**Тема 5 ІНФОРМАЦІЙНО-ДОВІДКОВЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ**

1. Класифікація інформації за режимом доступу.
2. Захист персональних даних у правоохоронній сфері.
3. Робота з відкритими даними (OSINT- інструментарій).
4. Спеціальні інформаційні системи та закриті бази даних правоохоронних органів.
5. Правові підстави доступу працівників правоохоронних органів до баз даних.

*Мета лекції* - ознайомити здобувачів із правовою природою та архітектурою інформаційного забезпечення правоохоронної діяльності, розкривши порядок класифікації даних, специфіку використання OSINT-інструментарію та закритих баз даних, а також юридичні механізми захисту персональних даних і підстави доступу до них

## 1. Класифікація інформації за режимом доступу.

Інформаційно-аналітична діяльність правоохоронних органів є основною складовою її роботи. Вона охоплює збір, обробку, аналіз та використання різноманітної інформації для забезпечення громадського порядку, протидії злочинності та забезпечення безпеки громадян тощо.

Завдяки інформаційно-аналітичній діяльності правоохоронні органи можуть ефективно прогнозувати та запобігати кримінальним правопорушенням, розкривати злочини швидше та ефективніше, а також сприяти здійсненню кримінального переслідування та здійснювати інші, передбачені законом функції. Важливою складовою цієї діяльності є аналіз отриманої інформації з використанням сучасних методів та технологій, що дозволяє отримати об'єктивну та достовірну картину ситуації. Правове регулювання цієї діяльності забезпечується деякими законодавчими актами, які встановлюють принципи, процедури та вимоги до збору, обробки та збереження інформації. Інформаційно-аналітична діяльність Національної поліції України є необхідною складовою для забезпечення правопорядку та безпеки у країні.

Адміністративно-правове регулювання інформаційно-аналітичного забезпечення ***Національної поліції*** здійснюється в рамках Законів України «Про Національну поліцію України», «Про інформацію», «Про захист персональних даних», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», а також на підставі підзаконних нормативно-правових актів, зокрема наказу МВС України від 29.02.2006 №

139 «Про затвердження Положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України» та ін.

Адміністративно-правове регулювання інформаційно-аналітичного забезпечення ***Державної прикордонної служби*** базується на комплексній системі законодавчих актів, ключовими з яких є Закони України «*Про Державну прикордонну службу України» , «Про прикордонний контроль», «Про державний кордон України» , а також «Про інформацію», «Про захист персональних даних*» та «*Про оперативно-розшукову діяльність*», що в сукупності визначають правовий режим обробки відомостей, порядок захисту персональних даних та засади аналітичного супроводу оперативно-службових завдань із гарантування безпеки державного кордону.

Адміністративно-правове регулювання інформаційно-аналітичного забезпечення ***СБУ*** базується на системі законів, де ключову роль відіграють Закони України «*Про Службу безпеки України» , «Про державну таємницю», «Про оперативно-розшукову» та «Про контррозвідувальну діяльність», «Про національну безпеку України*», що в сукупності визначають правовий механізм обробки інформації для прогнозування загроз та прийняття стратегічних рішень у сфері захисту державного суверенітету.

Кібербезпекова діяльність правоохоронних органів інтегрована в загальну систему інформаційно-аналітичного забезпечення через роботу спеціалізованих підрозділів та базується на положеннях Закону «*Про основні засади забезпечення кібербезпеки України»,* що дозволяє їм використовувати високотехнологічні системи моніторингу трафіку, платформи обміну даними про кіберінциденти та інструменти криміналістичного аналізу цифрового середовища для захисту об'єктів критичної інфраструктури від хакерських атак і ворожих інформаційних операцій.

*Ефективність використання цих інформаційних ресурсів прямо залежить від чіткої* ***класифікації*** *даних за режимом доступу, що є правовою гарантією захисту державної таємниці та прав громадян.*

Класифікація інформації за режимом доступу в Україні ґрунтується на розмежуванні *відкритої інформації*, що є загальнодоступною за замовчуванням, та *інформації з обмеженим доступом*, яка поділяється на три категорії:

*конфіденційну* (персональні дані та відомості під контролем приватних осіб), *таємну* (державна таємниця, розкриття якої загрожує національній безпеці) та
*службову* (гриф «ДСК», що стосується внутрішньої діяльності державних органів).
Таке правове структурування забезпечує баланс між правом суспільства на інформацію та необхідністю захисту державних і приватних інтересів через застосування «трискладового тесту» при обмеженні прав на ознайомлення з документами.

