформаційна безпека
телекомунікаційних мереж, 155

Інформаційна довідка про
правопорушення або подію, 132

Інформаційна послуга, 155

Інформаційна продукція, 155

Інформаційна система загального
доступу, 93

Інформаційна система органів
державної статистики, 155

Інформаційна система, 93

Інформаційна служба МВС України,
28

Інформаційна служба Національної
поліції України, 28

Інформаційна технологія, 155

Інформаційне забезпечення ІПС
базується, 112

Інформаційний обмін, 156

Інформаційний продукт (продукція),
156

Інформаційний ресурс, 94

Інформаційний ринок, 156

Інформаційний суверенітет держави,
156

Інформаційні агентства, 156

Інформаційні ресурси (об'єкти
обліку) ІПС, 112

Інформаційні ресурси АІС ОП, 29

Інформаційні ресурси Єдиного
державного реєстру судових рішень,
29

Інформаційні ресурси єдиної
інформаційної системи МВС, 29

Інформаційні ресурси науково-
технічної інформації, 94

Інформаційні ресурси системи
«Інформаційний портал
Національної поліції України», 112

Інформаційні ресурси спільного
користування, 94

Інформаційно-пошукова система
«Законодавство України», 30

Інформаційно-правові системи
«Ліга: Закон», 30

Інформаційно-телекомунікаційна
система «Інформаційний портал
Національної поліції України», 112

Інформаційно-телекомунікаційна
система Інтерполу I-24/7, 30

Інформаційно-телекомунікаційна
система, 156

Інформація довідково-енциклопедичного характеру, 156
 Інформація експертно-криміналістичних обліків, 31
 Інформація з обмеженим доступом, 156
 Інформація оперативних обліків, 31
 Інформація письмова, 157
 Інформація про особисте та сімейне життя особи (персональні дані про неї), 102
 Інформація про стан довкілля (екологічна інформація), 157
 Інформація про товар (роботу, послугу), 157
 Інформація про фізичну особу (персональні дані), 94
 Інформація, 156
 Інформація, що вводиться в оману, 157
 Інцидент кібербезпеки, 157
 ІПНП, 105
 ІПС, 50
 ІС, 13
 ІТ, 13

Канал електров'язку, 158
 Карта пам'яті або флеш-карта, 132
 Картка обліку комп'ютерної програми, 158
 Картотека особового складу, 94
 Картотека, 94
 Каталог документів, 95
 Категорія режиму секретності, 158
 Кваліфікація порушень ТЗІ, 82
 Кваліфіковані електронні довірчі послуги, 158
 Кегль, 158
 Кібератака, 158
 Кібербезпека, 158
 Кіберзагроза, 159
 Кіберзахист, 159
 Кіберзлочин (комп'ютерний злочин), 159
 Кіберзлочинність, 159
 Кіберпростір, 159

Кіберрозвідка, 159
 Кібертероризм, 159
 Кібершипінгство, 159
 Кінозйомка та відеозапис, 132
 Кінцеве обладнання, 159
 Кінцеві користувачі, 95
 Класифікація інформаційних систем, 95
 Класифікація інформаційно-пошукових систем в залежності від режиму організації пошуку, 95
 Класифікація основних видів обліків Міністерства внутрішніх справ України та Національної поліції, 31
 Класифікація правових інформаційних систем, 95
 Ключ, 96
 Ключові слова, 159
 КМУ, 16
 Кодекс, 159
 Комп'ютерна програма, 159
 Комплекс технічного захисту інформації, 159
 Комплекс технічного захисту інформації, 82
 Комплексна система захисту інформації системи ІПНП з підтвердженою відповідністю, 113
 Комплексна система захисту інформації, 160
 Комплексні системи захисту інформації, 31
 Контрафактний примірник твору, фонограми, відеограми, 160
 Контроль за використанням технічних приладів і технічних засобів, що мають функцію фото- і кінозйомки, відеозапису, 132
 Контроль за станом технічного захисту інформації в органах і підрозділах НПУ, 82
 Контроль та нагляд за внесенням інформації до ЄРДР, 32
 Контрольно-інспекторська робота з питань ТЗІ, 83

Конфіденційна інформація, 160
 Конфіденційність, 161
 Копія документа, 161
 Користувач архівними документами, 161
 Користувач бібліотеки, 161
 Користувач інформації в системі, 96
 Користувач системи Інтернет в НПУ, 113
 Користувачі АІС ОП, 32
 Користувачі електронних довірчих послуг, 161
 Користувачі ЄІС МВС, 32
 Користувачі ЄРДР, 32
 Користувачі ЄЦВТМ, 33
 Користувачі ІПС, 114
 Користувачі інформаційної системи (бази даних), 96
 Користувачі робочого місця віддаленого доступу до персонально-довідкового обліку, 33
 Користувачі системи ІПНП, 114
 Короткий (цифровий) формат дати, 161
 КП, 144
 КПК, 14
 Кримінальне провадження, 161
 Криптографічна система, 83
 Криптографічний захист інформації, 161
 Криптографічний захист інформації, 83
 Критична інформаційна інфраструктура, 161
 Критично важливі об'єкти інфраструктури, 161
 КСЗІ з підтвердженою відповідністю, 83
 КСЗІ, 31
 КУпАП, 118
 Легалізація комп'ютерних програм в органах виконавчої влади, 162
 Легенда, 162
 Лист, 162
 Ліцензійна комп'ютерна програма, 162
 Ліцензія на використання комп'ютерної програми, 162
 Ліцензія, 162
 Ліцензування, 162
 Локалізація програмних продуктів, 162
 Макет документа, 162
 Масова інформація, 162
 Матеріальні носії секретної інформації, 162
 Машиночитаний формат, 96
 МВС відповідно до покладених на нього завдань, 33
 МВС для виконання покладених на нього завдань має право, 34
 МВС, 8
 Мережева модель даних, 96
 Мережеве обладнання ЄЦВТМ, 83
 Мета ведення ЄРДР, 34
 Мета ведення Національного реєстру електронних інформаційних ресурсів, 34
 Мета застосування працівниками поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, 128
 Мета Концепції розвитку електронного урядування в Україні, 163
 Мета обробки інформації у функціональних підсистемах єдиної інформаційної системи МВС, 34
 Мета системи інформаційного забезпечення органів Національної поліції, 34
 Мета створення ЄЦВТМ, 35
 Мета створення ІПС, 114
 Мета створення системи «ЦУНАМІ», 128
 Мета функціонування єдиної інформаційної системи МВС, 35
 Метадані, 96

Мова діловодства в системі
Національної поліції України, 163
Мова інформації, 163
Монопольний (домінуючий)
оператор телекомунікацій, 163

На сторінці кожного набору даних
на Єдиному державному веб-порталі
відкритих даних розміщується, 35
На сторінці кожного набору даних,
що оприлюднюється, розпорядник
інформації розміщує таку
інформацію, 36
Набір даних, 96
НАВС, 8
Надання відомостей з ЄРДР, 36
Надання інформації з персонально-
довідкового обліку, 36
Найбільш відомі на українському
ринку правові ІПС, 163
Найбільш поширені в Україні
автоматизовані системи
документообігу, 163
Наказ, 163
Накопичення персональних даних,
96
Направлення запитів до оперативно-
довідкового і дактилоскопічного
обліків та їх одержання, 36
Наукова (науково-технічна)
продукція, 164
Науковий (науково-технічний)
проект, 164
Науково-інформаційна діяльність,
164
Науково-технічна діяльність, 164
Науково-технічна інформація, 164
Національна поліція відповідно до
покладених на неї завдань, 37
Національна поліція для виконання
покладених на неї завдань має право,
37
Національна поліція України, 38
Національна система
конфіденційного зв'язку, 164

Національна телекомунікаційна
мережа, 164
Національне центральне бюро
Інтерполу в Україні, 38
Національний архівний фонд, 165
Національний аудіовізуальний
продукт, 165
Національний інформаційний фонд
України, 102
Національний реєстр електронних
інформаційних ресурсів, 38
Національні електронні
інформаційні ресурси, 102
Національні ресурси не повинні
містити, 103
Національні ресурси, 103
Неавторизований користувач, 83
Недержавні ресурси, 103
Неліцензійна комп'ютерна
програма, 165
Неправомірне збирання комерційної
таємниці, 165
Несанкціоновані дії щодо інформації
в системі, 103
Несанкціоновані дії, 103
Номенклатура справ, 165
Нормативний документ, 165
Нотаріус, 165
НПА, 29
НПУ, 11
НЦБ Інтерполу України відмовляє
повністю або частково у виконанні
запитів, 38
НЦБ, 14

Об'єкт інформаційних відносин, 166
Об'єкт інформаційної діяльності, 83
Об'єкт критичної інформаційної
інфраструктури, 166
Об'єкт телекомунікацій, 84
Об'єкти бази даних Microsoft Access,
97
Об'єкти захисту в системі, 166
Об'єкти оперативно-довідкового і
дактилоскопічного обліків, 39

Обліковий запис, 166

Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог, 166

Обов'язки працівника поліції, пов'язані із застосуванням технічних приладів і технічних засобів фото- і кінозйомки, відеозапису, 128

Обов'язки технічного спеціаліста щодо обслуговування реєстратора мовленнєвої інформації, 132

