**Тема 1. Загальна характеристика сучасних інформаційних технологій в правоохоронній діяльності.**

План:

1.Поняття та особливості сучасних інформаційних технологій в правоохоронній діяльності.

2. Виклики та проблеми використання ІТ в правоохоронній діяльності.

3.Закордонний досвід застосування сучасних технологій в правоохоронній діяльності.

**1. Поняття та особливості сучасних інформаційних технологій в правоохоронній діяльності.**

Однією з важливих умов підвищення рівня боротьби зі злочинністю є широке використання сучасних досягнень науково-технічного прогресу, які за останні роки зробили прорив у галузі інформаційних технологій.

За попередніми даними Україна посідає 59-те місце у світі за рівнем розвитку інформаційних технологій. Єдиною конкурентною перевагою, яку наша країна має в цьому аспекті, є традиційно сильний ІТ-персонал, тобто в Україні дуже високий рівень підготовки програмістів.

Сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційного забезпечення, накопичення та систематизації інформації в базах даних. Це явне підтвердження загальновідомої тези "хто володіє інформацією, той володіє світом".

**Інформаційне забезпечення органів поліції** - це сукупність методів, заходів, засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій, а також їх ефективне використання для вирішення завдань, покладених на поліцію. Інформаційні підсистеми як компоненти систем інформаційного забезпечення призначені для збору, накопичення, зберігання та обробки інформації з певних областей бухгалтерського обліку і орієнтовані на використання в діяльності більшості правоохоронних органів, мають загальний характер і належать до загальних інформаційних систем.

**Сучасні інформаційні технології** - це сукупність методів, процесів та програмно-технічних засобів, які поєднані з метою збирання, обробки, зберігання, розповсюдження, відтворення і використання інформації у користувачів. Вони мають різні види, такі як технологія опрацювання даних, керування, підтримки прийняття рішень та експертних систем.

**Основними тенденціями розвитку інформаційних технологій у правоохоронних органах є:**

1) вдосконалення форм і методів управління системами інформаційного забезпечення;

2) централізація та інтеграція комп’ютерних банків даних;

3) впровадження новітніх комп’ютерних інформаційних технологій для ведення кримінологічних записів;

4) розвиток та широке використання ефективних та потужних комп’ютерних мереж;

5) використання спеціалізованих засобів захисту інформації;

6) встановлення ефективного обміну кримінологічною інформацією на міждержавному рівні.

Всі ці тенденції значно підвищують рівень боротьби зі злочинністю. Використання інформаційних технологій в правоохоронній діяльності має велике значення для поліпшення ефективності та результативності правоохоронних органів. Технології надають засоби для збору, обробки, зберігання та аналізу великих обсягів інформації, що допомагає виявляти злочини, розслідувати справи, забезпечувати безпеку громадян і боротися зі злочинністю.

**Особливості сучасних ІТ в правоохоронній діяльності**

1. **Широкий спектр застосування:** ІТ використовуються в усіх сферах діяльності поліції, від криміналістики та оперативно-розшукової діяльності до забезпечення громадського порядку та дорожнього руху.
2. **Інтеграція та обмін інформацією:** Сучасні ІТ дозволяють створювати єдині інформаційні системи, які об'єднують різні бази даних та забезпечують оперативний обмін інформацією між різними підрозділами та відомствами.
3. **Аналіз великих даних:** За допомогою спеціальних програмних засобів поліція може аналізувати великі обсяги даних для виявлення злочинних тенденцій, прогнозування злочинів та ідентифікації злочинців.
4. **Використання штучного інтелекту:** ШІ відкриває нові можливості для правоохоронних органів, дозволяючи автоматизувати багато процесів, покращити розпізнавання облич та інших об'єктів, а також прогнозувати злочинну поведінку.
5. **Мобільність та доступність:** Сучасні мобільні технології дозволяють поліцейським отримувати доступ до необхідної інформації та баз даних безпосередньо на місці події, що значно підвищує ефективність їх роботи.
6. **Захист інформації:** З огляду на чутливість інформації, з якою працюють правоохоронні органи, особлива увага приділяється питанням кібербезпеки та захисту даних від несанкціонованого доступу.

**Напрямки використання ІТ в правоохоронній діяльності**

* Системи відеоспостереження з функцією розпізнавання облич.
* Бази даних злочинців та правопорушників.
* Системи аналізу даних для прогнозування злочинності.
* Мобільні додатки для поліцейських.
* Системи автоматичної ідентифікації транспортних засобів.
* Кібербезпека та захист інформації.
* Використання дронів та інших безпілотних літальних апаратів.

