НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки ННІ № 1

Мультимедійний навчальний посібник

З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:

«ПЕРВИННА ПРОФЕСІЙНА ПІДГОТОВКА ЗА ПРОФЕСІЄЮ. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПОЛІЦЕЙСЬКІЙ ДІЯЛЬНОСТІ. БЕЗПЕКА РОБОТИ З ІНФОРМАЦІЄЮ»

Київ-2024 р.

ВИКЛАДАЧ ІЗ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Яровий Кирило Васильович – кандидат юридичних наук, викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції. З серпня 2009 року почав службу в правоохоронних органах. У 2013 році з відзнакою закінчив Луганський державний університет внутрішніх справ ім. Е.О. Дідоренка (факультет кримінальної міліції). У 2014 році з відзнакою отримав кваліфікаційний рівень магістр права.

З початку своєї кар'єри працював на офіцерських посадах у підрозділах кримінальної міліції, превентивної діяльності, організаційно-аналітичного забезпечення та оперативного реагування, кадрового забезпечення.

У 2019 році здобув науковий ступень кандидата юридичних наук. З листопада 2021 року працює в Національній академії внутрішніх справ на посаді викладача кафедри інформаційних технологій та кібербезпеки. Є автором та співавтором понад 20 наукових статей та науково-методичних праць. Область наукових інтересів: інформаційне право, кібербезпека, кримінальний аналіз, публічне управління та адміністрування.

Крім цього, член Центру українсько-європейського наукового співробітництва, Голова ради молодих вчених НАВС, член Ірпінської молодіжної ради, помічник-консультант народного депутата України IX скликання.

ЗМІСТ

Тема 1. Нормативно-правове регулювання у сфері інформаційних відносин. Система інформаційного забезпечення Національної поліції України

Лекція

Практичне завдання №1

Тема 2. Безпека роботи з інформацією

Лекція

Практичне заняття № 1

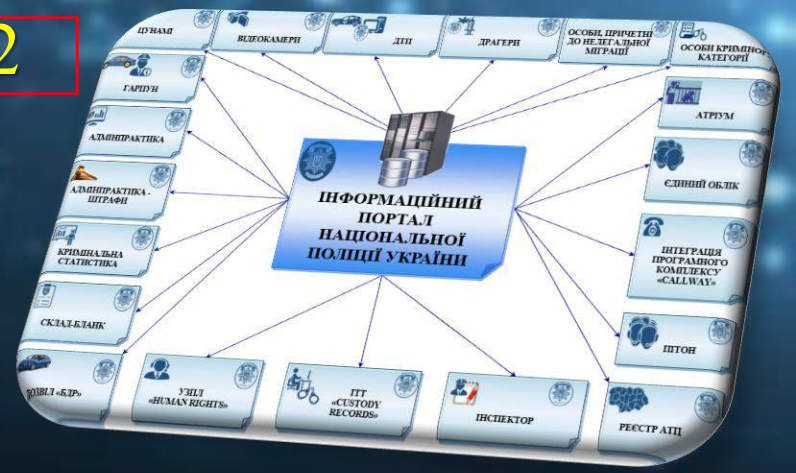
Практичне заняття №2

Тема 3. Використання поліцією можливостей ІТС «Інформаційний портал НПУ» та веб-ресурсу «Розшук» МВС України, ЄРДР у боротьбі зі злочинністю

Лекція

Практичне заняття № 1

Практичне заняття №2



Знайомство із слухачами навчальної дисципліни

НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки ННІ № 1

Мультимедійна презентація

Тема: «НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ У СФЕРІ ІНФОРМАЦІЙНИХ ВІДНОСИН. СИСТЕМА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ»

Тема 1:
Єдина інформаційна система Міністерства внутрішніх справ та основні інформаційні ресурси інших державних органів України

Питання:

1. Мета та завдання дисципліни
2. Єдина інформаційна система Міністерства внутрішніх справ
3. Система інформаційного забезпечення Національної поліції
4. Основні інформаційні ресурси інших державних органів України

Література до дисципліни:

1. Закони України:

Основна література:

1. Конституція (ст. 3, 19, 31, 32, 34)
2. Про Національну поліцію (ст. 25, 26, 27, 28)
3. Про інформацію (ст. 1, 9-21)

Додаткова література:

1. Про Національну програму інформатизації.
2. Про захист персональних даних.
3. Про державну таємницю.
4. Про електронні комунікації.
5. Про доступ до публічної інформації.
6. Про електронні документи та електронний документообіг
7. Про електронні довірчі послуги.
8. Про захист інформації в ІКС.
9. Кодекси: КК, КПК, КУАП тощо.

2. Підзаконні нормативно-правові акти:

2.1. Постанови Кабінету Міністрів України

Основна література:

1. № 1024 від 14.11.2018 «Про затвердження Положення про єдину інформаційну систему МВС та переліку її пріоритетних інформаційних ресурсів».

Додаткова література:

1. № 55 від 17.01.2018 «Деякі питання документування управлінської діяльності».
2. № 373 від 29.0.2006 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах».
3. № 357 від 10.05.2018 «Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів».

2.2. Відомчі накази МВС України:

Основна література:

1. № 676 від 03.08.2017 «Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України».
2. № 207 від 30.03.2022 № 207 «Деякі питання ведення обліку відомостей про притягнення особи до кримінальної відповідальності та наявності судимості».
3. № 613/380/93/228/414/510/2801/5 від 17.08.2020 «Про затвердження Інструкції про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол».

Додаткова література:

1. № 324 від 29.04.2021 «Про затвердження Типового положення про функціональну підсистему єдиної інформаційної системи МВС України».
2. № 665 від 16.09.2020 «Про затвердження Порядку функціонування центральної підсистеми єдиної інформаційної системи МВС України».
3. № 630 від 29.07.2019 «Деякі питання документування управлінської діяльності в МВС України».
4. № 357 від 27.04.2020 «Про затвердження Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України».
5. № 100 від 08.02.2019 «Про затвердження Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події».

6. №1376 від 06.11.2015 «Про затвердження Інструкції з оформлення матеріалів про адміністративні правопорушення в органах поліції».
7. №870 від 20.10.2017 «Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС».
8. №596 від 04.07.2016 «Про затвердження Положення про єдину цифрову відомчу телекомунікаційну мережу МВС».
9. №1351 від 26.12.2016 «Про затвердження Переліку відомостей, що становлять службову інформацію в системі МВС України».
10. Наказ Національної поліції України №945 від 12.10.2018 «Про затвердження Переліку відомостей, що становлять службову інформацію в системі Національної поліції України».

3. Навчальна література:

Основна література:

1. Інформаційні технології в діяльності Національної поліції: навчальний посібник / В.А. Кудінов; Ю.Ю. Орлов; О.Є. Пакриш. – К.: НАВС, 2017. – 100 с.
2. Інформаційне забезпечення органів Національної поліції: словник термінів / В. А. Кудінов. – К.: НАВС, 2019. – 236 с.
3. Інформатика в юридичній діяльності (в 2-х частинах): підручник / За заг. ред. В.А. Кудінова. – К.: НАВС, 2016, 2017. – 256 с., 332 с.

Додаткова література:

1. Інформаційне забезпечення ОВС: навчальний посібник / В.А. Кудінов; В.Г. Хахановський; В.М. Смаглюк. – К.: НАВС, 2015. – 108 с.
2. Інформаційні технології в правозастосовній практиці: навчальний посібник / В.А. Кудінов; В.М. Смаглюк; В.Г. Хахановський. – К.: НАВС, 2015. – 112 с.

4. Інтернет-ресурси:

Офіційні веб-портали:

1. Верховної ради України: http://www.rada.gov.ua
2. Міністерства внутрішніх справ України: http://www.mvs.gov.ua
3. Національної поліції України: http://www.npu.gov.ua/uk/
4. Національної академії внутрішніх справ: http://www.naiau.kiev.ua

Питання:

1. Мета та завдання дисципліни

1 курс (вересень-листопад 2021 р.)
«Інформаційні технології»

Лекцій – 4 н.г.
Семінарів – 0 н.г.
Практичні – 40 н.г.

ВСЬОГО: 44 н.г.

Самостійна робота – 46 н.г.

7 Тем
(основні поняття, Word, Excel, PowerPoint, Internet, правові ІПС, захист інформації)

Залік (2 н.г. – тест на ПК)

Завдання до семінару
(матеріали 1 курсу)

1. Формати дати (5: К-С-Д-П-О)
2. Інформаційна технологія
3. Інформація
4. Основні види інформаційної діяльності (8)
5. Види інформації за змістом (11)
6. Властивості інформації (14)
7. Інформація з обмеженим доступом (3)
8. Ступінь секретності секретної інформації (3)

2 курс (лютий-червень 2023 р.)
«Інформаційне забезпечення професійної діяльності»

Лекцій – 4 н.г.
Семінарів – 26 н.г.
Практичні – 14 н.г.

ВСЬОГО: 44 н.г.

Самостійна робота – 46 н.г.

6 Тем (Word, Excel, Access,
ІКС «ІПНП», «Розшукові обліки»,
експертні системи, ЄРДР, «ЦУНАМІ»)

Залік (2 н.г. – тест на ПК)

Мета дисципліни

теоретичні знання щодо інформаційного забезпечення органів Національної поліції

практичні уміння і навички щодо використання інформаційних технологій у боротьбі зі злочинністю

Основні завдання дисципліни

Здобуття знань, умінь і навичок з питань:

- ЄІС та основні види обліків МВС
- принципи побудови СІЗ органів НП
- поняття БД, банків даних та СУБД
- ІКС «Інформаційний портал НП»
- ІТП «Лінія-102» (система «ЦУНАМІ»)
- основні інформаційні ресурси інших державних органів України

Сприймання інформації

ЛЮДИНА ЗАСВОЮЄ

10 %	ПОЧУТОГО
20 %	ПОБАЧЕНОГО
50 %	ПОЧУТОГО та ПОБАЧЕНОГО
70 %	ОБГОВОРЕНОГО
80 %	ЗРОБЛЕНОГО
90 %	ОБГОВОРЕНОГО та ЗРОБЛЕНОГО

ЗАПАМ'ЯТОВУВАННЯ ІНФОРМАЦІЇ

№ з/п	*Орган чуття* *(слух, зір, нюх, смак, дотик)*	*3 год.*	*3 дні*
1.	СЛУХ	25 %	10 %
2.	ЗІР	72 %	20 %
3.	СЛУХ + ЗІР	85 %	65 %
4.	**СЛУХ + ЗІР + КОНСПЕКТ**	**> 90 %**	**> 80 %**

Епіграфи до дисципліни:

1. Хто володіє інформацією – той володіє світом.