Обов'язковий примірник документів, 166

Обов'язковий реквізит електронного документа, 166

Образ електронного примірника судового рішення або окремої думки судді, 84

Обробка інформації в системі, 166

Обробка персональних даних, 97

Обсяг документообігу, 166

Огляд, 167

Оголошення, 167

Одержання інформації, 167

Одержувач обов'язкового примірника документів, 167

Одержувач, 97

Он-лайн будинок юстиції, 39

Оновлення комп'ютерної програми, 167

Оперативне інформування, 129

Оперативне реагування, 129

Оперативний черговий, 129

Оперативно-розшукова діяльність, 167

Оператор служби «102», 129

Оператор телекомунікацій, 167

Оператор, провайдер телекомунікацій з істотною ринковою перевагою на ринку телекомунікаційних послуг, 167

Опис документів, 167

Опис справ в електронній формі, 167

Опис, 167

Опитувана особа на поліграфі, 121

Опитування з використанням поліграфа, 122

Оприлюднення набору даних, 97

Організаційна структура системи національних ресурсів, 168

Організаційно-розпорядча документація, 168

Організація проведення перевірок стану ТЗІ, 84

Організація роботи зі службовими документами, 168

ОРД, 11

Оригінал документа, 168

Оригінал електронного документа, 168

Оригінал службового документа, 168

Основним завданням взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України, 39

Основні види інформаційної діяльності, 168

Основні види продукції інформаційних агентств, 169

Основні властивості баз даних, 98

Основні завдання «Національної суспільної телерадіокомпанії України», 169

Основні завдання Адміністрації Держспецзв'язку, 84

Основні завдання АІС ОП, 40

Основні завдання Департаменту інформатизації МВС України, 40

Основні завдання для забезпечення формування системи національних ресурсів, 169

Основні завдання єдиної цифрової відомчої телекомунікаційної мережі МВС, 43

Основні завдання системи «Інформаційний портал Національної поліції України», 114

Основні напрями державної інформаційної політики, 169

Основні принципи використання поліграфа, 122
Основні принципи електронного документообігу, 170
Основні принципи інформаційних відносин, 170
Основні функції територіального сервісного центру МВС, 44
Особиста картка, 170
Особистий архівний документ, 170
Особистий документ, 170
Особливий формат дати, 170
Особова справа, 170
Отримання відомостей з персонально-довідкового обліку за запитами органів державної влади та їх територіальних органів, органів місцевого самоврядування, установ та організацій, у зв'язку зі здійсненням ними повноважень, визначених законодавством, 44
Отримання відомостей з персонально-довідкового обліку за зверненнями державних органів, які здійснюють правоохоронні функції, 45
Отримання відомостей з персонально-довідкового обліку за зверненнями судів усіх рівнів, 46
Отримання відомостей з персонально-довідкового обліку за зверненнями фізичних осіб, 46
Отримання інформації або перевірка тих чи інших відомостей за банками даних Інтерполу, 48
Отримувач, 170
Офіційний документ, 170
Офіційні веб-портали вищих державних органів України, 170
Офіційні веб-портали вищих навчальних закладів МВС України, 171
Офіційні веб-портали міністерств України, 171

Офіційні веб-портали підпорядкованих органів МВС України, 172
Офіційні веб-портали різних інших органів України, 172
Оформлення офіційного документа, 172
Охорона державної таємниці, 173
Охорона права на інформацію, 173

Паперова копія оригіналу електронного документа, 173
Паспорт набору даних повинен містити такі елементи, 49
Паспорт набору даних, 98
Паспорти на алфавітні та дактилоскопічні картотеки, 49
Патентні документи, 173
ПД, 48
ПЕОМ, 173
Первинний документ, 173
Перевірка за дактилоскопічними картотеками, 49
Перевірка наявності вже розпочатих досудових розслідувань, 50
Перевірка осіб за оперативно-довідковим обліком працівниками правоохоронних органів, 50
Перевірка стану документів, 173
Передавання даних, 173
Перелік автоматизованих систем інформаційно-технологічного забезпечення діяльності Верховної Ради України, 50
Перелік баз даних Інтегрованої інформаційно-пошукової системи МВС України, 115
Перелік основних наборів даних, які підлягають оприлюдненню у формі відкритих даних, 223
Перелік інформації, що подається до Міждержавного інформаційного банку, 51

Перелік корисних відкритих реєстрів та баз даних України, 227

Перелік пріоритетних інформаційних ресурсів єдиної інформаційної системи МВС України, 220

Перенесення абонентського номера, 173

Періодичність оновлення наборів даних, 52

Персональний номер, 173

Персональні дані, 98

Персонально-довідковий облік єдиної інформаційної системи МВС України, 53

Персонально-довідковий облік, 52

Першочергові проблеми розвитку електронного урядування в Україні, 174

Письмовий документ, 174

Під час приймання та реєстрації заяв та повідомлень про правопорушення або події, організації оперативного реагування на них працівникам підрозділу «102», диспетчерам, старшим зміни працівникам підрозділу «102» та диспетчерам, працівникам чергової служби НПУ забороняється, 129

Підзаконний акт, 174

Підписання проекту електронного документа, 174

Підрозділ «102», 130

Підрозділи документального забезпечення, 174

Підсистема «Мігрант», 53

Підсистема «Рубін-2002», 53

Підсистеми у структурі ЄЦВТМ, 53

Підстави для обробки персональних даних, 98

Підходи, якими керується МВС щодо забезпечення реалізації цілей Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року, 54

План захисту інформації в системі, 175

План, 175

Планова інвентаризація комп'ютерних програм, 175

Повідомлення, 175

Повний доступ до судових рішень, 85

Повний формат дати, 175

Повноваження державних органів у сфері захисту інформації в системах, 175

Повноваження МВС щодо функціонування єдиної інформаційної системи МВС, 54

Повноваження поліції у сфері інформаційно-аналітичного забезпечення, 54

Погоджувач, 176

Подання, 176

Податкова інформація, 176

Позапланова інвентаризація комп'ютерних програм, 176

Поліграф, 122

Поліція забезпечує збирання, накопичення мультимедійної інформації та біометричних даних, 54

Положення про систему Інтернет у телекомунікаційній мережі

Національної поліції України, 115

Положення, 176

Портативний відеореєстратор, 130

Порушення у сфері ТЗІ, 85

Порушення цілісності інформації в системі, 176

Порядок взаємодії Генеральної прокуратури України та

Міністерства внутрішніх справ

України щодо обміну інформацією з

Єдиного реєстру досудових розслідувань та інформаційних систем МВС, 55

Порядок взаємодії Міністерства внутрішніх справ України з центральними органами виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України, 56

Порядок видачі для прослуховування та знищення записаної мовленнєвої інформації на реєстратор, 133

Порядок використання безконтактного електронного носія, який імплантовано в паспорт громадянина України, 85

Порядок внесення відомостей до ЄРДР, 57

Порядок дій органів (підрозділів) Національної поліції в разі виявлення осіб, транспортних засобів і документів, відомості щодо яких містяться в банках даних інформаційної системи Міжнародної організації кримінальної поліції – Інтерполу, 57

Порядок доступу до інформації в системі, 176

Порядок обліку та зберігання записаної мовленнєвої інформації на реєстратор, 133

Порядок оголошення в Україні в розшук Інтерполу, 58

Порядок отримання доступу до системи Інтернет в НПУ, 115

Порядок проведення перевірок стану ТЗІ, 85

Порядок складання та подання запитів на отримання публічної інформації, розпорядником якої є Національна поліція України, 116

Послуга, 176

Послуги системи Інтернет в НПУ, 117

Постанова, 176

Постачальник послуг хостингу, 176

Постачальник, 176

Постійний реквізит документа, 176

Потреба органів виконавчої влади в комп'ютерних програмах, 177

Поширення інформації, 177

Поширення персональних даних, 103

Пошукові реквізити документа, 177

Пояснювальна записка, 177

Права Департаменту інформатизації МВС України, 59

Права керівника підрозділу інформаційних технологій щодо використання комп'ютерних програм, 177

Права підрозділу інформаційних технологій щодо обліку комп'ютерних програм, 177

Права працівників органів виконавчої влади, що використовують у своїй діяльності комп'ютерні програми, 178

Правила, 178

Право на інформацію, 178

Правова інформаційна система, 98

Правова інформація, 178

Правовий статус, 178

Правовласник, 178

Працівникам картотек забороняється, 86

Предметний каталог, 178

Предметний покажчик, 178

Приватні ресурси, 103

Призначення системи ІПНП, 117

Прийняття заяв і повідомлень про вчинені кримінальні правопорушення та інші події, 130

Приклади інформаційно-довідкових обліків експертно-криміналістичного призначення, 60

Приклади оперативних обліків, 60

Приклади оперативно-пошукових обліків експертно-криміналістичного призначення, 60

Прикладні програмісти, 98
Примірник відеограми, 179
Примірник електронного документа, 179
Примірник твору, 179
Примірник фонограми, 179
Принципи оприлюднення наборів даних у формі відкритих даних, 98
Принципи формування загальновідомчих та галузевих інформаційних підсистем, які складають основу системи інформаційного забезпечення органів Національної поліції, 60
Принципи формування та вимоги до змісту національних ресурсів, 179
Припинення існування е-ресурсу, включеного до Національного реєстру електронних інформаційних ресурсів, 86
Притягнення до кримінальної відповідальності, 179
Прихована реклама, 179
Пріоритетні напрями формування системи національних ресурсів, 179
Провайдер телекомунікацій, 179
Проводовий електрозв'язок, 179
Програма, 179
Програмно-технічний комплекс, що використовується під час надання електронних довірчих послуг, 180
Продукція інформаційного агентства, 180
Проект документа, 180
Проект електронного документа, 180
Пропозиція, 180
Протокол, 180
Публічна інформація у формі відкритих даних, 180
Публічна інформація, 180
Публічна інформація, що містить персональні дані фізичної особи, оприлюднюється та надається на запит у формі відкритих даних у разі додержання однієї з таких умов, 99