## 2. Захист персональних даних у правоохоронній сфері.

*Національне законодавство в галузі захисту персональних даних*
Конституція України, зокрема, стаття 32;
Закон України «Про захист персональних даних»;
Типовий порядок обробки персональних даних;
Порядок здійснення Уповноваженим ВРУ з прав людини контролю за додержанням законодавства про захист персональних даних;
Порядок повідомлення Уповноваженого ВРУ з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних у разі їх обробки, а також оприлюднення вказаної інформації;
ст. 188–39 «Порушення законодавства у галузі захисту персональних даних», ст. 188–40 «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини»;
Кримінальний кодекс України: ст. 182 «Порушення недоторканності приватного життя».

***Персональні дані*** — це інформація про особу (суб'єкта даних), за допомогою якої її можна прямо чи опосередковано ідентифікувати. Важливо підкреслити, що персональні дані — це лише дані про особу. Дані про компанію або установу не вважаються персональними.

Ідентифікованою вважається особа, яку можна безпомилково вирізнити серед інших осіб. Зазвичай для ідентифікації достатньо знати ім'я, прізвище, по батькові та реквізити документа, що посвідчує особу, або цифровий номер, присвоєний особі (наприклад, ідентифікаційний номер). Водночас не завжди потрібен повний набір таких відомостей. Деколи достатньо меншої кількості даних, щоб ідентифікувати особу. Наприклад, фотографія чи відеозапис можуть бути достатніми для того, щоб встановити конкретну особу.

***Наприклад**: базу даних «Розшук» Національної поліції України. Це автоматизований банк відомостей, у якому обробляється інформація щодо розшуку осіб. Для розшуку осіб Національна поліція України збирає інформацію про прізвище, власне ім'я та по батькові; фотографію; дату народження; опис зовнішності; особливі прикмети; стать; місце виявлення; опис одягу; зріст; вік.*

Важливий у контексті діяльності Національної поліції України, є характер даних про особу. Персональні дані поділяються на звичайні та спеціальні категорії персональних даних.

**Спеціальні категорії персональних даних** — це дані, що розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання чи членство в профспілках, генетичні дані, біометричні дані, що використовуються для однозначної ідентифікації особи, дані про здоров'я, а також дані про статеве життя та сексуальну орієнтацію. Вказані категорії персональних даних характеризуються як чутливі персональні дані, бо розкривають відомості чутливого характеру щодо особи або їх неконтрольоване використання може стати причиною дискримінації відповідного суб'єкта даних.

*Приклад. Національна поліція України збирає біометричні дані особи, зокрема шляхом дактилоскопіювання, у випадках, передбачених Кримінальним процесуальним кодексом України.*

Захист персональних даних у правоохоронній сфері регламентується Законом України «*Про захист персональних даних*» та спеціальними нормами Закону «*Про Національну поліцію*» (статті 25–28), які зобов'язують органи забезпечувати конфіденційність, цілісність та правомірність обробки відомостей про особу в інформаційних підсистемах. Правоохоронні органи мають право обробляти персональні дані (зокрема біометричні та цифрові) без згоди особи виключно для виконання визначених законом повноважень у сфері безпеки та правопорядку, проте вони несуть персональну відповідальність за запобігання несанкціонованому доступу до них, дотримуючись суворого режиму доступу та обов'язкового документування кожної операції з даними в електронних реєстрах.

Щодо СБУ та інших правоохоронних органів, захист персональних даних має ще суворіший режим, оскільки він часто перетинається з питаннями національної безпеки та державної таємниці.

Захист персональних даних у діяльності Служби безпеки України та інших спеціальних органів регулюється Законами України «*Про захист персональних даних», «Про Службу безпеки України» та «Про оперативно-*

*розшукову діяльність»*, які дозволяють збір та обробку відомостей про особу без її згоди в межах контррозвідувальних або слідчих дій, проте встановлюють жорсткі вимоги до внутрішнього контролю, технічного захисту каналів зв'язку та обмеженого кола осіб, які мають допуск до таких масивів. Зокрема, для СБУ, ДБР та НАБУ діють спеціальні відомчі інструкції, що зобов'язують документувати кожне звернення до персональних баз, а неправомірне розголошення таких даних тягне за собою кримінальну відповідальність за статтями про розголошення державної таємниці або втручання в приватне життя.

**3. Робота з відкритими даними (OSINT- інструментарій).**

Сучасні технології та інформаційні ресурси надають національним правоохоронним органам нові можливості для ефективного виконання їхніх завдань. Використання відкритих джерел інформації (Open Source Intelligence – OSINT) стає все більш важливим елементом інформаційно-аналітичної діяльності поліції України.