(У. Черчіль, 1946)

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

(Кудінов В.А., 2012)

3. Хто має та вміло використовує інформаційні технології – той володіє інформацією.

(Кудінов В.А., 2006)

Інформаційна технологія – це 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 (ст. 1 Закону України "Про Національну програму інформатизації").

Інформаційна система – це організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів (ст. 1 Закону України "Про захист інформації в інформаційно-комунікаційних системах").

Інформаційний ресурс – це сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо) (ст. 1 Закону України “Про Національну програму інформатизації”).

База даних (БД) – це іменована сукупність даних, що відображає стан об’єктів та їх відношень у визначеній предметній області (ст. 1 Закону України “Про Національну програму інформатизації).

Система управління базами даних (СУБД) – це сукупність мовних та програмних засобів, що призначені для створення, ведення та конкурентного використання бази даних багатьма користувачами.

Банк даних – це сукупність БД та СУБД.

Комп'ютерна система
апаратне забезпечення + програмне забезпечення

Інформаційна система
комп'ютерна система + інформаційні ресурси

Інформаційна-комунікаційна система
інформаційна система + електронні комунікації

Автоматизована система
інформаційна система + персонал

Основні характеристики ІПС

1. Повнота (відношення кількості знайдених за запитом документів до загального числа існуючих документів, що задовольняють даному запиту).
2. Точність (ступінь відповідності знайдених документів запиту користувача).
3. Актуальність (характеризується часом, що проходить з моменту публікації документів до занесення їх в індексну базу пошукової системи).
4. Швидкість пошуку.
5. Наочність представлення результатів.

Деякі скорочення назв реєстрів

ЄІС – Єдина інформаційна система.

ЄРДР – Єдиний реєстр досудових розслідувань.

ЄДРСР – Єдиний державний реєстр судових рішень.

ІАС – Інформаційно-аналітична система.

ІПНП – Інформаційний портал Національної поліції.

НАІС – Національна автоматизована інформаційна система Єдиного державного реєстру МВС України щодо транспортних засобів та їх власників.

ЦУНАМІ – Центр управління нарядами поліції.

Питання:

2. Єдина інформаційна система Міністерства внутрішніх справ

Єдина інформаційна система (ЄІС) МВС – це багатофункціональна інтегрована автоматизована система,

що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супроводження їх діяльності і становить сукупність взаємозв'язаних функціо-нальних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів електронної комунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію.

(Постанова Кабінету Міністрів України від 14.11.2018 № 1024)

Мета ЄІС МВС

оптимізації 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 економічній зоні;
3) цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, рятувальної справи, гасіння пожеж тощо;
4) міграції (імміграції та еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів.

Завдання ЄІС МВС

1) створення єдиного інформаційного простору системи МВС та центральних органів виконавчої влади 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, 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.

Функціональні підсистеми ЄІС МВС

1) національна система біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства;
2) інформаційний портал Національної поліції України;
3) Єдиний державний реєстр транспортних засобів;
4) Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху;
5) система фіксації адміністративних правопорушень у сфері забезпечення БДР в автоматичному режимі;
6) система екстреної допомоги населенню за єдиним телефонним номером 112;
7) інтегрована міжвідомча ІКС щодо контролю осіб, ТЗ та вантажів, які перетинають державний кордон;
8) інформаційно-комунікаційна система прикордонного контролю “Гарт-1” тощо.

Інформаційні ресурси ЄІС МВС –

це визначені групи взаємозв’язаних задокументованих одиниць інформації, які формуються і об’єднуються в автоматизованих інформаційних системах суб’єктів ЄІС МВС за певними ознаками, у тому числі зазначені в Переліку пріоритетних інформаційних ресурсів ЄІС МВС, затвердженому постановою Кабінету Міністрів України від 14 листопада 2018 р. №1024.

Перелік пріоритетних інформаційних ресурсів ЄІС МВС

ВСЬОГО – **37**, з них:

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


Єдина багатохонова система цифрового радіозв'язку
Система планування та управління об'єднаними силами із забезпечення громадської безпеки та ліквідації надзвичайних ситуацій
Єдиний Державний реєстр територіальних громад
Єдиний сервіс ідентифікації фізичних осіб
Міністерство внутрішніх справ України
Цифрова трансформація інтеграції відомчих інформаційних ресурсів (ЄІС МВС)
Забезпечення інтеграції та інтероперабельності інформаційних систем та реєстрів органів системи МВС. Належне функціонування та захист даних у національних електронних інформаційних ресурсах, що перебувають в компетенції органів системи МВС
«Безпечна країна»
Реєстр відомостей про статус особи у кримінальному провадженні та судимості
«Система 112»
Модернізація електронних інформаційних ресурсів у сфері безпеки дорожнього руху
Єдиний реєстр зброї

Пріоритетними проєктами інформатизації системи МВС України на сьогодні є:

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

Структура ЄІС МВС:

1) центральна підсистема (ЦП);
2) функціональні підсистеми (ФП);
3) транспортна мережа передачі даних;
4) центрів обробки даних, електронних комунікаційних мереж суб'єктів ЄІС МВС;
5) комплексні системи захисту інформації підсистем ЄІС МВС.

Власником і розпорядником ЄІС

є держава в особі МВС.

Володільцем інформації в ЦП ЄІС

є МВС.

Володільцями інформації у ФП ЄІС,

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

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

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

Інформаційна служба

1. МВС України:

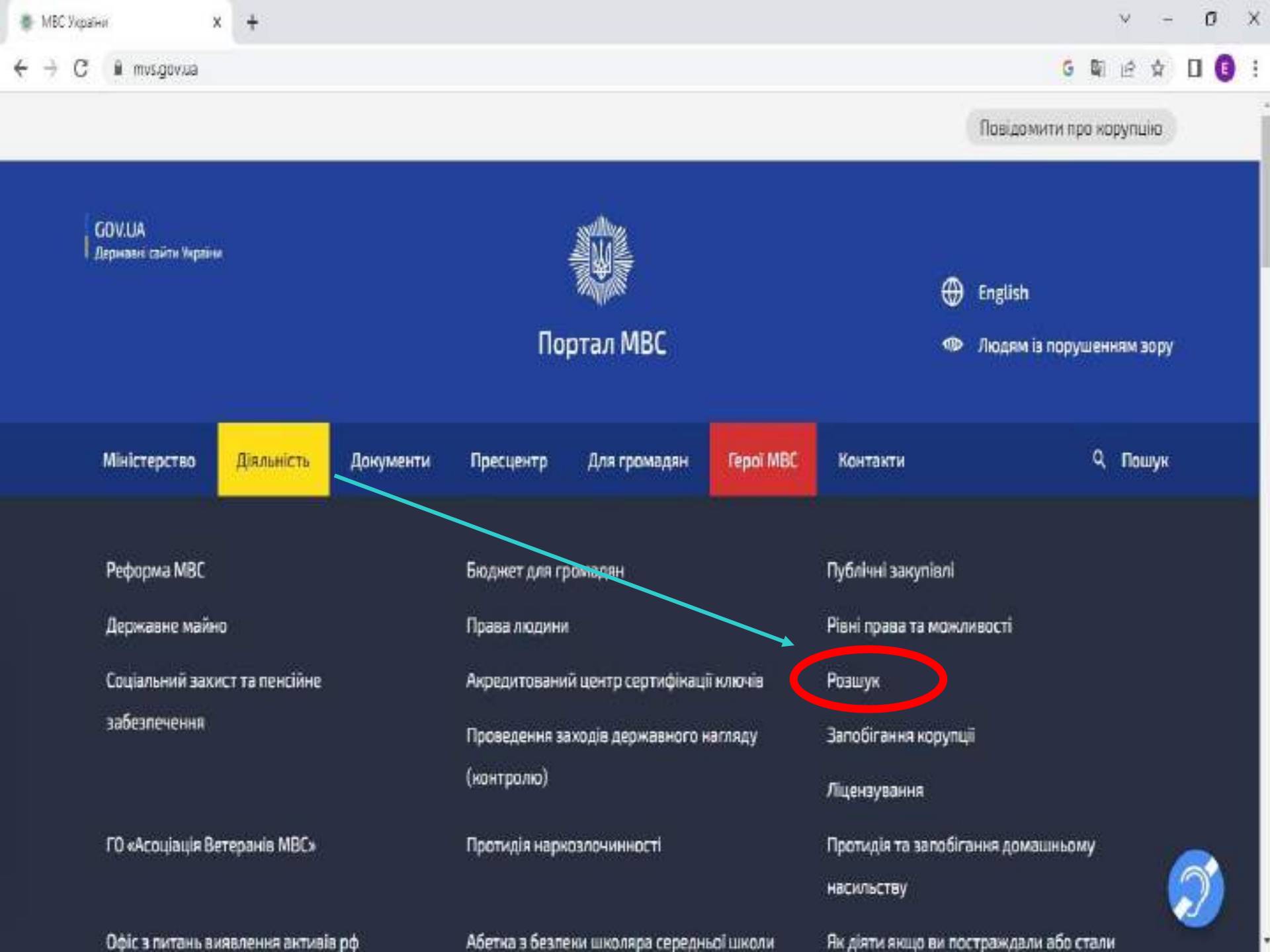
   Департамент інформатизації.