Рапорт, 180
Реалізація державної політики у сфері державних ресурсів полягає у розв'язанні таких завдань, 181
Реалізація державної політики у сфері недержавних ресурсів полягає у розв'язанні таких завдань, 181
Реалізація Концепції розвитку електронного урядування в Україні здійснюється за такими основними принципами, 181
Редакційна правка, 182
Реєстр оприлюднених наборів даних, 60
Реєстр ресурсів, 103
Реєстр, 182
Реєстратор, 182
Реєстратори ЄРДР, 61
Реєстраційна картка, 182
Реєстраційно-моніторингова картка, 182
Реєстрація документів, 182
Реєстрація е-ресурсу в Національному реєстрі електронних інформаційних ресурсів, 86
Реєстрація заяв і повідомлень про вчинені кримінальні правопорушення та інші події, 61
Реєстрація події, 130
Реєстри веб-порталу Міністерства юстиції України, 61
Режим секретності, 182
Результати навчання, 182
Реквізит документа, 182
Реквізит електронного документа, 182
Реквізит службового документа, 182
Реклама, 182
Реляційна модель даних, 99
Репродукція документа, 183
Рівні доступу для отримання інформації від НЦБ Інтерполу в Україні, 62
Рішення, 183

Робоче місце віддаленого доступу до персонально-довідкового обліку, 62
 Розголошення комерційної таємниці, 183
 Розмноження документів, 183
 Розпорядження, 183
 Розпорядник АІС ОП, 62
 Розпорядник ІПС, 117
 Розпорядник інформації, яка обробляється в АІС ОП, 62
 Розпорядник персональних даних, 99
 Розпорядник системи ІПП, 118
 Розсекречування матеріальних носіїв секретної інформації, 183
 Розшукові обліки на веб-порталі МВС України, 62
 Роумінг національний, 183
 РСО, 183
 Рухомий (мобільний) зв'язок, 183

Свідоцтво, 183
 Сегмент ЄЦВТМ, 86
 Сектор реагування патрульної поліції, 130
 Сервер для зберігання відеозаписів, 133
 Сервер ЄЦВТМ, 87
 Сервіс єдиної інформаційної системи МВС, 63
 Середній формат дати, 183
 Система «ЦУНАМІ», 130
 Система електронного документообігу установи, 183
 Система Інтернет в НПУ, 118
 Система інформаційного забезпечення органів Національної поліції, 63
 Система моніторингу, 184
 Система національних ресурсів, 104
 Система обов'язкового примірника документів, 184
 Система управління базами даних, 99
 Системи «Ліга: Закон», 184

Системи електронних комунікацій, 184
 Системний адміністратор центрального вузла АІС ОП, 63
 Системні програмісти, 100
 Скарга, 184
 Склад ЄЦВТМ, 87
 Склад інформаційних ресурсів (об'єктів обліку) ІПС, 118
 Склад Національного реєстру електронних інформаційних ресурсів, 64
 Склад Національної системи конфіденційного зв'язку, 184
 Склад регіонального вузла АІС ОП, 64
 Склад регіонального вузла ІПС, 123
 Склад територіального вузла ІПС, 123
 Склад центрального вузла АІС ОП, 65
 Склад центрального вузла ІПС, 124
 Склад центрального програмно-технічного комплексу системи ІПП, 124
 Склад центральної підсистеми єдиної інформаційної системи МВС, 65
 Слідчо-оперативна група, 133
 Служба діловодства, 184
 Служба єдиної інформаційної системи МВС, 66
 Служба захисту інформації, 185
 Служба, 56
 Службова електронна пошта, 185
 Службова записка, 185
 Службова інформація, 185
 Службовий документ, 133
 Службовий документ, 185
 Службовий електронний документ, 134
 Службовий електронний документ, 185
 Службовий твір, 185
 Соціологічна інформація, 186

Спеціальна телекомунікаційна система (мережа) подвійного призначення, 186
 Спеціальна телекомунікаційна система (мережа), 186
 Список, 186
 Споживач телекомунікаційних послуг (споживач), 186
 Справа, 186
 Сталість телекомунікаційної мережі, 186
 Станція для заряджання та зберігання відеозаписів портативних відеореєстраторів, 134
 Статистична інформація, 186
 Статистична методологія, 186
 Статистичне спостереження, 186
 Стационарна система технічних приладів і технічних засобів фото- і кінозйомки, відеозапису, 134
 Стенограма, 187
 Стратегічні пріоритети розвитку органів системи МВС на період до 2020 року, 67
 Стратегія формування системи ресурсів органів державної влади, 187
 Страхова копія документа, 187
 Страховий фонд копій документів, 187
 Строк (термін) придатності, 187
 Строк зберігання відеозаписів, 134
 Строк зберігання документа, 187
 Строк зберігання електронного документа, 187
 Строк розгляду запитів на інформацію, 187
 Строк служби, 188
 Строки зберігання інформації, порядок видалення та знищення інформації в єдиній інформаційній системі МВС, 68
 Структура АІС ОП, 69
 Структура єдиної інформаційної системи МВС, 69
 Структура ЄЦВТМ, 69
 Структура ІПС, 119
 Структура набору даних, 100
 Структура системи ІПНП, 119
 Структура та порядок роботи функціональних підсистем єдиної інформаційної системи МВС, 69
 Ступінь секретності («особливої важливості», «цілком таємно», «таємно»), 188
 Суб'єкт владних повноважень, 188
 Суб'єкт персональних даних, 100
 Суб'єкти АІС ОП, 69
 Суб'єкти відносин, пов'язаних із захистом інформації в системах, 188
 Суб'єкти відносин, пов'язаних із персональними даними, 104
 Суб'єкти електронного документообігу, 188
 Суб'єкти єдиної інформаційної системи МВС, 70
 Суб'єкти інформаційних відносин, 188
 Суб'єкти Національної системи конфіденційного зв'язку, 188
 Суб'єкти правових відносин ІПС, 120
 Суб'єкти ринку телекомунікацій, 188
 Суб'єкти системи ІПНП, 120
 СУБД, 90
 Судове рішення, 188
 Суспільно необхідні видання, 188
 Схема електронної ідентифікації, 189
 Схиленням до розголошення комерційної таємниці, 189
 Табель, 189
 Таблиця, 189
 Таємна інформація, 189
 Таємний архів, 189
 Тезаурус, 189
 Тези, 189
 Телебачення (телемовлення), 189

Телеграма, 189
 Телекомунікації (електров'язок), 125
 Телекомунікаційна мережа доступу системи ІПНП, 120
 Телекомунікаційна мережа доступу, 189
 Телекомунікаційна мережа загального користування, 189
 Телекомунікаційна мережа, 125
 Телекомунікаційна послуга, 189
 Телекомунікаційна система
 Інтерполу I-24/7, 70
 Телекомунікаційна система, 125
 Телекс, 190
 Телемережі, 190
 Телетайпограма, 190
 Телефонограма, 190
 Територіальний сервісний центр МВС, 71
 Терміни виконання запитів до оперативно-довідкового і дактилоскопічного обліків, 72
 Терміни виконання запитів, одержаних правоохоронними органами України з НЦБ Інтерполу в Україні, 72
 Терміни зберігання облікових документів в дактилоскопічних картотеках, 72
 Терміни зберігання облікових документів в оперативно-довідкових картотеках (банках даних), 73
 Термінологічний словник законодавства України інформаційно-пошукової системи «Законодавство України», 73
 Технічний захист інформації, 87
 Технічний захист секретної інформації, 190
 Технічний канал витоку інформації, 190
 Технічний спеціаліст, 134
 Технічні засоби захисту, 190
 Технічні засоби телекомунікацій, 190
 Технології Інтерполу, 73
 ТЗІ, 81
 Типи даних (типи полів таблиць) СУБД Microsoft Access, 100
 Типовий документ, 190
 Транспортна мережа передачі даних, 125
 Транспортна телекомунікаційна мережа, 125
 Трафарет, 190
 Трафік, 125
 Третя особа, 100
 ТСЦ, 33
 УІАП, 11
 Указ, 190
 Умови обробки інформації в системі, 87
 Унікальний документ, 190
 УОАЗОР, 128
 Уповноважена особа, 134
 Уповноважена особа, 190
 Управлінська інформація, 134
 Управлінське рішення, 134
 Управлінський документ, 191
 УРТЗІ, 82
 Установчі дані фізичної особи, 74
 Ухвала, 191
 Факс, 191
 Фальсифікація, 191
 Фальсифікована продукція, 191
 Фонограма, 135
 Фонограма, 191
 Фонодокумент, 135
 Фонодокумент, 191
 Формати дати, 191
 Формати для оприлюднення наборів даних, 104

Форми документів, що використовуються для формування та коригування оперативно-довідкового і дактилоскопічного обліків (банків даних), 74
Формуванню, використанню та захисту недержавних ресурсів сприятиме, 87
Формування банків даних НЦБ Інтерполу в Україні, 74
Формування електронних справ, 191
Формування інформаційних ресурсів поліцією, 74
Формуляр, 191
Фотодокумент, 191
Функції Microsoft Access, 100
Функції АІС ОП, 75
Функції єдиної інформаційної системи МВС, 75
Функції ЄЦВТМ, 75
Функціональними підсистемами єдиної інформаційної системи МВС, 77
Функціональні підсистеми єдиної інформаційної системи МВС, 77