Різні агенції по-різному дають визначення OSINT, але одне загальноприйняте визначення походить від Довідника НАТО з відкритих джерел розвідки, який визначає OSINT як «*розвідувальну інформацію, яка створюється на основі загальнодоступної інформації та своєчасно збирається, використовується та поширюється належним чином для відповідної аудиторії з метою вирішення конкретної розвідувальної та інформаційної вимоги»*

Інформація з відкритих джерел - *«інформація, яку будь-який член громадськості може переглядати, купувати або запитувати, не вимагаючи спеціального правового статусу або несанкціонованого доступу. Цифрова інформація з відкритих джерел – це загальнодоступна інформація в цифровому форматі, яку зазвичай отримують з Інтернету».*

OSINT передбачає використання загальнодоступних джерел, таких як газети, телефонні довідники, телебачення, радіопередачі, і, цифрових джерел, таких як веб-сайти, блоги, форуми та платформи соціальних мереж, для збору інформації, яка може сприяти аналізу розвідданих. Деякі джерела можуть розглядати платні набори даних, які можна отримати через покупку, як інформацію з відкритих джерел, а інші – ні. Але головне, щоб інформація була доступна у відкритих джерелах.

Методи OSINT широко використовуються в кіберрозслідуваннях.

Величезна кількість і різноманітність відкритих джерел, особливо в Інтернеті, мають великий обсяг інформації, яку можна зібрати. Від IP-адрес, інформації про веб-сайти та заголовків електронних листів до публікацій у соціальних

мережах і онлайнових баз даних дослідники можуть використовувати OSINT для збору інформації та виявлення моделей діяльності.

Оскільки він покладається на загальнодоступні джерела, інформацію з відкритих джерел можна збирати без попередження суб'єктів розслідування, що робить його ефективним підходом для початкових запитів або коли потрібна обережність. OSINT широко використовується в приватному секторі, а також для збору інформації про ділових партнерів, співробітників або потенційних загроз.

Методи OSINT також є цінними для встановлення контексту вкіберрозслідуваннях. Загальнодоступна інформація може надати передісторію, встановити зв'язки між суб'єктами або розкрити мотиви та поведінку.

*Використання слідчими методів OSINT*

Використання методів OSINT може зменшити попит на інші ресурси. Коли цінну інформацію можна отримати з відкритих джерел, немає необхідності вдаватися до більш дорогих, трудомістких або нав'язливих методів. Це може включати операції, які вимагають спеціальних інструментів, спостереження або агентів під прикриттям.

Оперативна безпека (Operations Security – OPSEC) є критично важливим аспектом, який слід враховувати під час проведення OSINT-розслідувань. Процес збору розвідданих залишає за собою сліди, і ця інформація може бути зібрана супротивниками, щоб сформувати ширшу картину, яка скомпрометує розслідування.

У OSINT-розслідуваннях, де слідчі широко використовують онлайн-джерела для збору даних, оперативна безпека має першорядне значення. Будь-яка цифрова діяльність, від перегляду веб-сторінок до онлайн-взаємодій, може відстежуватися. Ці цифрові відбитки можуть виявити особу слідчого або його організацію, характер розслідування та інші конфіденційні деталі, які можуть перешкодити процесу розслідування, скомпрометувати слідчих або навіть поставити під загрозу їхнє життя в екстремальних випадках. Типовим прикладом є підключення до Інтернету з IP-адреси правоохоронного органу під час проведення OSINT-розслідувань. Зловмисник, маючи доступ до журналів веб-сервера, може ідентифікувати IP-адресу та пов'язати її з органом розслідування. Інформація з відкритих джерел часто оновлюється, іноді в режимі реального часу або майже в режимі реального часу, що дозволяє слідчим отримувати своєчасні та дієві дані, що є вирішальним у кіберрозслідуваннях. Відкриті джерела часто надають інформацію, яку можна перевірити на кількох платформах або за допомогою підтверджуючих доказів, що підвищує надійність висновків. Якщо ціль має великий цифровий слід,

навіть можливо, що більше інформації можна зібрати з відкритих джерел, ніж за допомогою інших методів розслідування.