2. Національна поліція:

   Департамент інформаційно-аналітичної підтримки.

ІСТОРІЯ ІНФОРМАЦІЙНОЇ СЛУЖБИ

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


МВС України
mvs.gov.ua
Повідомити про корупцію
GOV.UA
Державні сайти України
Портал МВС
English
Людям із порушенням зору
Міністерство
Діяльність
Документи
Прессцентр
Для громадян
Герої МВС
Контакти
Пошук
Реформа МВС
Державне майно
Соціальний захист та пенсійне забезпечення
ГО «Асоціація Ветеранів МВС»
Офіс з питань виявлення активів рф
Бюджет для громадян
Права людини
Акредитований центр сертифікації ключів
Проведення заходів державного нагляду (контролю)
Протидія наркозлочинності
Абетка з безпеки школяра середньої школи
Публічні закупівлі
Рівні права та можливості
Розшук
Запобігання корупції
Ліцензування
Протидія та запобігання домашньому насильству
Як діяти якщо ви постраждали або стали

Twitter МВС

Даний веб-ресурс призначений для надання допомоги:

- Зниклі громадяни
- Невпізнані 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

Шановні користувачі

На сайті представлено детальну інформацію, куди Ви зможете звернутися за вказаними телефонами, або зателефонувавши 102.

Бугаєв внутрішніх справ висловлює вдячність за будь-яку допомогу.

Зверніть увагу, що даний пошуковий ресурс є копією офіційної бази МВС України і періодично оновлюється.

Shadow Mode

Шановні користувачі

Даний вебресурс призначений для надання допомоги:

- зі встановлення місцезнаходження безвісті зниклих людей
- пошуку мобільних телефонів
- пошуку осіб, які втратили пам'ять
- транспортних засобів у розшуку
- розшуку тих, хто переховується від органів влади
- зброї у розшуку
- пошуку викрадених культурних цінностей
- перевірка легітимності довідки про судимість
- пошук паспорту громадянина України серед викрадених та втрачених

Для уточнення інформації звертайтеся за телефоном "гарячої лінії" МВС України 15-39 або зателефонувавши 102.
Міністерство внутрішніх справ та Національна поліція України висловлюють вдячність за будь-яку допомогу.
Зверніть увагу, що даний пошуковий ресурс є копією офіційної бази МВС України і періодично оновлюється.

Розшукові обліки МВС України

https://wanted.mvs.gov.ua/

1. Зниклі громадяни.
2. Неопізнані трупи.
3. Культурні цінності.
4. Мобільні телефони.
5. Зброя у розшуку.
6. Транспортні засоби у розшуку.
7. Особи, які переховуються від органів влади.
8. Особи, що не можуть надати про себе відомостей внаслідок хвороби або неповнолітнього віку.
9. Перевірка легітімності довідки про судимість.
10. Пошук паспорта громадянина України серед викрадених та втрачених.

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

Є функціональною підсистемою ЄІС МВС України.

Це структурована автоматизована база даних,

яка використовується для збирання, зберігання, обліку, пошуку, узагальнення, захисту, перевірки достовірності відомостей, перетворення та відображення інформації, забезпечення доступу до даних про притягнення особи до кримінальної відповідальності, відсутність (наявність) судимості або обмежень, передбачених кримінальним процесуальним законодавством України.

Об’єкти обліку ІАС

1) фізичні особи:

–які набули статусу підозрюваного, обвинуваченого (підсудного), засудженого;

–щодо яких застосовано примусові заходи медичного чи виховного характеру;

–яких звільнено від кримінальної відповідальності;

–яких оголошено в розшук;

2) громадяни України, яких засуджено судами інших держав;

3) архівна інформація репресивних органів.

Право на запит та отримання відомостей з ІАС мають:

1) державні органи, які здійснюють правоохоронні функції, органи прокуратури, суди всіх рівнів;

2) органи державної влади, органи місцевого самоврядування, установи та організації, у зв'язку із здійсненням ними повноважень, визначених законодавством;

3) фізичні особи.

Перевірка осіб за ІАС проводиться за:

1) вимогою; 2) листом; 3) запитом.

Номер витягу

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Департамент інформатизації

Перевірка достовірності

унікальний електронний ідентифікатор (QR-код)

ПОВНИЙ/СКОРОЧЕНИЙ

ВИТЯГ
з інформаційно-аналітичної системи «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості»

Виданий про те, що громадянин(ка) _____,
(громадянство, прізвище, ім'я, по батькові (за наявності))

_____
(число, місяць, рік, місце народження)

на території України станом на _____
(число, місяць, рік)

_____
(результати перевірки за інформаційно-аналітичною системою «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості»)

Витяг надано для _____
(мета запиту)

Питання:

3. Система інформаційного забезпечення Національної поліції

Система інформаційного забезпечення Національної поліції

– це сукупність інформаційних підсистем певних обліків, побудованих з урахуванням дотримання таких вимог:

1) наявності нормативно-правової бази;
2) організаційно-кадрового забезпечення інформаційних підрозділів;
3) організації підготовки та перепідготовки кадрів;
4) наявності відповідних технічних, програмних та електронних комунікаційних технологій;
5) матеріально-технічного та фінансового забезпечення.

Система інформаційного забезпечення Національної поліції

МЕТА

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

ЗАВДАННЯ

1. Забезпечення можливості оперативного отримання інформації у повному, систематизованому та зручному для користування вигляді.
2. Збір, обробка та узагальнення інформації для оцінки ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях управління.
3. Забезпечення усіх динамічної та ефективної інформаційної взаємодії органів Національної поліції, інших правоохоронних органів та державних установ.
4. Забезпечення захисту інформації.

Принципи побудови інформаційних підсистем:

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

Основні види обліків:

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

Інформація оперативних обліків:

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

Інформація експертно-криміналістичного призначення:

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

Приклади оперативно-пошукових обліків:

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

Приклади інформаційно-довідкових обліків:

Колекції зразків:

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

Національна поліція має доступ до баз (банків) даних:

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

Закон України

“Про Національну поліцію”

Стаття 25. Повноваження поліції у сфері інформаційно-аналітичного забезпечення (початок)

Поліція в рамках інформаційно-аналітичної діяльності:

1) **формує** бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України;

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

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

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

Стаття 25. Повноваження поліції у сфері інформаційно-аналітичного забезпечення (закінчення)

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.

Діяльність поліції, пов’язана із захистом і обробкою персональних даних, здійснюється на підставах, визначених Конституцією України, Законом України "Про захист персональних даних", іншими законами України.

Стаття 26. Формування інформаційних ресурсів поліцією (початок)

Поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи МВС України (**18 пунктів**).

Під час наповнення баз (банків) даних, визначених у **пункті 7**, поліція забезпечує збирання, накопичення **мультимедійної інформації** (фото, відео-, звукозапис) та **біометричних даних** (дактилокартки, зразки ДНК).

Примітка: **п.7** – 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).

Стаття 26. Формування інформаційних ресурсів поліцією (продовження 1)

***Бази (банки) даних, що входять до єдиної інформаційної системи МВС України*:**

1) осіб, щодо яких поліцейські здійснюють профілактичну роботу;

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

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

4) розшуку безвісно зниклих;

Стаття 26. Формування інформаційних ресурсів поліцією (продовження 2)

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

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

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

Стаття 26. Формування інформаційних ресурсів поліцією (продовження 3)

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

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

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

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

Стаття 26. Формування інформаційних ресурсів поліцією (продовження 4)

12) викрадених (втрачених) документів за зверненням громадян;

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

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

Стаття 26. Формування інформаційних ресурсів поліцією (закінчення)

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

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

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

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

Стаття 27. Використання поліцією інформаційних ресурсів (початок)

Поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади.

Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано.

Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій Міністерства внутрішніх справ України.

Стаття 27. Використання поліцією інформаційних ресурсів (закінчення)

В електронному архіві фіксуються:

1) прізвище, ім’я, по батькові поліцейського;

2) номер спеціального жетона поліцейського;

3) вид отриманої інформації;

4) реєстр, з якого отримувалася інформація;

5) час отримання інформації;

6) інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів.