Характеристика, 191

Центр прийняття повідомлень системи «ЦУНАМІ», 131
Централізована бібліотечна система, 104
Центральна підсистема єдиної інформаційної системи МВС, 77
Центральний вузол доступу системи Інтернет в НПУ, 120
Центральний програмно-технічний комплекс системи ПНП, 120

Цифровий багатоканальний реєстратор мовленнєвої інформації з вмонтованим автоматичним визначником номерів телефонів та таксофонів, 135
Цілі Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року, 77
Цілісність, 191
ЦОВВ, 16
ЦУНАМІ, 127

Частина 1 статті 3 Конституції України, 78
Частина 1 статті 31 Конституції України, 78
Частина 2 статті 19 Конституції України, 78
Частина 2 статті 3 Конституції України, 78
Частина 2 статті 32 Конституції України, 78
Частина 3 статті 32 Конституції України, 78
Частина 4 статті 32 Конституції України, 78
Чергова служба, 135
ЧЧ, 76

Шляхи досягнення мети Концепції розвитку електронного урядування в Україні, 87

Юридична особа, 191

Microsoft Access, 100

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Закони України:

Основна:

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
2. Про внесення змін до Закону України «Про інформацію» : Закон України від 13 січ. 2011 р. № 2938-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 313.
3. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93.
4. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314.
5. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05 лип. 1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.
6. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481.
7. Про звернення громадян : Закон України від 02 жовт. 1996 р. № 393/96-ВР // Відомості Верховної Ради УРСР. – 1996. – № 47. – Ст. 256.
8. Про Національну поліцію : Закон України від 02 лип. 2015 р. № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40-41. – Ст. 379.
9. Про Національну програму інформатизації : Закон України від 04 лют. 1998 р. № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28. – Ст. 181.
10. Про телекомунікації : Закон України від 18 листоп. 2003 р. № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – ст. 155.

Додаткова:

11. Кодекс України про адміністративні правопорушення від 07 груд. 1984 р. № 80731-X.
12. Кримінальний кодекс України від 05 квіт. 2001 р. № 2341-III.
13. Кримінальний процесуальний кодекс України від 13 квіт. 2012 р. № 4651-VI.
14. Про авторське право і суміжні права : Закон України від 23 груд. 1993 р. № 3792-XII // Відомості Верховної Ради України. – 1994. – № 13. – Ст. 64.
15. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.
16. Про адвокатуру та адвокатську діяльність : Закон України від 05 лип. 2012 р. № 5076-VI // Відомості Верховної Ради України. – 2013. – № 27. – Ст. 282.
17. Про банки і банківську діяльність : Закон України від 07 груд. 2000 р. № 2121-III // Відомості Верховної Ради України. – 2001. – № 5-6. – Ст. 30.

18. Про бібліотеки і бібліотечну справу : Закон України від 27 січ. 1995 р. № 32/95-ВР // Відомості Верховної Ради України. – 1995. – № 7. – Ст. 45.

19. Про видавничу справу : Закон України від 05 черв. 1997 р. № 318/97-ВР // Відомості Верховної Ради України. – 1997. – № 32. – Ст. 206.

20. Про вищу освіту : Закон України від 01 лип. 2014 р. № 1556-VII // Відомості Верховної Ради України. – 2014. – № 37-38. – Ст. 2004.

21. Про державну підтримку засобів масової інформації та соціальний захист журналістів : Закон України від 23 верес. 1997 р. № 540/97-ВР // Відомості Верховної Ради України. – 1977. – № 50. – Ст. 302.

22. Про державну статистику : Закон України від 17 верес. 1992 р. № 2614-XII // Відомості Верховної Ради України. – 1992. – № 43. – Ст. 608.

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

24. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16 листоп. 1992 р. № 2782-XII // Відомості Верховної Ради України. – 1993. – № 1. – Ст. 1.

25. Про електронні довірчі послуги : Закон України від 05 жовт. 2017 р. № 2155-VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 400.

26. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275.

27. Про захист від недобросовісної конкуренції : Закон України від 07 черв. 1996 р. № 236/96-ВР // Відомості Верховної Ради України. – 1996. – № 36. – Ст. 164.

28. Про захист прав споживачів : Закон України від 12 трав. 1991 р. № 1023-XII // Відомості Верховної Ради УРСР. – 1991. – № 30. – Ст. 379.

29. Про інформаційні агентства : Закон України від 28 лют. 1995 р. № 74/95-ВР // Відомості Верховної Ради України. – 1995. – № 13. – Ст. 83.

30. Про інформацію : Закон України від 02 жовт. 1992 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

31. Про Концепцію Національної програми інформатизації : Закон України від 04 лют. 1998 р. № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28. – Ст. 182.

32. Про науково-технічну інформацію: Закон України від 25 черв. 1993 р. № 3322-XII // Відомості Верховної Ради України. – 1993. – № 33. – Ст. 345.

33. Про наукову і науково-технічну діяльність : Закон України від 26 листоп. 2015 р. № 848-VIII // Відомості Верховної Ради України. – 1992. – № 12. – Ст. 165.

34. Про Національний архівний фонд та архівні установи : Закон України від 24 груд. 1993 р. № 3814-XII // Відомості Верховної Ради України. – 1994. – № 15. – Ст. 86.

35. Про Національну систему конфіденційного зв'язку : Закон України від 10 січ. 2002 р. № 2919-III // Відомості Верховної Ради України. – 2002. – № 15. – Ст. 103.

36. Про нотаріат : Закон України від 02 верес. 1993 р. № 3425-XII // Відомості Верховної Ради України. – 1993. – № 39. – Ст. 383.

37. Про обов'язковий примірник документів : Закон України від 09 квіт. 1999 р. № 595-XIV // Відомості Верховної Ради України. – 1999. – № 22-23. – Ст. 199.

38. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII // Відомості Верховної Ради України. – 1999. – № 22. – Ст. 303.

39. Про освіту : Закон України від 05 верес. 2017 р. № 2145-VIII // Відомості Верховної Ради України. – 2017. – № 38-39. – Ст. 380.

40. Про рекламу : Закон України від 03 лип. 1996 р. № 270/96-ВР // Відомості Верховної Ради України. – 1996. – № 39. – Ст. 181.

41. Про Суспільне телебачення і радіомовлення України : Закон України від 17 квіт. 2014 р. № 1227-VII // Відомості Верховної Ради України. – 2014. – № 27. – ст. 904.

42. Про телебачення і радіомовлення : Закон України від 21 груд. 1993 р. № 3759-XII // Відомості Верховної Ради України. – 1994. – № 10. – ст. 43.

2. Підзаконні нормативно-правові акти:

2.1. Укази Президента України:

Основна:

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

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

Додаткова:

45. Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних : Указ Президента України від 24 верес. 2001 р. № 891/2001.

46. Про Доктрину інформаційної безпеки України : Указ Президента України від 25 лют. 2017 р. № 47/2017.

47. Про Єдиний державний реєстр нормативних актів : Указ Президента України від 27 черв. 1996 р. № 468/96.

48. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет і забезпечення широкого доступу до цієї мережі в Україні : Указ Президента України від 31 лип. 2000 р. № 928/2000.

49. Про першочергові завдання щодо впровадження новітніх інформаційних технологій : Указ Президента України від 20 жовт. 2005 р. № 1497/2005.

50. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27 верес. 1999 р. № 1229/99.

2.2. Постанови та розпорядження Кабінету Міністрів України:

Основна:

51. Деякі питання документування управлінської діяльності : Постанова Кабінету Міністрів України від 17 січ. 2018 р. № 55.

52. Про затвердження Положення про Єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів : Постанова Кабінету Міністрів України від 14 листоп. 2018 р. № 1024.

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

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

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

56. Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року : Розпорядження Кабінету Міністрів України від 15 лист. 2017 р. № 1023-р.

Додаткова:

57. Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів : Постанова Кабінету Міністрів України від 10 трав. 2018 р. № 357.

58. Деякі питання адміністрування Державних та Єдиних реєстрів, держателем яких є Міністерство юстиції <http://zakon4.rada.gov.ua/laws/show/1272-99-%D0%BF>: Постанова Кабінету Міністрів України від 14 лип. 1999 р. № 1272.

59. Про затвердження Концепції формування системи національних електронних інформаційних ресурсів : Розпорядження Кабінету Міністрів України від 05 трав. 2003 р. № 259-р.

60. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України: Постанова Кабінету Міністрів України від 03 верес. 2014 р. № 411.

61. Про затвердження Положення про Єдину базу даних електронних адрес, номерів факсів (телефаксів) суб'єктів владних повноважень: Постанова Кабінету Міністрів України від 05 січ. 2011 р. № 5.

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

63. Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів : Постанова Кабінету Міністрів України від 17 берез. 2004 р. № 326.

64. Про затвердження Порядку ведення Єдиного державного реєстру судових рішень : Рішення Вищої Ради Правосуддя від 19 квіт. 2018 року.

65. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах : Постанова Кабінету Міністрів України від 16 листоп. 2002 р. № 1772.

66. Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності : Постанова Кабінету Міністрів України від 19 верес. 2018 р. № 749.

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

68. Про затвердження Порядку легалізації комп'ютерних програм в органах виконавчої влади : Постанова Кабінету Міністрів України від 04 берез. 2004 р. № 253.

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

70. Про затвердження Угоди про обмін інформацією у сфері боротьби зі злочинністю : Постанова Кабінету Міністрів України від 03 серп. 2011 р. № 823.

71. Про Перелік автоматизованих систем інформаційно-технологічного забезпечення діяльності Верховної Ради України : Розпорядження Голови Верховної Ради України від 01 лип. 2003 р. № 663.