**1. Системи відеоспостереження з функцією розпізнавання облич:**

* **Функціонал**: Ці системи поєднують відеокамери високої роздільної здатності з програмним забезпеченням, яке здатне автоматично ідентифікувати людей за їхніми обличчями.
* **Застосування**:
	+ **Пошук злочинців**: Виявлення осіб, які перебувають у розшуку, в місцях масового скупчення людей (аеропорти, вокзали, торгові центри тощо).
	+ **Попередження злочинів**: Ідентифікація потенційних злочинців або осіб, які можуть становити загрозу громадській безпеці.
	+ **Розслідування злочинів**: Аналіз відеозаписів для встановлення обставин злочину та ідентифікації учасників.
* **Переваги**:
	+ Підвищення оперативності та ефективності розшукових заходів.
	+ Можливість запобігання злочинам завдяки своєчасному виявленню підозрілих осіб.
	+ Спрощення процесу розслідування злочинів.
* **Недоліки**:
	+ Порушення права на приватність.
	+ Можливість помилкової ідентифікації.
	+ Висока вартість обладнання та програмного забезпечення.

**2. Бази даних злочинців та правопорушників:**

* **Функціонал**: Централізовані бази даних, які містять інформацію про осіб, які вчинили злочини або інші правопорушення.
* **Застосування**:
	+ **Ідентифікація злочинців**: Перевірка осіб, затриманих за підозрою у вчиненні злочину.
	+ **Розслідування злочинів**: Отримання інформації про раніше судимих осіб, які можуть бути причетними до скоєння нового злочину.
	+ **Аналіз злочинності**: Виявлення тенденцій та закономірностей у злочинній діяльності.
* **Переваги**:
	+ Швидкий та зручний доступ до необхідної інформації.
	+ Можливість обміну інформацією між різними правоохоронними органами.
	+ Сприяння розкриттю злочинів та притягненню винних до відповідальності.
* **Недоліки**:
	+ Необхідність забезпечення захисту персональних даних.
	+ Можливість помилок та неточностей в базі даних.
	+ Ризик зловживання інформацією з бази даних.

**3. Системи аналізу даних для прогнозування злочинності:**

* **Функціонал**: Програмне забезпечення, яке аналізує великі обсяги даних (статистика злочинності, дані про місцевість, соціально-економічні фактори тощо) для прогнозування можливих злочинів.
* **Застосування**:
	+ **Визначення "гарячих точок"**: Виявлення районів, де найбільш ймовірне скоєння злочинів.
	+ **Планування операцій**: Розробка стратегій та планів для запобігання злочинам у визначених районах.
	+ **Перерозподіл ресурсів**: Ефективне використання сил та засобів поліції для боротьби зі злочинністю.
* **Переваги**:
	+ Можливість завчасно реагувати на загрози та запобігати злочинам.
	+ Більш ефективне використання ресурсів правоохоронних органів.
	+ Покращення громадської безпеки.
* **Недоліки**:
	+ Можливість помилкових прогнозів.
	+ Етичні питання, пов'язані з використанням даних для прогнозування злочинності.
	+ Залежність від якості та повноти даних.

**4. Мобільні додатки для поліцейських:**

* **Функціонал**: Спеціальні мобільні додатки, які надають поліцейським доступ до необхідної інформації та інструментів безпосередньо на місці події.
* **Застосування**:
	+ **Доступ до баз даних**: Перевірка осіб, транспортних засобів, документів тощо.
	+ **Оформлення документів**: Складання протоколів, звітів та інших документів в електронному вигляді.
	+ **Зв'язок та координація**: Обмін інформацією з колегами та іншими підрозділами.
	+ **Фото- та відеофіксація**: Зйомка місця події, опитування свідків тощо.
* **Переваги**:
	+ Підвищення оперативності та ефективності роботи поліцейських.
	+ Зменшення кількості помилок та зловживань.
	+ Покращення комунікації та координації між підрозділами.
* **Недоліки**:
	+ Залежність від якості зв'язку та заряду батареї.
	+ Ризик втрати або пошкодження пристрою.
	+ Необхідність навчання поліцейських роботі з додатками.