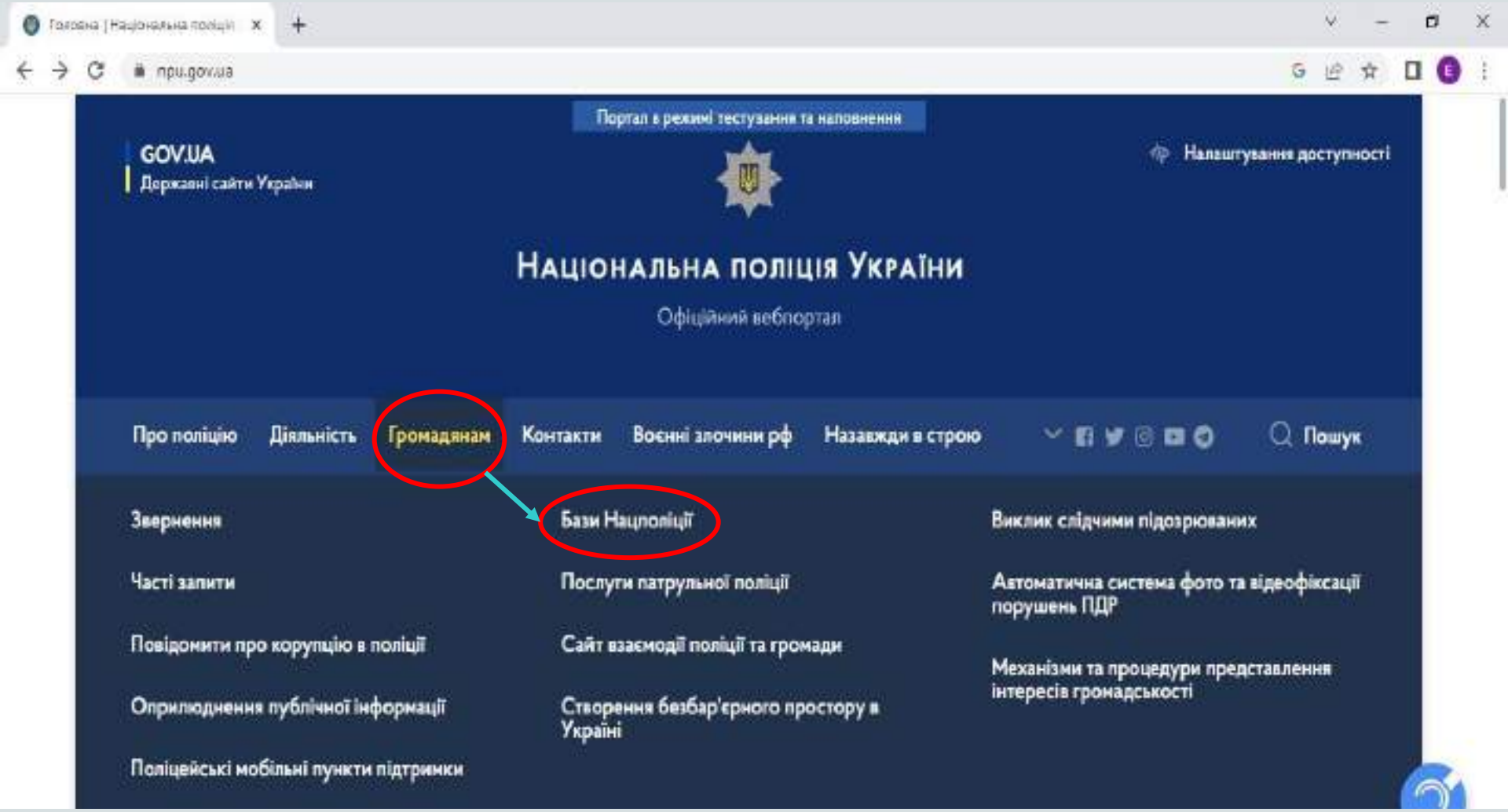
Стаття 28. Відповідальність за протиправне використання інформаційних ресурсів

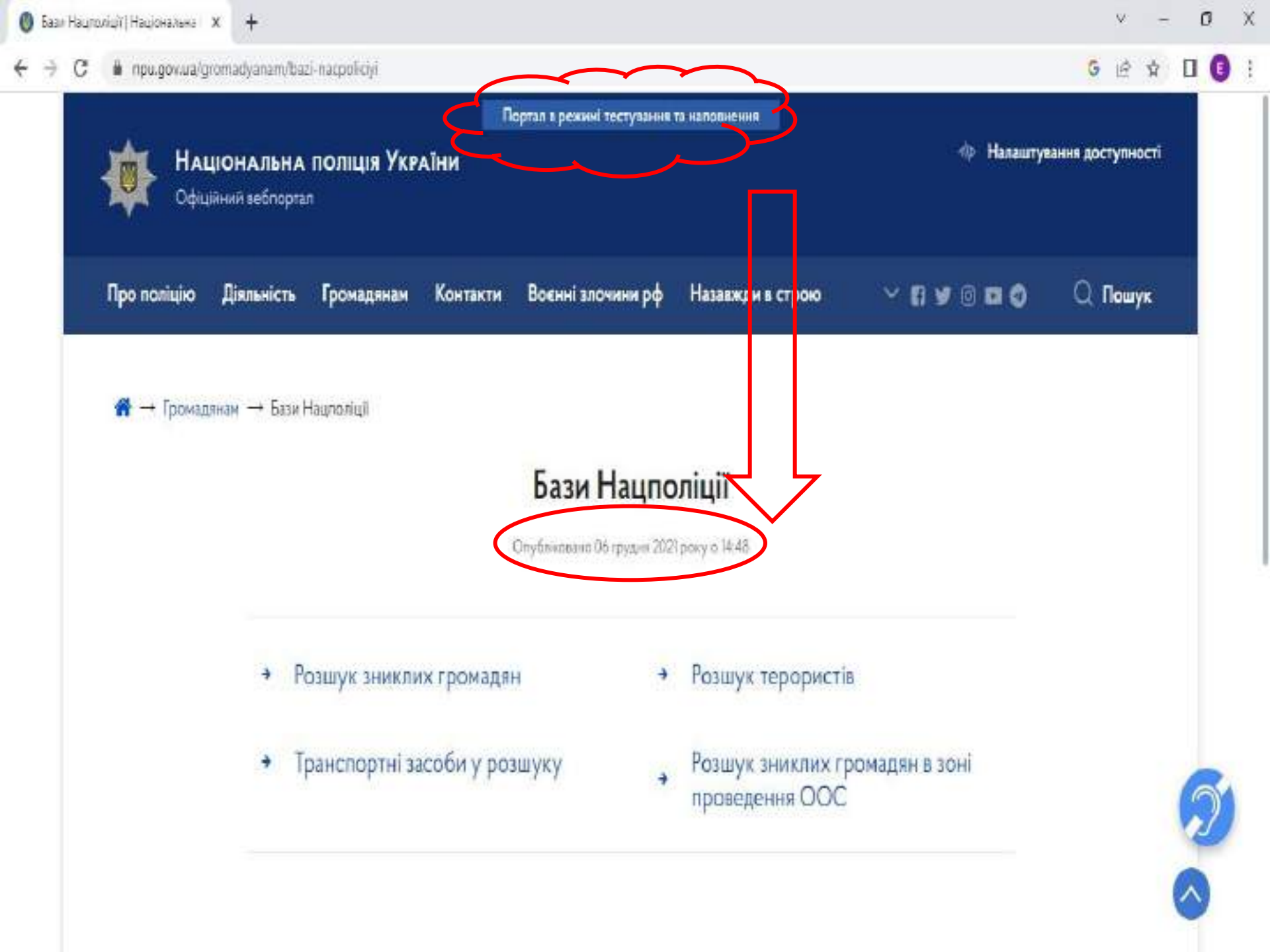
Поліція вживає всіх заходів для недопущення будь-яких порушень прав і свобод людини, пов'язаних з обробкою інформації.

Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації.

Міністерство внутрішніх справ України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами (банками) даних.

Бази даних на веб-порталі Національної поліції України




Бази Нацполіції | Національна
npu.gov.ua/gromadyanam/bazi-nacpolitsiyi
Портал в режимі тестування та наповнення
Національна поліція України
Офіційний вебпортал
Налаштування доступності
Про поліцію
Діяльність
Громадянам
Контакти
Воєнні злочини рф
Назавжди в строю
Пошук
Громадянам → Бази Нацполіції
Бази Нацполіції
Опубліковано 06 грудня 2021 року о 14:48
Розшук зниклих громадян
Розшук терористів
Транспортні засоби у розшуку
Розшук зниклих громадян в зоні проведення ООС

Бази даних на веб-порталі Національної поліції України
https://npu.gov.ua/

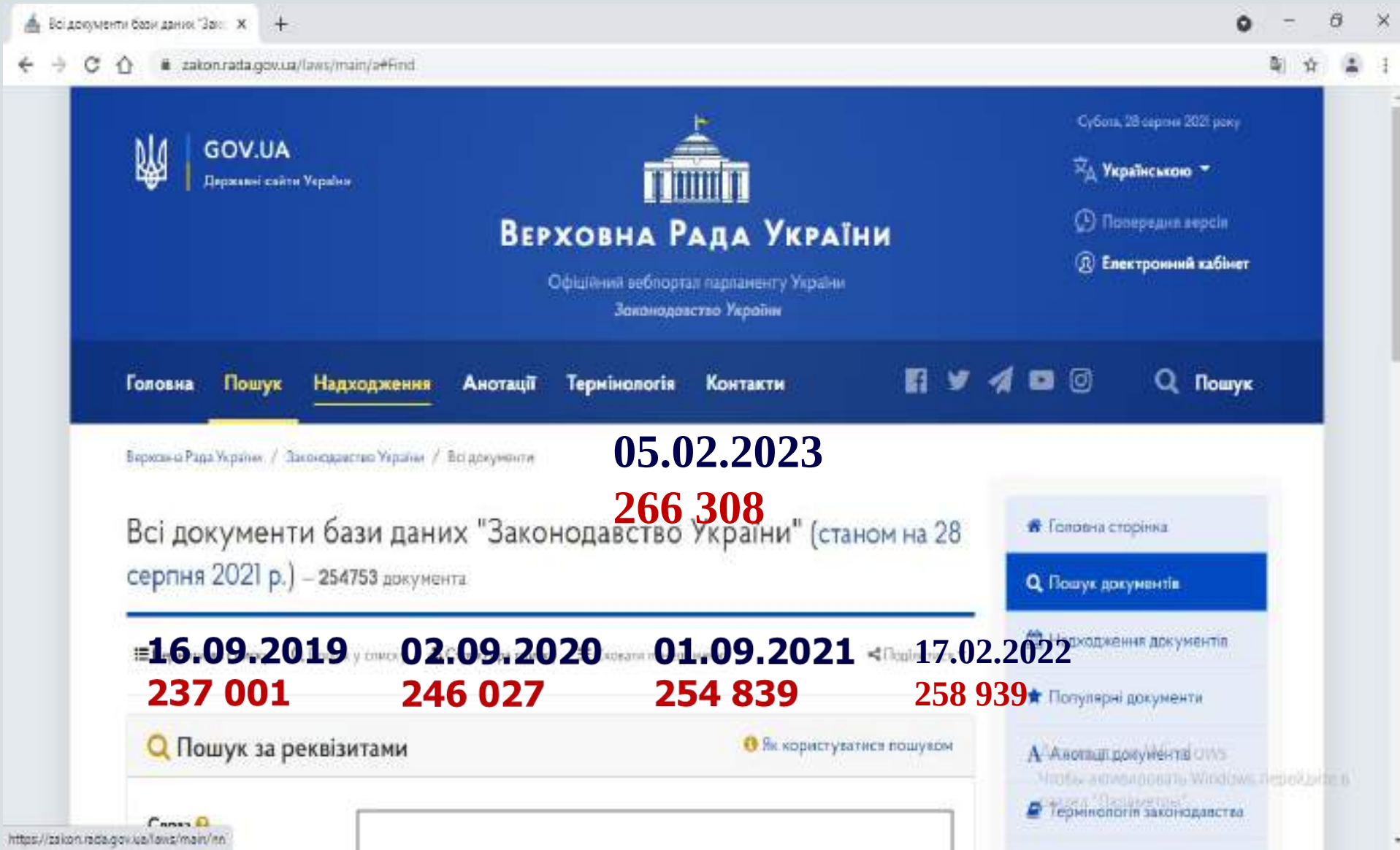
1. Транспортні засоби у розшуку.
2. Розшук зниклих громадян.
3. Розшук терористів.
4. Розшук зниклих громадян в зоні проведення ООС.