2.3. Відомчі накази правоохоронних органів:

Основна:

72. Концепція інформатизації Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України, на 2016-2020 роки : Наказ МВС України від 14 черв. 2016 р. № 511.

73. Концепція програми інформатизації Міністерства внутрішніх справ на 2018-2020 роки, затверджена рішенням колегії МВС від 05 лист. 2018 р. № 18км : Наказ МВС України від 11 груд. 2018 р. № 1004.

74. Про Єдиний реєстр досудових розслідувань : Наказ Генеральної прокуратури України від 17 серп. 2012 р. № 69.

75. Про затвердження Змін до Положення про Департамент інформатизації Міністерства внутрішніх справ України : Наказ МВС України від 04 лют. 2019 р. № 80.

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

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

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

79. Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису : Наказ МВС України від 18 груд. 2018 р. № 1026.

80. Про затвердження Інструкції про порядок ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події : Наказ МВС України від 06 листоп. 2015 р. № 1377.

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

82. Про затвердження Переліку відомостей, що становлять службову інформацію в системі Національної поліції України : Наказ Національної поліції України від 12 жовт. 2018 р. № 945.

83. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС: Наказ МВС України від 20 жовт. 2017 р. № 870.

84. Про затвердження Положення про Департамент інформатизації Міністерства внутрішніх справ України : Наказ МВС України від 31 січ. 2018 р. № 70.

85. Про затвердження Положення про Єдину цифрову відомчу телекомунікаційну мережу МВС : Наказ МВС України від 04 лип. 2016 р. № 596.

86. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України : Наказ МВС України від 12 жовт. 2009 р. № 436.

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

Додаткова:

88. Про затвердження Зводу відомостей, що становлять державну таємницю : Наказ Служби безпеки України від 12 серп. 2005 р. № 440.

89. Про затвердження Інструкції з автоматизованого обліку адміністративних правопорушень : Наказ МВС України від 04 лип. 2016 р. № 595.

90. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : Наказ МВС України від 07 лип. 2017 р. № 575.

91. Про затвердження Інструкції з організації діяльності чергової служби органів (підрозділів) Національної поліції України : Наказ МВС України від 23 трав. 2017 р. № 440.

92. Про затвердження Інструкції з оформлення матеріалів про адміністративні правопорушення в органах поліції : Наказ МВС України від 06 листоп. 2015 р. № 1376.

93. Про затвердження Інструкції з оформлення поліцейськими матеріалів про адміністративні правопорушення у сфері забезпечення безпеки дорожнього руху, зафіксовані не в автоматичному режимі : Наказ МВС України від 07 листоп. 2015 р. № 1395.

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

95. Про затвердження Інструкції про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідуванні злочинів : Наказ МВС, Служби безпеки, Державної митної служби, Генеральної прокуратури, Державного комітету у справах охорони державного кордону, Державної податкової адміністрації України від 09 січ. 1997 р. № 3/1/2/5/2/2.

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

97. Про затвердження Інструкції про порядок формування, ведення та використання оперативно-довідкового і дактилоскопічного обліку в органах внутрішніх справ та органах (установах) кримінально-виконавчої системи України : Наказ МВС України та Державного департаменту України з питань виконання покарань від 23 серп. 2002 р. № 823/188.

98. Про затвердження положення «Про територіальний сервісний центр МВС» : Наказ МВС України від 29 груд. 2015 р. № 1646.

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

100. Про затвердження Положення про порядок ведення Єдиного реєстру досудових розслідувань : Наказ Генеральної прокуратури України від 06 квіт. 2016 р. № 139.

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

102. Про затвердження Порядку взаємодії Генеральної прокуратури України та Міністерства внутрішніх справ України щодо обміну інформацією з Єдиного реєстру досудових розслідувань та інформаційних систем органів внутрішніх справ : Наказ Генеральної прокуратури України та МВС України від 17 листоп. 2012 р. № 115/1046.

103. Про затвердження Порядку взаємодії Міністерства внутрішніх справ України з центральними органами виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України : Наказ МВС України від 25 листоп. 2016 р. № 1250.

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

105. Про затвердження Порядку дій органів (підрозділів) Національної поліції в разі виявлення осіб, транспортних засобів і документів, відомості щодо яких містяться в банках даних інформаційної системи Міжнародної організації кримінальної поліції – Інтерполу : Наказ МВС України від 02 жовт. 2018 р. № 808.

106. Про організацію доступу до відомостей персонально-довідкового обліку єдиної інформаційної системи Міністерства внутрішніх справ України : Наказ МВС України від 29 листоп. 2016 р. № 1256.

107. Про організацію роботи із запитами на публічну інформацію в Національній поліції України: Наказ МВС України від 07 лют. 2017 р. № 95.

3. Навчальна література:

Основна:

108. Інформаційні технології в правозастосовній діяльності: підручник / [В. А. Кудінов, О. Є. Пакриш, В. М. Смаглюк, В. Г. Хахановський]; за заг. ред. В. А. Кудінова. – Київ : НАВС, 2018. – 176 с.

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

110. Кудінов В. А. Інформаційне забезпечення ОВС: навч. посіб. / В. А. Кудінов, В. М. Смаглюк, В. Г. Хахановський. – Київ : НАВС, 2015. – 108 с.

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

Додаткова:

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

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

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

115. Кудінов В. А. Інформаційні технології в психології: навч. посіб. / В. А. Кудінов, О. Є. Пакриш. – Київ : НАВС, 2017. – 88 с.

4. Інтернет-ресурси:

Основна:

116. Офіційний веб-портал Верховної ради України [Електронний ресурс]. – Режим доступу: <http://www.rada.gov.ua>.

117. Офіційний веб-портал Міністерства внутрішніх справ України [Електронний ресурс]. – Режим доступу: <http://www.mvs.gov.ua>.

118. Офіційний веб-портал Міністерства юстиції України [Електронний ресурс]. – Режим доступу: <https://minjust.gov.ua>.

119. Офіційний веб-портал Національної академії внутрішніх справ [Електронний ресурс]. – Режим доступу: <http://www.naiu.kiev.ua>.

120. Офіційний веб-портал Національної поліції України [Електронний ресурс]. – Режим доступу: <http://www.npu.gov.ua/uk>.

Додаткова:

121. Офіційне інтернет-представництво Президента України [Електронний ресурс]. – Режим доступу: <http://www.president.gov.ua/ua>.

122. Офіційний веб-портал Кабінету Міністрів України [Електронний ресурс]. – Режим доступу: <https://www.kmu.gov.ua/ua>.

123. Офіційний веб-портал Національної бібліотеки ім. В. І. Вернадського [Електронний ресурс]. – Режим доступу: <http://www.nbuv.gov.ua>.

**ПЕРЕЛІК ПРІОРИТЕТНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ
ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МВС УКРАЇНИ**

(відповідно до постанови Кабінету Міністрів України
від 14 листопада 2018 р. № 1024)

Інформаційні ресурси єдиної інформаційної системи МВС	Суб'єкти єдиної інформаційної системи МВС
1	2
<i>1. Відомості, що містяться в:</i>	
Єдиному державному реєстрі транспортних засобів	МВС
Реєстрі адміністративних правопорушень у сфері безпеки дорожнього руху	-"
інтегрованої інформаційно-пошукової системи	-"
реєстрі атестованих аварійно-рятувальних служб	ДСНС
Єдиному державному демографічному реєстрі	ДМС
національній системі біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства	-"
Єдиний інформаційно-аналітичний системі управління міграційними процесами	-"
Єдиному реєстрі досудових розслідувань про правопорушення, провадження за якими здійснюються працівниками органів Національної поліції, а також осіб, яким вручено повідомлення про підозру та стосовно яких закінчено досудове розслідування у кримінальному провадженні	Генеральна прокуратура України
Єдиному державному реєстрі судових рішень у справах про адміністративні правопорушення та про притягнення осіб до кримінальної відповідальності за рішеннями суду, що набрали законної сили	ДСА
<i>2. Відомості про:</i>	
облік вогнепальної зброї	МВС
дактилоскопічний облік	-"
криміналістичний облік експертної служби	-"
персонально-довідковий облік	-"

1	2
осіб, щодо яких поліцейські проводять профілактичну роботу	Національна поліція
виявлені кримінальні та адміністративні правопорушення, осіб, які їх вчинили, рух кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких надіслано до суду	-"-
розшук підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду	-"-
розшук осіб, зниклих безвісти	-"-
установлення особи невідомих трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком	-"-
зареєстровані в органах поліції кримінальні або адміністративні правопорушення, події, які загрожують особистій чи публічній безпеці, надзвичайні ситуації	-"-
осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученнями органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт)	-"-
осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією	-"-
зареєстровані кримінальні та адміністративні корупційні правопорушення, осіб, які їх вчинили, та результати розгляду цих правопорушень у судах	-"-
іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні	-"-
викрадені номерні речі, цінності та інше майно, які мають характерні ознаки для ідентифікації, або речі, пов'язані із вчиненням правопорушень, відповідно до заяв громадян	-"-
викрадені (втрачені) документи за зверненням громадян	-"-