**5. Системи автоматичної ідентифікації транспортних засобів:**

* **Функціонал**: Системи, які автоматично розпізнають номерні знаки автомобілів та звіряють їх з базами даних.
* **Застосування**:
	+ **Пошук викрадених автомобілів**: Виявлення транспортних засобів, які перебувають у розшуку.
	+ **Контроль дорожнього руху**: Фіксація порушень правил дорожнього руху (перевищення швидкості, проїзд на червоне світло тощо).
	+ **Розслідування злочинів**: Ідентифікація автомобілів, які можуть бути причетними до скоєння злочинів.
* **Переваги**:
	+ Підвищення ефективності розшукових заходів.
	+ Автоматизація контролю за дотриманням правил дорожнього руху.
	+ Спрощення процесу розслідування злочинів, пов'язаних з використанням транспортних засобів.
* **Недоліки**:
	+ Можливість помилкового розпізнавання номерних знаків.
	+ Порушення права на приватність.
	+ Висока вартість обладнання та програмного забезпечення.

**6. Кібербезпека та захист інформації:**

* **Функціонал**: Комплекс заходів та технологій, спрямованих на захист інформаційних систем та даних від несанкціонованого доступу, використання, зміни або знищення.
* **Застосування**:
	+ **Захист баз даних**: Запобігання витоку конфіденційної інформації.
	+ **Боротьба з кіберзлочинністю**: Виявлення та розслідування кіберзлочинів.
	+ **Забезпечення безпеки інформаційних систем**: Захист від вірусів, хакерських атак та інших загроз.
* **Переваги**:
	+ Збереження конфіденційності та цілісності даних.
	+ Запобігання фінансовим втратам та іншим збиткам.
	+ Підвищення довіри громадян до правоохоронних органів.
* **Недоліки**:
	+ Постійне виникнення нових кіберзагроз.
	+ Необхідність постійного оновлення систем захисту.
	+ Висока вартість забезпечення кібербезпеки.

**7. Використання дронів та інших безпілотних літальних апаратів:**

* **Функціонал**: Безпілотні літальні апарати, оснащені відеокамерами та іншими сенсорами, які можуть використовуватися для виконання різноманітних завдань.
* **Застосування**:
	+ **Патрулювання**: Спостереження за громадським порядком, виявлення правопорушень.
	+ **Пошукові операції**: Пошук зниклих людей, огляд важкодоступних місць.
	+ **Розслідування злочинів**: Фіксація місця події, документування доказів.
	+ **Контроль за дорожнім рухом**: виявлення порушень та фіксації дорожньо-транспортних пригод.
* **Переваги**:
	+ **Ефективність**: БПЛА можуть швидко та ефективно обстежувати великі території, що особливо важливо під час пошукових операцій або ліквідації наслідків надзвичайних ситуацій.
	+ **Безпека**: Використання БПЛА дозволяє зменшити ризик для життя поліцейських під час виконання небезпечних завдань.
	+ **Економія**: Використання БПЛА може бути більш економічно вигідним, ніж використання гелікоптерів або інших пілотованих літальних апаратів.
* **Недоліки**:
	+ **Регулювання**: Використання БПЛА в правоохоронній діяльності потребує чіткого правового регулювання, щоб забезпечити захист прав громадян та запобігти зловживанням.
	+ **Технічні обмеження**: БПЛА мають обмежений час польоту та можуть залежати від погодних умов.
	+ **Конфіденційність**: Використання БПЛА для спостереження може викликати питання щодо порушення права на приватність.

Усі ці застосування інформаційних технологій допомагають підвищити ефективність та результативність правоохоронних органів. Однак, важливо забезпечувати баланс між використанням технологій і захистом приватності та прав громадян. Процес впровадження та використання технологій повинен бути супроводжуваний відповідним законодавством, етичними нормами та механізмами контролю, щоб запобігти можливому зловживанню та порушенню прав людини.

З розвитком нових інформаційних технологій посилилась тенденція до використання персонального комп’ютерного обладнання, сфера його застосування розширилася. В результаті спостерігаються позитивні тенденції, серед яких: загальне підвищення рівня комп’ютерної грамотності працівників правоохоронних органів, розширення переліку комп’ютерних інформаційних записів; розширення "географії" використання сучасних засобів обчислювальної техніки у всіх сферах діяльності, розвиток технологій електронної обробки інформації; створення комп’ютерної мережі для обміну інформацією.