Питання:

4. Основні інформаційні ресурси інших державних органів України

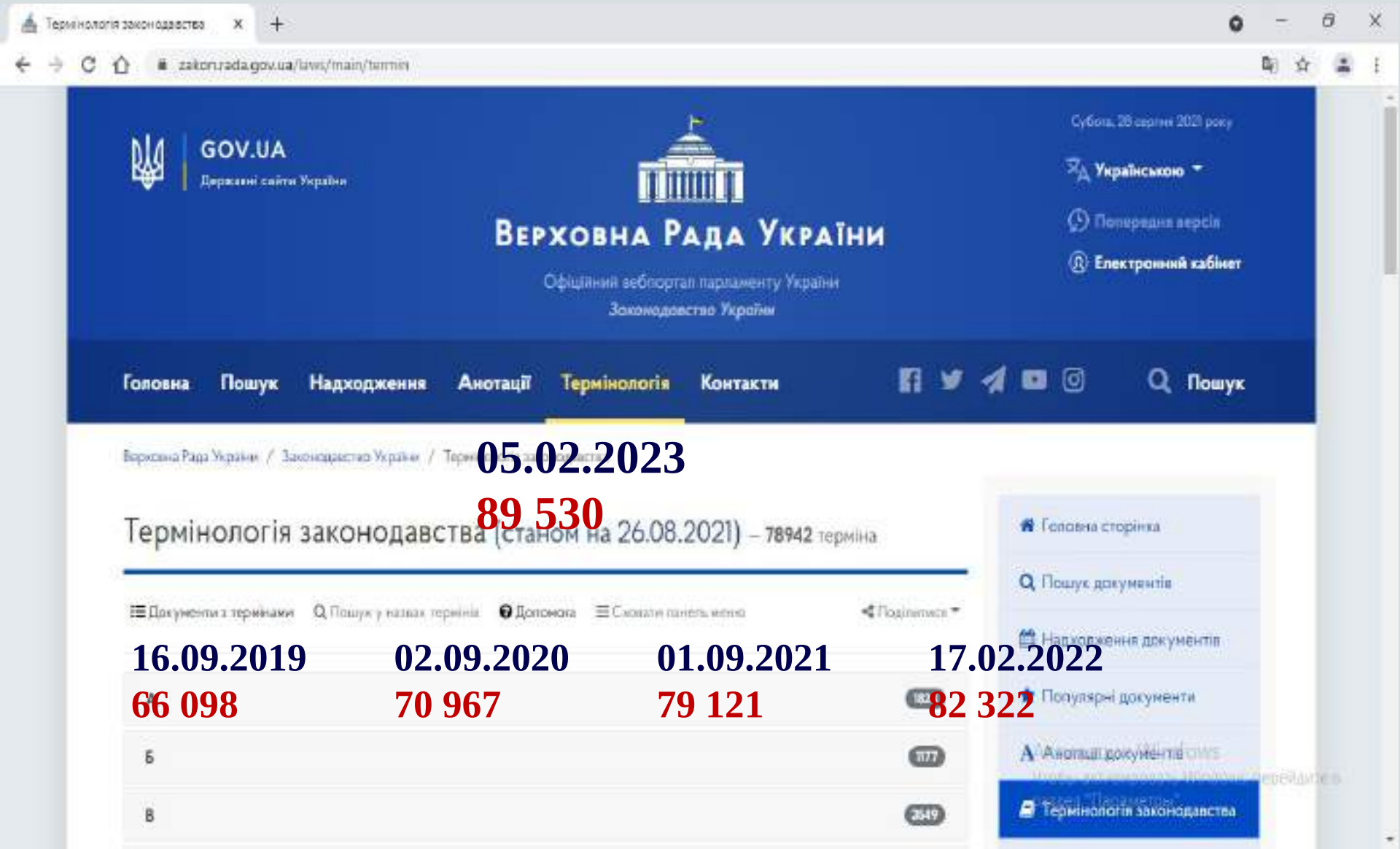
ВЕБ-ПОРТАЛ ВЕРХОВНОЇ РАДИ УКРАЇНИ

Інформаційно-пошукова система «Законодавство»