Використовуючи OSINT-технології, можна обмежити кількість конкретних запитів на інформацію до інших установ або зовнішніх організацій, таких як постачальники онлайн-послуг. Таким чином, запити мають бути зосереджені лише на тих питаннях, на які не можуть відповісти відкриті джерела, підвищуючи загальну ефективність процесу розслідування. Інформація з відкритих джерел, зазвичай, є безкоштовною та широко доступною, що робить її економічно ефективним вибором і полегшує для слідчих збір необхідної інформації без фінансових витрат або складних (міжнародних) правових процедур. Таким чином, слідчі можуть оптимізувати свої ресурси, підвищити швидкість і надійність своїх розслідувань і потенційно виявити критичні фрагменти інформації, які можуть бути недоступні за допомогою інших засобів.

## 4. Спеціальні інформаційні системи та закриті бази даних правоохоронних органів.

При виконанні своїх службових обов'язків працівники різних підрозділів поліції накопичують широкий спектр інформації для своєчасного вжиття практичних заходів щодо боротьби зі злочинністю та правопорушеннями. Така інформація має бути надійно захищена та обмежена у доступі до сторонніх та третіх осіб.

Інформаційно-аналітичною діяльністю працівників поліції є:

- створення бази даних, яка належить до інформаційної системи МВС України;
- використання інформаційно-аналітичної роботи та інформаційно-пошукової діяльності;

створення та використання баз даних МВС України, а також даних різних державних органів влади;

- проведення інформаційно-пошукової та аналітичної роботи;
- створення взаємодії щодо обміну інформацією з іншими органами державної влади, правоохоронними органами України та міжнародними організаціями.

Інформація, що отримується та використовується посадовими особами Національної поліції України, має бути систематизована для її подальшого використання. Тому поліція України впровадила в свою професійну діяльність автоматизовану інформаційно-аналітичну систему (АІС) для боротьби зі злочинністю. За допомогою автоматизованої інформаційної системи працівники інформаційної служби можуть систематизувати інформацію, постійно поповнювати базу даних новою інформацією, аналізувати існуючу та

оновлювати її. Це дає можливість оперативно надавати необхідну інформацію за відповідним запитом у найкоротші терміни, що відповідає найголовнішій меті роботи підрозділів Національної поліції України при виконанні службових завдань та ефективної боротьби із злочинністю і різними правопорушеннями.

Відповідно до Закону України «Про Національну поліцію» від 02.07.2025 №580-VIII, «Поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених законом». Засобами реалізації інформаційно-аналітичної діяльності є системи передачі даних та зв'язку, створення баз даних правової інформації, застосування інформаційно-телекомунікаційних технологій та інформаційних систем, використання правових, технічних, програмних, інформаційних та організаційних засобів.

*Автоматизовані інформаційні системи, що використовуються правоохоронними органами*

**Автоматизована інформаційна система (АІС)** визначається як організаційно-технічна система, що реалізує технологію обробки інформації за допомогою технічних і програмних засобів.

*Види*
*автоматизованих інформаційних систем, що використовуються правоохоронними органами у своїй діяльності за* ***призначенням***

– АІС, призначені для збору та обробки облікової, реєстраційної та статистичної інформації
– АІС, призначені для обробки інформації оперативного призначення;
– АІС, що використовуються для оперативно-розшукової діяльності;
– АІС, що використовуються для криміналістичного опрацювання інформації;
– АІС, що використовуються для експертної діяльності;
– АІС для адміністративного призначення

*Види*
*автоматизованих інформаційних систем, що використовуються правоохоронними органами у своїй діяльності за* ***рівнем складності***

– автоматизовані інформаційно-довідкові системи (АІДС);
– автоматизовані системи управління (АСУ);
– автоматизовані робочі місця (АРМ);
– автоматизовані інформаційно-пошукові системи (АІПС);
– автоматизовані системи обробки даних (АСОД);
– експертні системи (ЕС), експертні консультаційні системи, а також системи підтримки прийняття управлінських рішень

Основним органом, відповідальним за формування інформаційної підсистеми поліції, є *Департамент інформатизації Міністерства внутрішніх справ України*. Відповідно до законодавства України та нормативно-правових актів центральних органів виконавчої влади, цей Департамент виступає структурним підрозділом апарату МВС, який здійснює організацію, спрямовану на інформаційно-аналітичне забезпечення правоохоронної діяльності в органах і підрозділах Міністерства внутрішніх справ України та захист персональних даних під час їх обробки.

Органом, який відповідає за формування розвідувальних ресурсів національної поліції в регіонах, є *Департамент інформаційно- аналітичного забезпечення* (ДІАЗ). Він є структурним підрозділом обласних головних управлінь Національної поліції України.

Департамент інформаційно-аналітичного забезпечення є структурним підрозділом Головного управління Національної поліції в області (ГУНП) і організовує та здійснює заходи, спрямовані на забезпечення правоохоронної діяльності поліції області.