У підсумку зазначимо, що інтеграція інформаційних технологій у діяльність Національної поліції України дозволяє вдосконалити механізми управління, забезпечує належне функціонування правоохоронних органів, а саме, швидко отримує доступ до певної інформації, необхідної для виконання своїх обов’язків, аналізує їх , використовувати досягнення науково-технічної думки для оптимізації слідчих дій. Розвиток комп’ютерних технологій дає можливість створювати нові методи роботи, підвищувати професіоналізм кожного працівника правоохоронних органів.

**2. Виклики та проблеми використання ІТ в правоохоронній діяльності.**

**1. Етичні питання, пов'язані з використанням технологій розпізнавання облич та аналізу даних**

* **Порушення приватності**: Масове використання систем розпізнавання облич може призвести до тотального стеження за громадянами та порушення їх права на приватність.
* **Дискримінація**: Технології розпізнавання облич можуть бути упередженими та призводити до дискримінації певних груп населення, наприклад, за расовою або етнічною ознакою.
* **Помилкові ідентифікації**: Помилкові ідентифікації можуть призвести до затримання або звинувачення невинних людей.
* **Зловживання**: Інформація, отримана за допомогою технологій розпізнавання облич та аналізу даних, може бути використана для зловживань з боку правоохоронних органів або інших осіб.

**2. Забезпечення конфіденційності та захисту персональних даних**

* **Витік даних**: Бази даних, які містять персональні дані громадян, можуть стати об'єктом хакерських атак або неправомірного доступу з боку зловмисників.
* **Нецільове використання даних**: Персональні дані можуть бути використані для цілей, які не передбачені законом або не відповідають згоді громадян.
* **Зберігання даних**: Тривале зберігання персональних даних може становити загрозу для приватності громадян, особливо якщо ці дані стають застарілими або неактуальними.

**3. Необхідність постійного оновлення та модернізації обладнання та програмного забезпечення**

* **Швидкий розвиток технологій**: Інформаційні технології розвиваються дуже швидко, тому обладнання та програмне забезпечення правоохоронних органів потребують постійного оновлення та модернізації, щоб залишатися ефективними та актуальними.
* **Висока вартість**: Оновлення та модернізація обладнання та програмного забезпечення потребують значних фінансових витрат, що може бути проблемою для правоохоронних органів з обмеженим бюджетом.
* **Сумісність**: Нове обладнання та програмне забезпечення повинні бути сумісними з існуючими системами, щоб забезпечити інтеграцію та обмін інформацією між різними підрозділами.

**4. Підготовка кваліфікованих кадрів, здатних ефективно використовувати сучасні ІТ**

* **Недостатня кваліфікація**: Багато співробітників правоохоронних органів можуть не мати достатньої кваліфікації для ефективного використання сучасних ІТ.
* **Необхідність навчання**: Підготовка кваліфікованих кадрів потребує часу та ресурсів, а також постійного підвищення кваліфікації співробітників у зв'язку зі швидким розвитком технологій.
* **Мотивація**: Співробітники правоохоронних органів повинні бути мотивовані до використання сучасних ІТ та мати можливість отримувати підтримку та допомогу у разі виникнення проблем.

**5. Висока вартість впровадження та підтримки сучасних інформаційних систем**

* **Закупівля обладнання та програмного забезпечення**: Впровадження сучасних інформаційних систем потребує значних фінансових витрат на закупівлю обладнання, програмного забезпечення та ліцензій.
* **Встановлення та налаштування**: Встановлення та налаштування складних інформаційних систем потребує залучення кваліфікованих фахівців, що також пов'язано з витратами.
* **Технічна підтримка**: Підтримка працездатності інформаційних систем потребує постійного обслуговування та технічної підтримки, що також потребує фінансових витрат.

**3. Закордонний досвід застосування сучасних технологій в правоохоронній діяльності.**

Наразі у світі відбувається велика кількість, можна навіть назвати це «вибухом», нових технологічних відкриттів, метою яких, безумовно, є побудова «розумного», «цифрового» суспільства і держави. У сучасному світі навряд чи залишилася хоч одна сфера людської діяльності, в яку цифрові технології не принесли кардинальних змін. Так само, не менш важливим буде застосування новітніх технологій у діяльності поліції. Цифрова трансформація відкриває нам нові можливості в поліцейській діяльності, а саме аналіз величезних масивів даних, підвищення внутрішньої ефективності системи та прискорення її роботи. Саме такі властивості цифрових технологій можуть запропонувати працівникам поліції нові інструменти впливу у протидії злочинності та підвищить якість їх роботи.