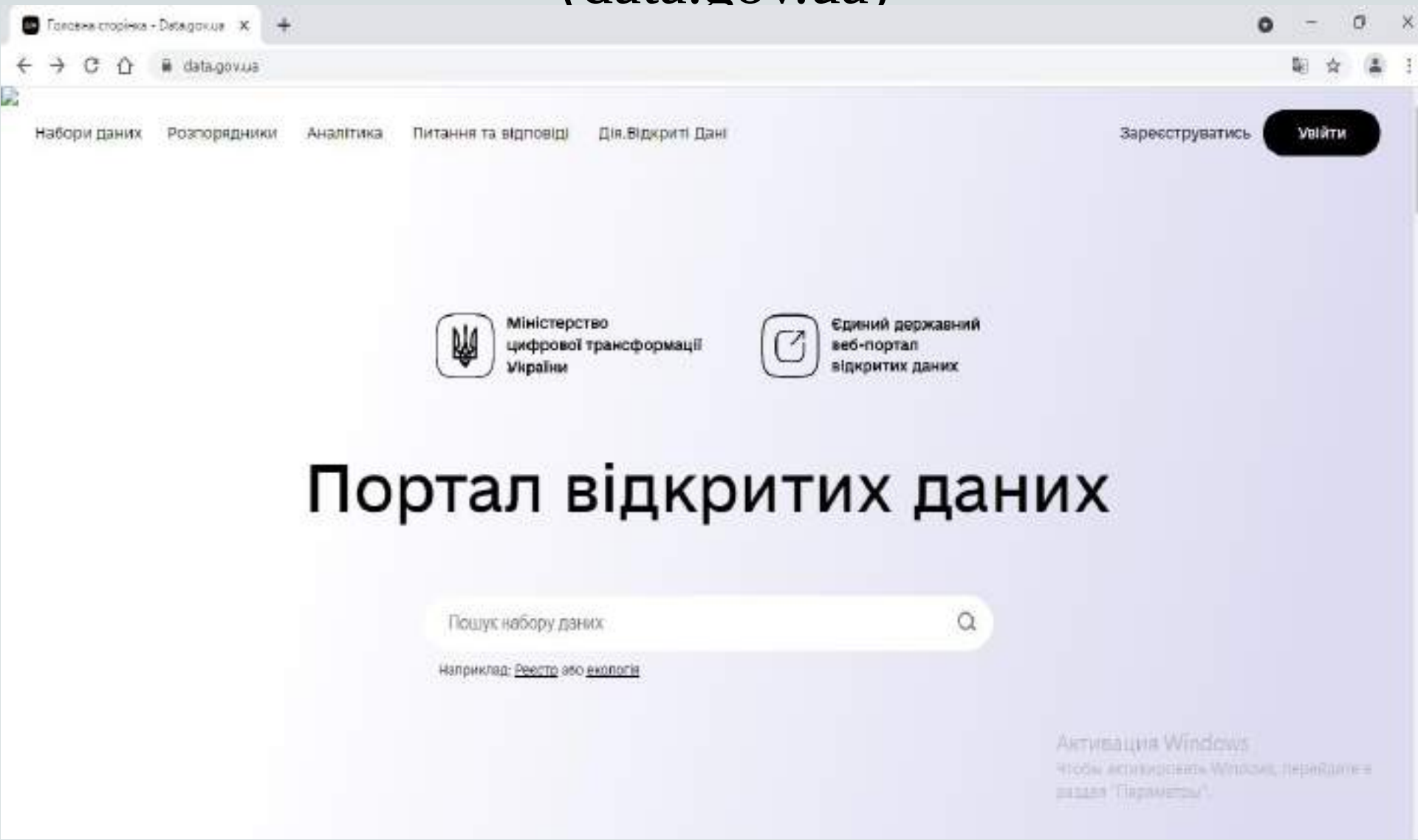
ВЕБ-ПОРТАЛ ВЕРХОВНОЇ РАДИ УКРАЇНИ

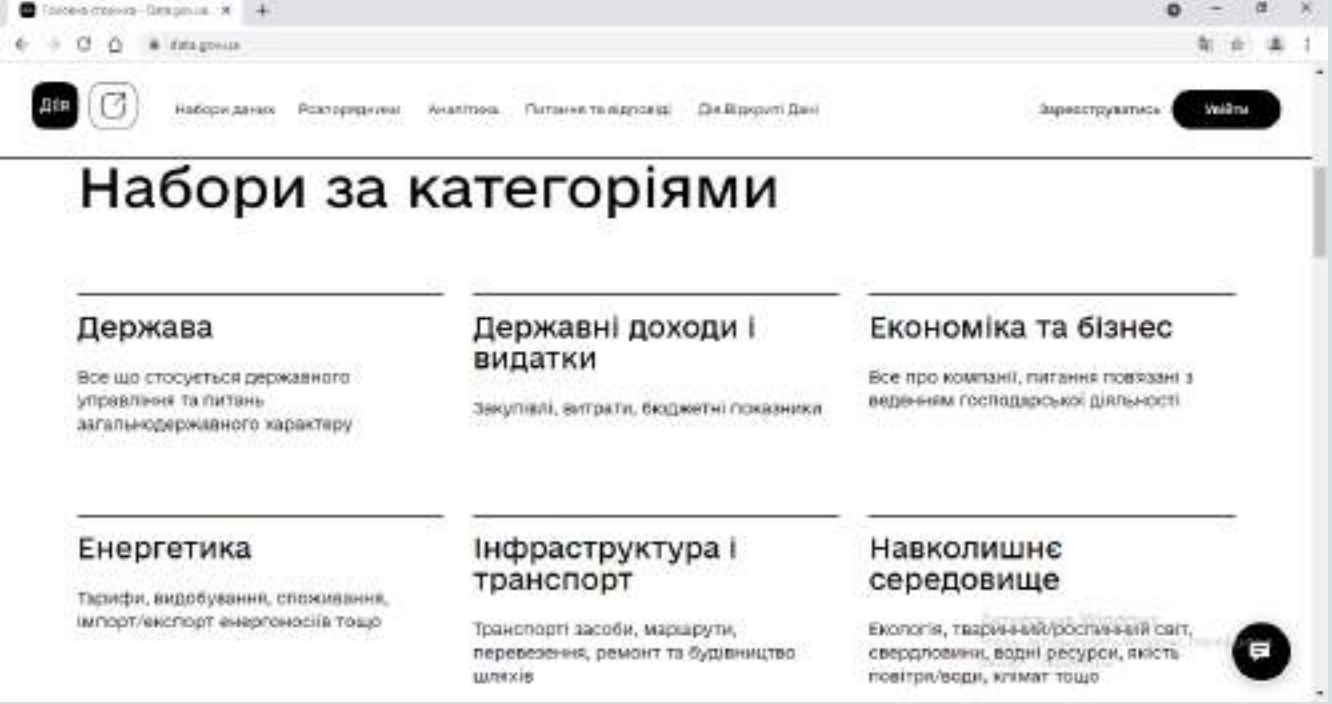
Інформаційно-пошукова система «Законодавство»



МІНІСТЕРСТВО ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УКРАЇНИ

(data.gov.ua)

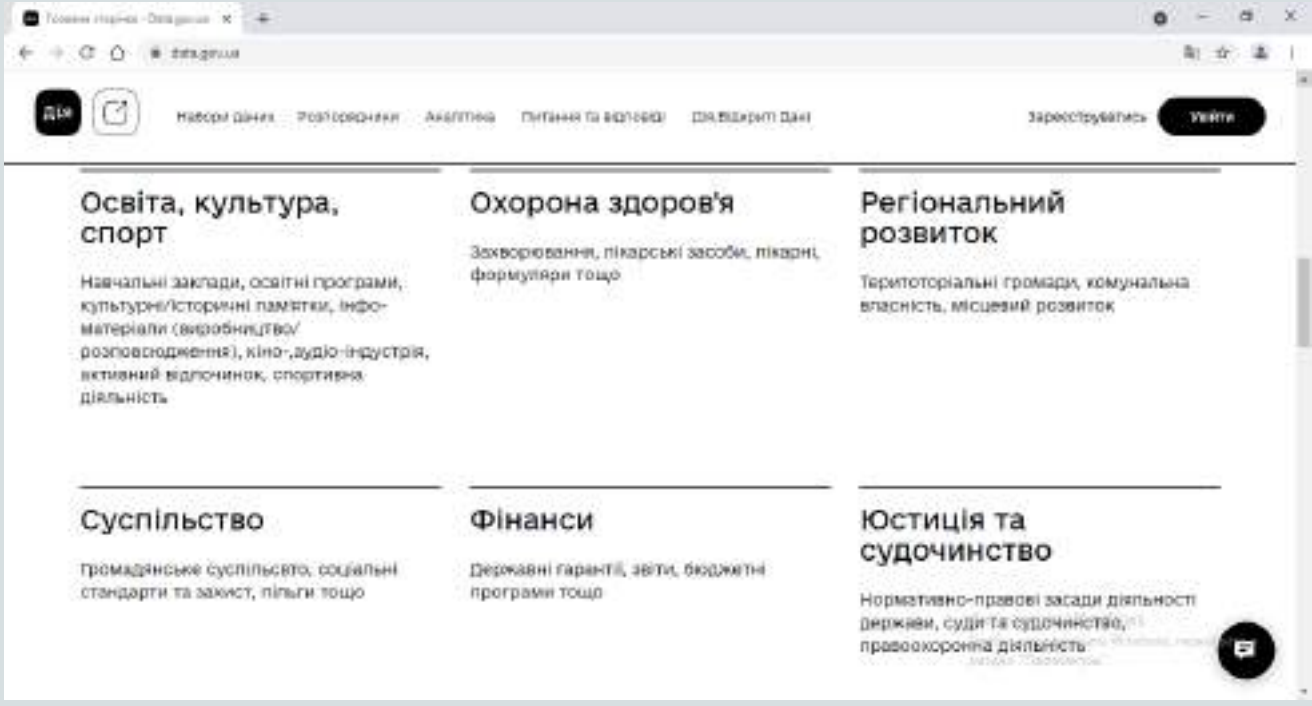




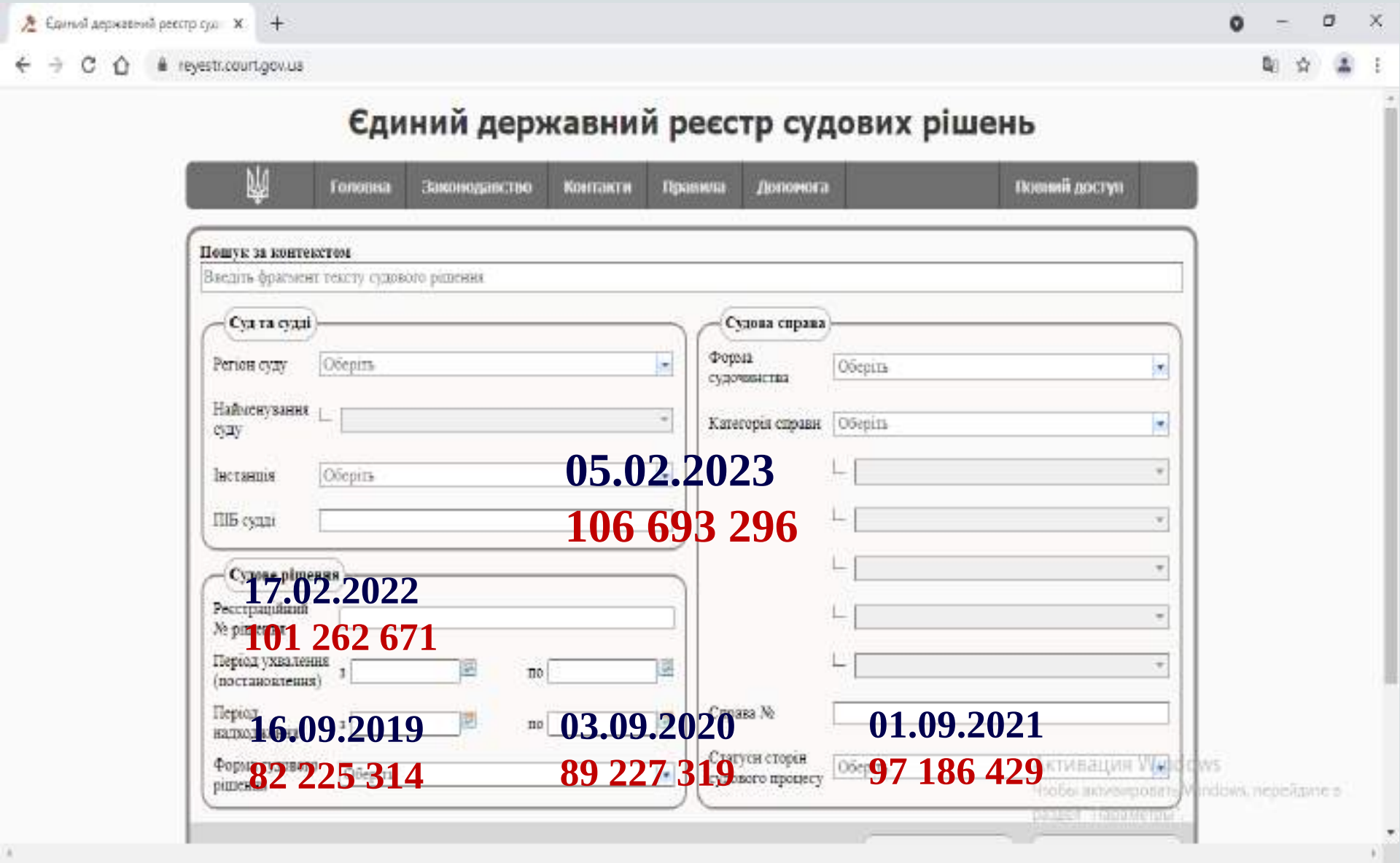
05.02.2023
29 281

17.02.2022
40 955

01.09.2021
38 722



ВЕБ-САЙТ «ЄДИНИЙ ДЕРЖАВНИЙ РЕЄСТР СУДОВИХ РІШЕНЬ»



Банки даних Генерального секретаріату Інтерполу

1. Інформацію про осіб.
2. Інформацію про транспортні засоби, які перебувають у розшуку.
3. Інформацію про плавзасоби, які перебувають у розшуку.
4. Інформацію про викрадені, втрачені, підроблені, недійсні документи, що підтверджують громадянство, посвідчують особу чи її спеціальний статус.
5. Інформацію про твори мистецтва / культурні цінності.
6. Інформацію про вогнепальну зброю.
7. Сліди рук, вилучені з місць вчинення злочину;
8. Дактилоскопічні карти.
9. ДНК-профілі.
10. Зображення дітей, які зазнали сексуальної експлуатації.
11. Інші дані.