*Основними напрямами його діяльності є:*

– збір, обробка, зберігання та архівування статистичної, слідчої, оперативної, довідкової, криміналістичної та облікової інформації;
– організація створення, розвитку та експлуатації автоматизованих та інтелектуальних інтегрованих інформаційних систем;
– розробка корпоративної інформаційної мережі для обласних управлінь поліції;
– інформаційне забезпечення органів поліції, надання інформації фізичним та юридичним особам;
– облік правопорушників, скоєних злочинів, ведення кримінальної статистики злочинності;
– інформаційна підтримка органів поліції щодо зберігання та захисту ділової документації;
– впровадження сучасних інформаційних технологій та інформаційних систем у діяльність Головного управління поліції;
– підготовка національних та галузевих статистичних звітів про стан діяльності в області, регіоні та країні.

**5.** Правові підстави доступу працівників правоохоронних органів до баз даних.

Основні вимоги щодо обробки персональних даних визначені Законом України «Про захист персональних даних».

Один із головних критеріїв законності обробки персональних даних — наявність правових підстав для такої обробки. Підстави — це певні передумови, у разі настання яких, можна обробляти персональні дані.
У статті 11 Закону України «Про захист персональних даних» закріплюється *шість підстав* для обробки персональних даних.

- згода особи на обробку її персональних даних;
- укладення та виконання правочину;
- життєво важливі інтереси суб'єкта даних;
- виконання володільцем персональних даних обов'язку, передбаченого законом;
- виконання офіційних повноважень органами державної влади та іншими суб'єктами владних повноважень;
- легітимні інтереси інших осіб.

Вказаний перелік підстав обробки персональних даних вичерпний.

Основними правовими підставами доступу співробітників правоохоронних органів до баз даних є закони, що визначають статус відповідних органів, зокрема «*Про Національну поліцію*» (ст. 25–27 щодо інформаційних підсистем), «*Про Службу безпеки України*», *«Про оперативно-розшукову діяльність»* та *«Про державну таємницю»,* які надають співробітникам право отримувати інформацію, необхідну для виконання службових завдань (розкриття злочинів, контррозвідка, розшук). Безпосередній механізм доступу регламентується відомчими наказами (наприклад, Наказ МВС про *Єдину інформаційну систему (ЄІС)* або Положення про *ЄРДР*), які встановлюють, що підставою для входу в базу є виключно наявність **службової необхідності**, оформленого **авторизованого доступу** (електронного підпису) та реєстрації запиту в системі логування, що дозволяє відстежити законність дій кожного працівника.

**Література:**

1. Про Національну поліцію : Закон України від 02.06.2014. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text
2. Про інформацію : Закон України від 02.10.1992. URL https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. Про захист персональних даних : Закон України від 01.06.2010. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
4. Про державну таємницю : Закон України від 21.01.1994. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

5. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.06.1994. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
6. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12
7. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення: 03.03.2026).
8. Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV. URL: https://zakon.rada.gov.ua/laws/show/661-15.
9. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19
11. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення : наказ Офісу Генерального прокурора від 30.06.2020 № 298. URL: https://zakon.rada.gov.ua/laws/show/v0298905-20
12. Деякі питання функціонування єдиної інформаційної системи Міністерства внутрішніх справ : постанова Кабінету Міністрів України від 14.11.2018 № 1024. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-п.
13. Про затвердження Порядку формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» : наказ Міністерства внутрішніх справ України від 18.12.2018 № 1022. URL: https://zakon.rada.gov.ua/laws/show/z0010-19.
14. Про затвердження Інструкції з формування та ведення інформаційної підсистеми "Гарпун" інформаційно-комунікаційної системи "Інформаційний портал Національної поліції України: Наказ Міністерства внутрішніх справ від 13.06.2018 № 497. URL: https://zakon.rada.gov.ua/laws/show/z0787-18#Text
15. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення: Наказ Офісу генерального прокурора від 30 червня 2020 № 298. URL: https://zakon.rada.gov.ua/laws/show/v0298905-20#Text
16. Посібник з європейського права у сфері захисту персональних даних. Київ: К.І.С., 2020. 432 с. URL:https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf.
17. Інформаційно-аналітичне забезпечення правоохоронної діяльності: навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 180 с.

18. Особливості захисту персональних даних в діяльності Національної поліції України. Пам’ятка. 2025. 81 с. URL: https://rm.coe.int/hr-pamiatka-2025-2web/488029c7a9