Варто розглянути це питання в аспекті аналізування досвіду зарубіжних країн, щодо впровадження нових технологій для допомоги в роботі правоохоронних органів. І так, середньорічний темп зростання загальносвітових витрат правоохоронних органів на програмні засоби та обладнання становить 9,3%. У 2018 році фінансування оцінили в $ 11,6 млрд, за 2020 рік витрачено вже понад $ 13,6 млрд, а до 2023 року, за підрахунками аналітичної компанії Markets and Markets, бюджет збільшиться до $ 18,1 млрд. Гроші витрачаються не тільки на зброю і засоби захисту, але і на високоточні інформаційні технології.

Інновації наразі впроваджують по всьому світу, щоб швидше знаходити і затримувати порушників. Ось, наприклад, у Китаї з’явилось одне із найновітніших винаходів - так зване «всевидюче око». У березні 2018 року поліцейські з Пекіна почали тестувати «розумні» окуляри для розпізнавання осіб і автомобільних номерів. Використання таких окулярів в Китаї почалося ще в лютому. Гаджет, розроблений компанією LLVision Technology, вперше протестували в китайській провінції Хенань. За допомогою «розумних» окулярів поліцейські з Хенаня затримали 7 підозрюваних і виявили 26 випадків підробки документів менш ніж за тиждень. Китайська влада також сприяє розвитку технологій на основі біометричних даних для виявлення злочинців. З 2017 року в Китаї збирають зразки голосів громадян і відбитки їхніх пальців для створення бази даних.

Однак інноваційність зарубіжної поліції цим не обмежується. Раніше ніхто навіть і подумати не міг, що поліцейських зможуть замінити роботи, але в Дубаї запустили роботу залізних поліцейських. Ще у березні 2018 року в аеропорту з'явився робот-митник, який здатний розпізнавати обличчя і відправляти попередження про підозрілих пасажирів. Він оснащений системами теплового і рентгенівського сканування, тому може відразу перевіряти вміст багажу.

Поліція Дубая вже прийняла в штат робота-поліцейського для патрулювання торгового центру. Робот ідентифікує підозрюваних і передає відеозаписи в поліцейську дільницю, а громадяни можуть повідомити про порушення через сенсорний екран на його грудях. До 2030 року влада ОАЕ планує замінити чверть поліцейського складу на роботів.

Крім того, досить розповсюдженою є практика патрулювання на вулицях міст самоврядних дронів. Згідно даних звіту за березень 2020 року дослідницького центру з вивчення дронів Бард-коледжу близько 102 країни використовують БПЛА. Вони оснащені камерою з 360-градусним кутом огляду і здатні виявляти правопорушення та розпізнавати людей, що знаходяться в розшуку. А в США Amazon оформила патент на мініатюрні дрони, які отримали назву UAVA (Unmanned Aerial Vehicle Assistant), що перекладається як «безпілотний літальний апарат-асистент». За командою «злетіти» дрон підіймається в повітря для виконання команд, оснащений відеокамерою. Він зможе зазирнути туди, куди живому співробітнику заходити небезпечно, і тим самим позбавить поліцейських від невиправданого ризику. Дрони також борються з браконьєрами і контрабандистами.

Так, у США функціонує так звана «Розумна поліція», яка використовує новітні технології у вигляді сучасних поліцейських патрульних машин, які оснащені новітніми інтегрованими ІТ-системами замість застарілої радіозв'язку. «Розумна поліція» активно використовує мініатюрні дрони UAVA (безпілотний літальний апарат-асистент) для патрулювання. Також в межах проекту «SMART on CRIME» («Розумні технології/підходи до злочинності») в США розробляється алгоритм для оцінки підсудних.

Використання новітніх інформаційних технологій являє собою ідеальне поєднання використання актуальної інформації та сучасного програмного забезпечення, а також можливість скоординованого патрулювання території та покращення діяльності, пов’язаної з попередженням та розкриттям злочинів.

Враховуючи вищенаведені факти ефективного використання інформаційних технологій в діяльності поліції зарубіжних країн, варто зазначити, що використання новітніх перспективних технологій значно поліпшить рівень роботи поліцейських щодо розкриття та попередження злочинів. Також не варто забувати, що необхідною умовою для підвищення дієвості поліції завжди буде залишатись якісна підготовка фахівців і підвищення кваліфікації співробітників Національної поліції України по профілях, пов'язаних з системним аналізом і автоматизованими системами.