Правоохоронні органи України отримують інформацію з банків даних Інтерполу

1. Безпосередньо - за наявності прямого доступу до відповідних банків даних (у тому числі під час здійснення прикордонного контролю).

2. Шляхом надсилання запиту до уповноваженого підрозділу або уповноваженого територіального підрозділу.

Генеральний секретаріат Інтерполу здійснює публікацію оповіщень різних кольорів, наприклад: червоного, синього, зеленого, жовтого, чорного, пурпурного, помаранчевого.

САЙТ МІНІСТЕРСТВА ЮСТИЦІЇ УКРАЇНИ

ЕЛЕКТРОННІ СЕРВІСИ

ДЕРЖАВНІ РЕЄСТРИ

1. Єдиний державний реєстр судових рішень.
2. Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
3. Державний реєстр речових прав на нерухоме майно.
4. Єдиний державний реєстр осіб, які вчинили корупційні правопорушення.
5. Єдиний реєстр нотаріусів.
6. Єдина база даних електронних адрес, номерів факсів, телефаксів суб’єктів владних повноважень.
7. Реєстр громадських об’єднань тощо.

ВИСНОВКИ

Розглянули на лекції 1:

1) мету, завдання та структуру дисципліни;
2) поняття єдиної інформаційної системи МВС;
3) поняття системи інформаційного забезпечення Національної поліції;
4) основні інформаційні ресурси інших державних органів України (ВРУ, ЄДРСР, Інтерполу, МЮ).

Розглянемо на лекції 2:

можливості ІТС «Інформаційний портал НПУ».

Online-тестування

Тема 1: «Нормативно-правове регулювання у сфері інформаційних відносин. Система інформаційного забезпечення Національної поліції України»

Пам'ятайте

Під час виконання практичних завдань пам'ятай про правила безпеки життєдіяльності при роботі з комп'ютером!

Крок 1. Створити новий документ Word виконавши команду *Файл-Створити-Новий документ* або необхідно виконати команду *Ctrl + N*.

Крок 2. Встановити параметри документа: шрифт – Times New Roman; кегль – 14; інтервал – 1; поля: верхнє, нижнє: 2 см, ліве: 3 см, праве: 1 см.

Крок 3. Використовуючи розшукові обліки МВС України встановити осіб, що зображені на фотографіях на про них відомості, що зазначені нижче:

1. Ім'я та прізвище особи
2. Дата народження
3. Місце народження
4. Професійні дані
5. Остання геолокація (місто, країна)
6. Контакти, активність у соціальних мережах

Фото 1

Фото 2

Фото 3

Крок 4. Скласти інформаційну довідку щодо зібраної інформацію на встановлених осіб, вказавши дані у вигляді скріншотів та URL-адрес (*зразок додається нижче*). Презентувати результати роботи.

Крок 5. Встановити пароль на документ, виконавши команду *Файл- Відомості-Захист документа-Зашифрувати та встановити пароль.*

Крок 6. Зберегти документ як «Ваше Прізвище – П.з. 1.1» у папці «Тема 1», виконавши команду *Файл-Зберегти як*.

(Приклад інформаційної довідки)

ІНФОРМАЦІЙНА ДОВІДКА

Дійсним доповідаю, щодо у ході здійснення пошуку інформації у мережі Інтернет щодо встановлення осіб по фотографіях, використовуючи розшукові обліки МВС України виявлено наступне:

Фото 1

№ з/п	Відомості	URL-адреси, скріншоти
1.	Ім'я та прізвище особи	
2.	Дата народження	
3.	Місце народження	
4.	Професійні дані	
5.	Остання геолокація (місто, країна)	
6.	Контакти, активність у соціальних мережах	

Фото 2

№ з/п	Відомості	URL-адреси, скріншоти
…	…	…

Фото 3

№ з/п	Відомості	URL-адреси, скріншоти
…	…	…

Слідчий слідчого відділу
Васильківського РУП
ГУНП в Київській області
лейтенант поліції **Ірина КРАВЧУК**
____._____.2024

НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки ННІ № 1

Мультимедійна презентація

Тема: «Безпека роботи з інформацією»

ЗМІСТ

- Визначення кібергігієни
- Основні типи кібератак
- Сучасна класифікація хакерів
- Фундаментальні кіберзагрози
- Основні принципи виявлення загрози безпеки
- Основні правила кібергігієни
- Використання надійних паролів
- Види паролів
- Безпека користування Wi-Fi

Вступ

- Тотальна цифровізація усіх процесів щодня робить потенційними жертвами кіберзлочинців все більшу кількість користувачів мережі.

- Інтернет-банкінг, соціальні мережі, e-mail розсилки - усе це є інструментом для кібератак, тому важливо знати, на що звертати увагу та як реагувати на загрози.

Визначення кібергігієни

КІБЕРГІГІЄНА — це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації.

Кожна людина повинна захищати свої персональні дані, інформацію і обчислювальні пристрої.

Типи кібератак

- Вейлинг
- Викрадач браузеру
- Фішінг
- Фармінг
- Шпигунське/рекламне програмне забезпечення
- Спам
- Вішинг

ВЕЙЛИНГ – використання електронної пошти, системи миттєвого обміну повідомленнями чи соціальними мережами для збирання особистої інформації (наприклад, облікових даних для входу) керівників вищої ланки.

ФІШИНГ – використання електронної пошти, системи миттєвого обміну повідомленнями чи соціальних мереж для збирання особистої інформації (наприклад, облікових даних для входу), у якому зловмисник видає себе за довірену особу.

ШПИГУНСЬКЕ/РЕКЛАМНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ – шкідливий код, який передається електронною поштою або через завантаження з Інтернету і може використовуватися для збору інформації про користувача або встановлення рекламних банерів у програми, веб-браузери або веб-сторінки.

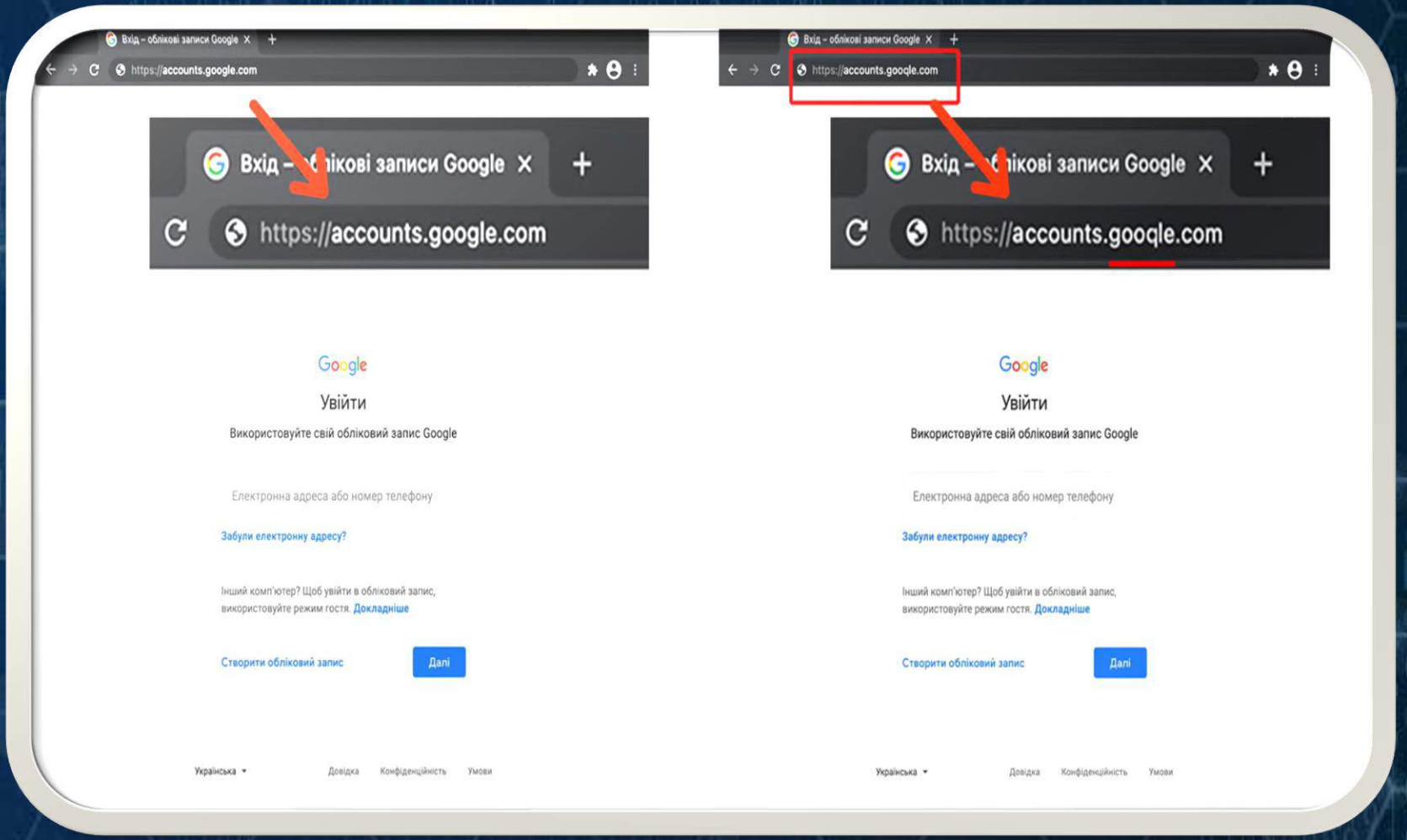
ВІШИНГ – використання голосового зв'язку для збирання особистої інформації (наприклад, облікових даних при вході), у якому зловмисник видає себе за довірену особу.