1	2
знайдені, вилучені предмети і речі, у тому числі заборонені або обмежені в обігу, а також документи з ознаками підробки, які мають індивідуальні (заводські) номери	-"
викрадені транспортні засоби, які розшукуються у зв'язку з безвісним зникненням особи, виявлені безгосподарні транспортні засоби, а також викрадені, втрачені номерні знаки	Національна поліція
видані дозвільні документи у сфері безпеки дорожнього руху та дозволи на рух окремих категорій транспортних засобів	-"
зброю, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї	-"
викрадену, втрачену, вилучену, знайдену зброю, а також добровільно здану зброю з числа тієї, що незаконно зберігалася	-"
осіб, які перетнули державний кордон	Адміністрація Держприкордонслужби
осіб, яким органами охорони державного кордону заборонено в'їзд в Україну	-"
іноземців та осіб без громадянства, які перевищили строк реєстрації паспортних документів в Україні	-"
транспортні засоби, що перетнули державний кордон	-"
осіб, затриманих за порушення законодавства про державний кордон	-"
зареєстровані надзвичайні ситуації, у тому числі пожежі	ДСНС
<i>3. Відомості, що формуються у процесі провадження оперативно-розшукової діяльності відповідно до закону</i>	Національна поліція

**ПЕРЕЛІК ОСНОВНИХ НАБОРІВ ДАНИХ, ЯКІ ПІДЛЯГАЮТЬ
ОПРИЛЮДНЕННЮ У ФОРМІ ВІДКРИТИХ ДАНИХ**

(відповідно до постанови Кабінету Міністрів України від 21.10.2015 № 835,
в редакції постанови Кабінету Міністрів України від 20.12.2017 № 1100)

Усі розпорядники інформації

- ✓ Довідник підприємств, установ (закладів) та організацій розпорядника інформації та підпорядкованих йому організацій, у тому числі їх ідентифікаційних кодів, офіційних веб-сайтів, адрес електронної пошти, телефонів та адрес
- ✓ Інформація про організаційну структуру розпорядника інформації
- ✓ Нормативи, що затверджуються та підлягають оприлюдненню відповідно до закону розпорядником інформації
- ✓ Переліки національних стандартів, які в разі добровільного застосування є доказом відповідності продукції вимогам технічних регламентів
- ✓ Звіти, в тому числі щодо задоволення запитів на інформацію
- ✓ Інформація про систему обліку, види інформації, яка зберігається розпорядником
- ✓ Реєстр наборів даних, що перебувають у володінні розпорядника інформації
- ✓ Адміністративні дані, що збираються (обробляються) та підлягають оприлюдненню відповідно до вимог закону, розпорядника інформації
- ✓ Нормативно-правові акти, акти індивідуальної дії (крім внутрішньоорганізаційних), прийняті розпорядником інформації, проекти рішень, що підлягають обговоренню, інформація, визначена законодавством про засади регуляторної політики
- ✓ Фінансова звітність суб'єктів господарювання державного сектору економіки
- ✓ Переліки регуляторних актів із зазначенням дати набрання чинності, строку проведення базового, повторного та періодичного відстеження їх результативності та інформації про місце їх оприлюднення
- ✓ Звіти про виконання фінансових планів суб'єктів господарювання державного сектору економіки

Верховна Рада України

- Нормативно-правова база України (база даних “Законодавство України”)
- Інформація про розгляд питань порядку денного Верховної Ради України
- Інформація про законопроекти, що зареєстровані у Верховній Раді України
- Інформація про народних депутатів України

Мін'юст

- Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань
- Реєстр громадських об'єднань
- Єдиний реєстр громадських формувань
- Єдиний реєстр нотаріусів
- Державний реєстр атестованих судових експертів
- Єдиний реєстр спеціальних бланків нотаріальних документів
- Повідомлення про торги з реалізації конфіскованого та арештованого майна та їх результати, про майно для безоплатної передачі
- Державний реєстр друкованих засобів масової інформації та інформаційних агентств як суб'єктів інформаційної діяльності
- Реєстр методик проведення судових експертиз
- Єдиний державний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення
- Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство
- Єдиний реєстр арбітражних керуючих (розпорядників майна, керуючих санацією, ліквідаторів) України
- Єдиний державний реєстр нормативно-правових актів
- Реєстр суб'єктів, які надають послуги, пов'язані з електронним цифровим підписом
- Електронний реєстр чинних, блокованих та скасованих посиленних сертифікатів відкритих ключів засвідчувальних центрів та центрів сертифікації ключів
- Реєстр адміністративно-територіального устрою
- Єдиний державний реєстр осіб, щодо яких застосовано положення Закону України "Про очищення влади"

Генеральна прокуратура України

- Інформація про зареєстровані кримінальні правопорушення та результати їх досудового розслідування

МВС

- ❖ Інформація про осіб, які переховуються від органів влади
- ❖ Інформація про викрадені (вилучені) культурні цінності
- ❖ Інформація про транспортні засоби, що перебувають у розшуку у зв'язку з їх незаконним заволодінням
- ❖ Інформація про викрадену, втрачену зброю
- ❖ Інформація про стан аварійності на автомобільних дорогах
- ❖ Реєстр зареєстрованих порушень правил дорожнього руху
- ❖ Реєстр суб'єктів проведення обов'язкового технічного контролю транспортних засобів
- ❖ Інформація про викрадені/втрачені паспорти громадянина України
- ❖ Відомості про заклади, що здійснюють підготовку водіїв

- ❖ Відомості про номерні знаки, доступні для видачі в результаті реєстрації транспортних засобів
- ❖ Інформація про виявлені адміністративні правопорушення
- ❖ Інформація про дорожньо-транспортні пригоди
- ❖ Інформація про зареєстровані транспортні засоби та їх власників

Національна поліція

- Інформація про стан застосування законодавства про адміністративну відповідальність органами Національної поліції

Казначейство

- ✓ Довідник адміністративно-територіальних одиниць України (TL_TERRA)

ДРС

- Єдиний державний реєстр декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування

ДФС

- Перелік територіальних органів ДФС, митних постів із зазначенням адрес їх місць розташування

МОЗ

- Єдиний державний реєстр закладів охорони здоров'я

МОН

- ❖ Єдина державна електронна база з питань освіти (відомості з Реєстру вищих навчальних закладів)

Мінінфраструктури

- Перелік поштових індексів та відділень поштового зв'язку України
- Інформація про місця концентрації дорожньо-транспортних подій на автомобільних дорогах загального користування

Мінсоцполітики

- ✓ Класифікатор професій

Пенсійний фонд України

- Державний реєстр загальнообов'язкового державного соціального страхування

Адміністрація Держспецзв'язку

- Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом
- Переліки суб'єктів господарювання, які мають ліцензії на провадження господарської діяльності з надання послуг у галузях технічного захисту інформації та криптографічного захисту інформації
- Перелік сертифікованих засобів криптографічного захисту інформації
- Перелік технічних засобів, які можуть застосовуватися в телекомунікаційних мережах загального користування України
- Перелік засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації

Держстат

- Класифікація країн світу (КС)
- Класифікація валют (КВ)
- Класифікатор об'єктів адміністративно-територіального устрою України

Фонд державного майна

- ❖ Єдиний реєстр об'єктів державної власності

Нацкомфінпослуг

- Державний реєстр фінансових установ
- Єдиний реєстр бюро кредитних історій

Національна рада з питань телебачення і радіомовлення

- ✓ Державний реєстр суб'єктів інформаційної діяльності у сфері телебачення і радіомовлення

НКЦПФР

- Інформація, що міститься в Реєстрі правопорушень на ринку цінних паперів

Національний банк

- Довідник банків України

Фонд гарантування вкладів фізичних осіб

- Інформація про банки, в яких запроваджена тимчасова адміністрація

ДСА

- ❖ Реєстр електронних адрес органів державної влади, їх посадових та службових осіб
- ❖ Єдиний державний реєстр судових рішень
- ❖ Судова статистика
- ❖ Перелік судів із зазначенням коду ЄДРПОУ, юридичних адрес та електронних адрес для листування
- ❖ Реєстр судових справ з результатами автоматичного розподілу між суддями та результатами повторного автоматичного розподілу справ відповідно до положення про автоматизовану систему документообігу суду
- ❖ Реєстр судових засідань (номер справи, суддя, сторони, результат засідання, дата і причина перенесення)

Центральна виборча комісія

- Державний реєстр виборців
- Адреси місцезнаходження окружних виборчих комісій
- Адреси місцезнаходження дільничних виборчих комісій звичайних та спеціальних виборчих дільниць, утворених на постійній основі, до яких належать виборча адреса виборця і адреси приміщень для голосування

Місцеві держадміністрації

- ✓ Схеми планування територій областей (для облдержадміністрацій)
- ✓ Схеми планування територій районів (для райдержадміністрацій)

Органи місцевого самоврядування

- Основні положення генеральних планів населених пунктів та детальних планів територій
- Перелік об'єктів комунальної власності

ПЕРЕЛІК КОРИСНИХ ВІДКРИТИХ РЕЄСТРІВ ТА БАЗ ДАНИХ УКРАЇНИ

Список відкритих реєстрів та баз даних України, які допоможуть запобігти шахрайським діям, виявити фіктивні підприємства, фірми, приватних підприємців, з'ясувати ряд інших питань в юридичній діяльності [108]:

1. База даних Верховної Ради України «Законодавство України»
<http://zakon.rada.gov.ua/laws>
2. Офіційні документи Президента України
<http://www.president.gov.ua/documents>
3. Пошук нормативно-правових документів Кабінету Міністрів України (Урядовий портал)
<http://www.kmu.gov.ua/control/npd/search>
4. «Єдиний державний реєстр нормативно-правових актів» (Міністерство юстиції України)
<http://www.reestrnpa.gov.ua/REESTR/RNAweb.nsf/vWWWGroupParam1/searchext?OpenDocument>
5. «Єдина база даних електронних адрес, номерів факсів суб'єктів владних повноважень»
<http://email.court.gov.ua>
6. «Поштові індекси та відділення поштового зв'язку України» (Українське державне підприємство «Укрпошта»)
http://services.ukrposhta.com/postindex_new
7. «Національний реєстр електронних інформаційних ресурсів» (Державний центр інформаційних ресурсів України)
<http://e-resurs.gov.ua>
8. Кабінет електронних сервісів (Міністерство юстиції України): «Державний реєстр речових прав на нерухоме майно»; «Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство»; «Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців»; «Реєстр громадських об'єднань»; «Державний реєстр друкованих ЗМІ та інформаційних агентств, як суб'єктів інформаційної діяльності»; «Єдиний реєстр громадських формувань»; «Єдиний реєстр арбітражних керуючих»; «Єдина база даних електронних адрес, номерів факсів, телефаксів суб'єктів владних повноважень»; «Єдиний державний реєстр судових рішень»; «Електронний реєстр апостилів»; «Єдиний державний реєстр осіб, які вчинили корупційні правопорушення»; «Єдиний державний реєстр осіб, щодо яких застосовано положення Закону України “Про очищення влади”»; «Єдиний реєстр нотаріусів»
<https://kap.minjust.gov.ua/services/registry>
9. Національний портал відкритих даних: «Реєстр громадських організацій»; «Реєстр операторів, провайдерів телекомунікацій» та інші
<http://data.gov.ua>

10. Перелік електронних інформаційних БД державних установ України
https://uk.wikipedia.org/wiki/Державний_реєстр
11. «Єдиний державний реєстр судових рішень»
<http://www.reyestr.court.gov.ua>
12. МВС України. Розшук: «Зниклі громадяни»; «Неопізнані трупи»; «Культурні цінності»; «Мобільні телефони»; «Зброя у розшуку»; «Транспортні засоби у розшуку»; «Особи, які переховуються від органів влади»; «Особи, що не можуть надати про себе відомостей внаслідок хвороби або неповнолітнього віку»; «Перевірка легітимності довідки про судимість»; «Пошук паспорта громадянина України серед викрадених та втрачених»
<http://mvs.gov.ua/mvs/control/uk/investigation>
13. «Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань» (Міністерство юстиції України)
<https://usr.minjust.gov.ua/ua/freesearch>
14. База даних ДФСУ: «Дізнайся більше про свого бізнес-партнера» (Державна фіскальна служба України)
<http://sfs.gov.ua/businesspartner>
15. «Єдиний ліцензійний реєстр»; «Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань»; «Реєстр документів дозвільного характеру» (Державне підприємство «Інформаційно-ресурсний центр»)
<http://irc.gov.ua/ua/Poshuk-v-YeLR.html>
16. Реєстри Нацкомфінпослуг: «Єдиний реєстр бюро кредитних історій»; «Державний реєстр страхових та перестрахових брокерів»; «Реєстр аудиторських фірм та аудиторів, які можуть проводити аудиторські перевірки фінансових установ» та інші
<http://nfp.gov.ua/content/inshi-reestri-ta-pereliki.html>
17. «Реєстр аудиторських фірм та аудиторів» (Аудиторська палата України)
<http://apu.com.ua/reestr-auditorskikh-firm-ta-auditoriv>
18. «Реєстр платників ПДВ» (Електронний кабінет платника)
<http://sfs.gov.ua/reestr>
19. «Державний реєстр фінансових установ» (Комплексна інформаційна система Держфінпослуг)
<http://kis.nfp.gov.ua>
20. «Структури власності банків України» (Національний банк України)
http://bank.gov.ua/control/uk/publish/article?art_id=6738234&cat_id=51342
21. «База жителів України»
<http://www.nomer.org/allukraina>
22. «Єдиний реєстр адвокатів України» (Національна асоціація адвокатів України)
<http://erau.unba.org.ua>

23. «Реєстр адвокатів, які надають безоплатну вторинну правову допомогу» (Координаційний центр з надання правової допомоги)
<http://legallaid.gov.ua/ua/reiestry-advokativ>
24. «Єдиний реєстр нотаріусів»
<http://ern.minjust.gov.ua/pages/default.aspx>
25. «Єдиний реєстр спеціальних бланків нотаріальних документів» (Державне підприємство «Національні інформаційні системи»)
<http://rnb.nais.gov.com>
26. «Реєстр атестованих судових експертів» (Мінюст України)
<http://rase.minjust.gov.ua>
27. «Реєстр методик проведення судових експертиз» (Міністерство юстиції України)
<http://rmpse.minjust.gov.ua>
28. «Інформація про стан розгляду заяви (запиту)» (Державний реєстратор речових прав на нерухоме майно)
<http://rrp.informjust.ua>
29. «Реєстр громадських об'єднань»
<http://rgo.informjust.ua>
30. «Єдиний реєстр громадських формувань»
<http://rgf.informjust.ua/home/index>
31. «Державний реєстр друкованих ЗМІ та інформаційних агентств, як суб'єктів інформаційної діяльності»
<http://dzmi.informjust.ua>
32. «Автоматизована система виконавчого провадження» (Міністерство юстиції України)
<https://asvpweb.minjust.gov.ua/#/search-debtors>
33. «Єдиний державний реєстр декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування» (Національне агенство з питань запобігання корупції)
<https://public.nazk.gov.ua>
34. Відкрита база декларацій чиновників «Декларації»
<http://declarations.com.ua>
35. Реєстри Єдиного державного порталу адміністративних послуг
<http://poslугy.gov.ua>
36. «Реєстр послуг для всіх (по категоріях)» (Офіційний веб-портал адміністративних послуг міста Києва)
<http://ac.dozvil-kiev.gov.ua>
37. «Перевірка коду IMEI мобільних телефонів» (Український державний центр радіочастот)
<http://www.ucrf.gov.ua/baza-imei/perevirka-kodu-imei>
38. Перевірка документа про освіту
<https://osvita.net/ua/checkdoc>
39. Он-лайн перевірка своїх даних в Державному реєстрі виборців
<https://www.drvgov.ua/apex/f?p=111:LOGIN>

**ВИТЯГ З ПЕРЕЛІКУ ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ
СЛУЖБОВУ ІНФОРМАЦІЮ В СИСТЕМІ МВС УКРАЇНИ**
(відповідно до наказу МВС України від 26 грудня 2016 р. № 1351)

1. У сфері роботи з персоналом, організації освітньої та наукової діяльності службовою інформацією є інформація, що розкриває: персональні дані (за сукупністю всіх відомостей: прізвище, ім'я, по батькові, дата та місце народження, місце проживання, посада, найменування органу, підрозділу) працівників установ, за винятком відомостей, які віднесені до державної таємниці тощо.

2. У сфері зв'язку та телекомунікаційних мереж службовою інформацією є інформація, що розкриває: 1) інформацію про параметри налаштування апаратного обладнання, програмних засобів, паролів та кодів доступу, що використовуються при побудові та функціонуванні телекомунікаційних мереж МВС; 2) інформацію, що розкриває структуру, топологію, технічні параметри, особливості функціонування телекомунікаційної мережі МВС тощо.

3. У сфері інформаційних технологій службовою інформацією є інформація, що розкриває: 1) організацію, структуру, топологію, паролі доступу до централізованих обліків, баз (банків) даних та програмно-технічних комплексів, які входять до ЄІС МВС; 2) організацію, структуру, топологію, паролі доступу до централізованих обліків, баз (банків) даних та програмно-технічних комплексів інших інформаційно-телекомунікаційних систем системи МВС; 3) паролі доступу до централізованих обліків, баз (банків) даних та програмно-технічних комплексів інформаційно-телекомунікаційних систем органів державної влади, надані МВС.

4. У сфері охорони інформації з обмеженим доступом службовою є інформація, що розкриває: 1) організацію та фактичний стан забезпечення охорони державної таємниці, за винятком відомостей, які віднесені до державної таємниці; 2) систему охорони, перепускний, внутрішньооб'єктовий режим, технічне обладнання режимних об'єктів, зон, приміщень, де здійснюються роботи, пов'язані з державною таємницею, в умовах мирного часу, якщо при цьому не розкриваються відомості, які віднесені до державної таємниці; 3) зміст інформації, яка вноситься до форм облікової документації матеріальних носіїв інформації з обмеженим доступом, актів звірки їх наявності, знищення, у тому числі з питань мобілізаційної підготовки, територіальної оборони та цивільного захисту на особливий період, які не містять відомостей, що становлять державну таємницю; 4) зміст, організацію, результати службових розслідувань за фактами розголошення державної таємниці, втрат матеріальних носіїв секретної інформації, інших порушень режиму секретності, норм і вимог технічного захисту інформації першої та другої категорій, за винятком відомостей, які віднесені до державної таємниці;

5) порядок надання доступу працівників установ до режимних приміщень, для проведення робіт, пов'язаних з носіями секретної інформації; 6) засоби та заходи захисту інформації на режимній території, в інформаційно-телекомунікаційних та комп'ютерних мережах, у режимних приміщеннях установ, за винятком відомостей, які віднесені до державної таємниці; 7) заходи безпеки інформації на об'єктах, де циркулює інформація з обмеженим доступом, за винятком відомостей, які віднесені до державної таємниці; 8) перелік технічних засобів, що використовуються для проведення вимірювань захищеності об'єктів інформаційної діяльності від витoku інформації технічними каналами; 9) відомості, що зберігаються на ідентифікаторах комплексів засобів захисту інформації від несанкціонованого доступу, за винятком відомостей, які віднесені до державної таємниці; 10) відомості про планування, упровадження заходів, фактичний стан, наявність недоліків в організації технічного захисту інформації в установах, за винятком відомостей, що становлять державну таємницю; 11) відомості про результати експертних випробувань комплексних систем захисту інформації в автоматизованих системах на відповідність вимогам нормативно-правових актів з питань технічного захисту інформації тощо.

5. *У сфері криптографічного захисту інформації службовою є інформація, що розкриває:* 1) відомості про зміст заходів, фактичний стан, планування, наявність недоліків в організації, забезпеченні безпеки спеціальних видів зв'язку та криптографічного захисту інформації, якщо ці відомості не становлять державну таємницю; 2) відомості про порядок обліку, використання, пересилання, знищення та поводження із засобами криптографічного захисту службової інформації та ключовими документами до них, нормативною, технічною та експлуатаційною документацією; 3) відомості про технічні характеристики та зміст ключових даних до засобів криптографічного захисту службової інформації; 4) відомості про криптографічні системи, засоби криптографічного захисту службової інформації, якщо вони розкривають їх криптографічну схему (схему захисту, принципи побудови або криптографічні параметри), номенклатуру, кількість засобів криптографічного захисту службової інформації, місця їх розташування, порядок уведення в експлуатацію; 5) відомості про номенклатуру, тактико-технічні характеристики засобів криптографічного захисту секретної інформації, якщо ці відомості не становлять державну таємницю; 6) відомості про порядок поводження з матеріальними носіями інформації, яка оброблена з використанням засобів криптографічного захисту інформації, якщо ці відомості не становлять державну таємницю тощо.

6. *У сфері здійснення ОРД службовою є інформація, що розкриває:* тактику і організацію розшуку злочинців, безвісти зниклих осіб, безвісти зниклих дітей та осіб деяких інших категорій, за винятком відомостей, які віднесені до державної таємниці (безпосередньо відомості про особу (злочинець, безвісти зниклий), яка розшукується правоохоронними органами, не є інформацією з обмеженим доступом) тощо [81].

ВИТЯГ З ПЕРЕЛІКУ ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ СЛУЖБОВУ ІНФОРМАЦІЮ В СИСТЕМІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

(відповідно до наказу Національної поліції України
від 12 жовтня 2018 р. № 945)

1. *Відомості у сфері здійснення оперативно-розшукової діяльності та досудового розслідування про:* тактику і організацію розшуку злочинців, безвісно зниклих осіб, безвісно зниклих дітей та осіб деяких інших категорій, за винятком відомостей, які віднесені до державної таємниці (безпосередньо відомості про особу (злочинець, безвісно зниклий), яка розшукується органами та підрозділами поліції, не є інформацією з обмеженим доступом).

2. *Відомості у сфері застосування оперативно-технічних заходів про:* 1) відомості, які використовуються під час здійснення оперативно-розшукової діяльності, про результати аналізу інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо; 2) засоби електронно-обчислювальної та телекомунікаційної техніки, що використані при побудові інформаційно-телекомунікаційних і комп'ютерних мереж органів та підрозділів поліції тощо.

3. *Відомості у сфері охорони об'єктів службовою є:* 1) інформація про: спеціальне програмне забезпечення, протоколи інформаційного обміну, лінії зв'язку, у тому числі між складовими частинами систем передавання тривожних сповіщень у системі централізованого нагляду поліції охорони, тощо; 2) інформація, що розкриває: систему охорони за допомогою засобів електронного фіксування та зберігання перебігу подій за участю нарядів і чергових змін підрозділів поліції охорони, на територіях (у приміщеннях) об'єктів, що знаходяться під охороною, або територій обслуговування тощо.

4. *Відомості у сфері боротьби з окремими видами злочинів службовою є інформація, що розкриває:* осіб, організації, організовані групи і злочинні організації, відомості стосовно яких отримано в ході оперативно-розшукових, профілактичних заходів та кримінального аналізу, за винятком відомостей, які віднесені до державної таємниці тощо.

5. *Відомості у сфері зв'язку, інформаційно-телекомунікаційних та комп'ютерних мереж службовою є:* 1) інформація про: параметри налаштування апаратного обладнання та програмних засобів, що використані при побудові телекомунікаційних мереж; побудову та принципи роботи елементів інформаційно-телекомунікаційних систем, призначених для передавання інформації за межі відповідної комп'ютерної мережі або обміну інформацією між органами та підрозділами поліції зазначених об'єктів відкритими каналами зв'язку; засоби електронно-обчислювальної та телекомунікаційної техніки, що використані при побудові інформаційно-телекомунікаційних і комп'ютерних мереж органів та підрозділів поліції;

2) інформація, що розкриває: номенклатуру, кількість та окремі характеристики технічних засобів, що використовуються в спеціальних телекомунікаційних системах органів та підрозділів поліції; структуру, топологію, технічні параметри телекомунікаційної мережі органів та підрозділів поліції; паролі або коди доступу до інформаційно-телекомунікаційних та комп'ютерних мереж для відкритої та конфіденційної інформації тощо.

6. *Відомості у сфері охорони державної таємниці*: 1) відомості, які вносяться до форм облікової документації матеріальних носіїв інформації з обмеженим доступом, актів звірки їх наявності, поводження, знищення з питань мобілізаційної підготовки, територіальної оборони та цивільного захисту на особливий період, які не містять відомостей, що становлять державну таємницю; 2) висновки за результатами службових перевірок (розслідувань) за фактами розголошення відомостей, що становлять державну таємницю, втрат матеріальних носіїв секретної інформації, інших порушень режиму секретності, норм і вимог технічного захисту інформації першої та другої категорій за винятком відомостей, які віднесені до державної таємниці та зміст відповідних висновків; 3) засоби та заходи захисту інформації на режимній території, в інформаційно-телекомунікаційних та комп'ютерних мережах, у режимних приміщеннях, за винятком відомостей, які віднесені до державної таємниці; 4) заходи безпеки інформації на об'єктах, де циркулює інформація з обмеженим доступом, за винятком відомостей, які віднесені до державної таємниці; 5) перелік технічних засобів, що використовуються для проведення вимірювань захищеності об'єктів інформаційної діяльності від витoku інформації технічними каналами; 6) відомості, що зберігаються на ідентифікаторах комплексів засобів захисту інформації від несанкціонованого доступу, за винятком відомостей, які віднесені до державної таємниці; 7) відомості про результати перевірок стану технічного захисту інформації, за винятком відомостей, що становлять державну таємницю; 8) відомості про планування, упровадження заходів, фактичний стан, наявність недоліків в організації технічного захисту інформації, за винятком відомостей, що становлять державну таємницю; 9) відомості про результати експертних випробувань комплексних систем захисту інформації в автоматизованих системах на відповідність вимогам нормативно-правових актів з питань технічного захисту інформації; 10) відомості про технічні характеристики (специфікацію) засобів технічного захисту інформації, що використовуватимуться на об'єктах інформаційної діяльності тощо.

7. *Відомості у сфері криптографічного захисту інформації, що розкривають*: 1) відомості з питань організації та забезпечення безпеки спеціальних видів зв'язку та криптографічного захисту інформації, якщо ці відомості не становлять державної таємниці; 2) відомості про зміст заходів, фактичний стан, планування, наявність недоліків в організації, забезпеченні безпеки спеціальних видів зв'язку та криптографічного захисту інформації, якщо ці відомості не становлять державну таємницю; 3) відомості про порядок обліку, використання, пересилання та поводження із засобами криптографічного захисту службової інформації та ключовими документами до

них, нормативною, технічною та експлуатаційною документацією у сфері криптографічного захисту службової інформації; 4) відомості про технічні характеристики та зміст ключових даних до засобів криптографічного захисту службової інформації; 5) відомості про криптографічні системи, засоби криптографічного захисту службової інформації, якщо вони розкривають їх криптографічну схему (схему захисту, принципи побудови або криптографічні параметри), номенклатуру, кількість засобів криптографічного захисту службової інформації, місця їх розташування, порядок введення в експлуатацію; 6) відомості про порядок поводження з матеріальними носіями інформації, яка оброблена з використанням засобів криптографічного захисту інформації, якщо ці відомості не становлять державну таємницю тощо.

8. *Відомості у сфері інформаційно-аналітичного забезпечення службовою є інформація про:* 1) відомості щодо осіб, які підозрюються, звинувачуються в учиненні кримінального правопорушення, узяті під варту або піддані адміністративному арешту та засуджені, у тому числі їх фотографії та дактилоскопічні дані, за винятком відомостей, які віднесені до державної таємниці (не вважається інформація службовою, якщо зазначені дані запитуються суб'єктом персональних даних або за його дозволом третіми особами); 2) назву, кількість і заводські номери зброї, що перебуває в користуванні громадян (у тому числі їх персональні дані), підприємств, установ, організацій, господарських об'єднань, яка обліковується органами та підрозділами поліції у сфері дозвільної системи та яка перебуває в користуванні поліцейських (за окремими показниками); 3) організацію, структуру, топологію, паролі доступу до баз даних органів та підрозділів поліції; 4) відомості про результати аналітичного дослідження у ході проведення кримінального аналізу за окремими злочинами, що містяться в аналітичних висновках, які є складовою аналітичного продукту тощо [82].

ДЛЯ НОТАТОК

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Навчальне видання

КУДІНОВ Вадим Анатолійович

**ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ
ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ**

Словник термінів

Комп'ютерна верстка В.А. Кудінова

Підписано до друку 20.05.2019. Формат 60х84/16. Папір офсетний.

Обл.-вид. арк. 14,75. Ум. друк. арк. 13,72.

Тираж 300 прим.

Редакційно-видавничий центр
Національної академії внутрішніх справ
03035, Київ-35, пл. Солом'янська, 1

Друк: ФО-П 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