ФАРМІНГ - використання підробленої копії довіреного сайту збору особистої інформації (наприклад, облікових даних при вході).

СПАМ – спам або небажана пошта, яка використовується для розсилки реклами, шкідливих посилань та програм або шахрайського контенту.

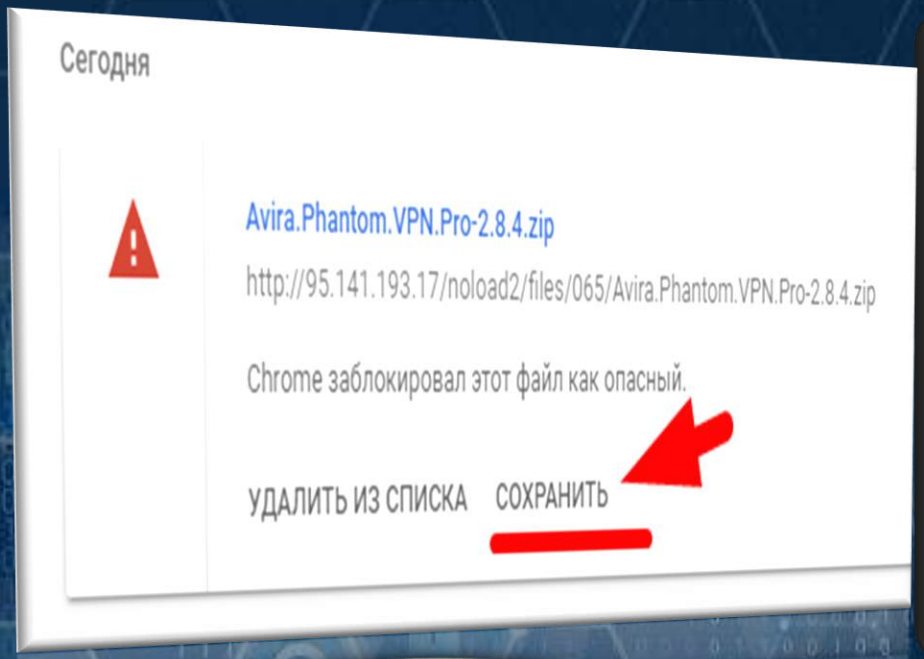
ВИКРАДАЧ БРАУЗЕРУ – шкідливий код, який змінює конфігурацію браузеру.

Приклади



Кібершахраї намагаються видавати себе за реальні ресурси, змінюючи літери у назві домену для заволодіння особистими даними.

Головною метою зловмисників є донесення до кінцевого користувача рекламного продукту.



Дестабілізація роботи пристроїв та доступ до віддаленого доступу.

Сучасна класифікація хакерів

ХАКЕРИ-ДИЛЕТАНТИ («скрипт-кідді»)	Термін з'явився в 1990 році і відноситься до підлітків або недосвідчених хакерів, які використовують існуючі сценарії, інструменти та експлойти для заподіяння шкоди. Зазвичай правопорушення немає мети отримання прибутку.
БРОКЕР ВРАЗЛИВОСТЕЙ	Хакер, який намагається виявити вразливі місця для кібератак та повідомити про них продавцям, іноді за винагороду.
ХАКТИВІСТИ	Хакери, які підтримують будь-які політичні та соціальні ідеї, а також публічно протестують проти організацій чи урядів, публікуючи статті, відеоролики, організуючи виток конфіденційної інформації та розподіляючи атаки типу «відмова в обслуговуванні».

Сучасна класифікація хакерів

КІБЕРЗЛОЧИНЦІ

Зловмисники, які з метою неправомірного використання комп'ютеру, мережі Інтернет або мережевого пристрою здійснюють злочини у кіберпросторі.

СПОНСОВАНІ ДЕРЖАВОЮ

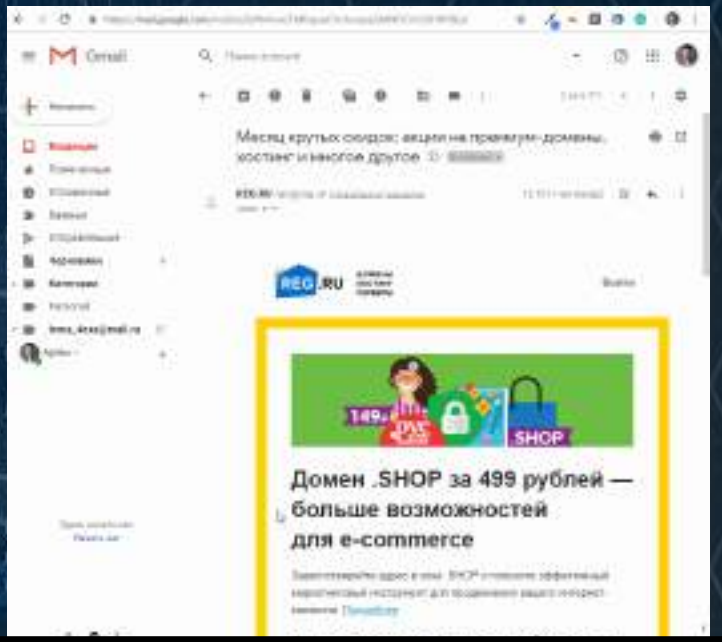
Хакери, які займаються крадіжками державних секретів, збиранням розвідувальних даних та саботажем мережевих інфраструктур. Їхньою метою є іноземні уряди, терористичні групи та корпорації.

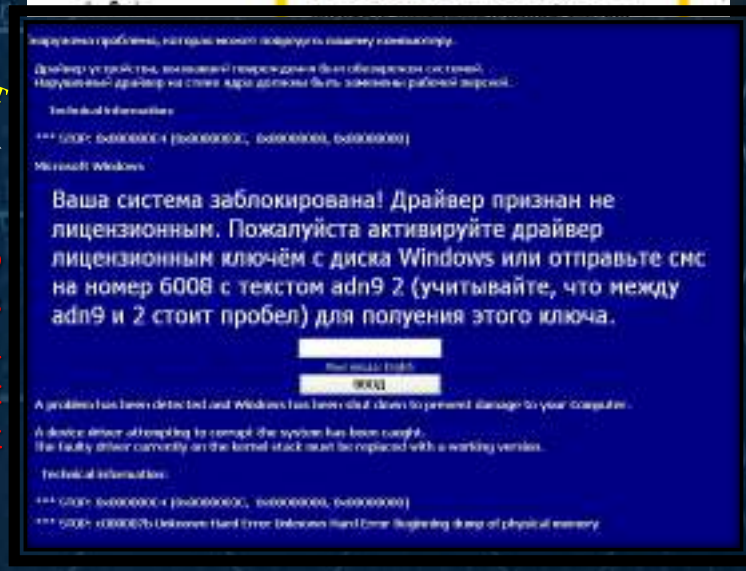
Як працюють хакери?

Приклад кібератаки

Зловмисник:
Обізнаний хакер, який відправляє шпіонське програмне забезпечення

Користувачі:
Недосвідчені особи, які використовують програмне забезпечення на своїх пристроях, яким загрожує небезпека





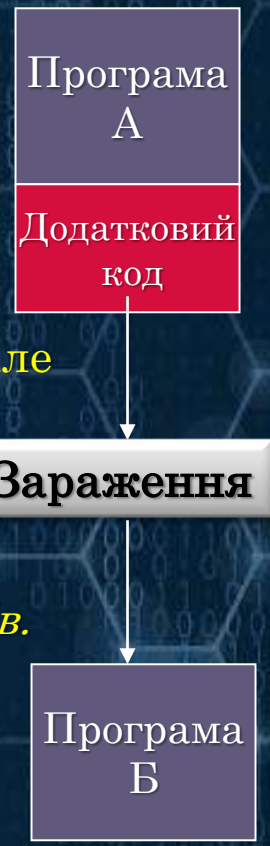
Вартість розробки програмного забезпечення 1-2 тис. $. Прибуток хакерів за розсилку програмного забезпечення на 1 млн адресів електронної пошти становить 8 тис. $. 10 000 ПК зламаних шпіонськими програмами - 1 тис. $.

Фундаментальні кіберзагрози

- Віруси
- Хробаки
- Троянські коні / Логічні бомби
- Соціальна інженерія
- Руткіти
- Ботнети

Віруси

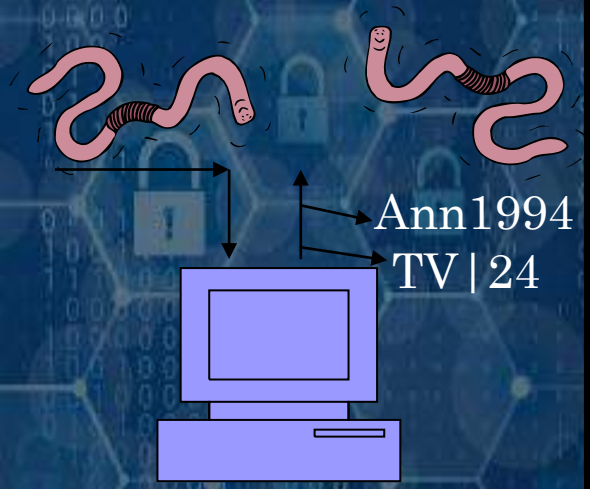
ВІРУСИ - шкідливий виконуваний код, вкладений у виконуваний файл, наприклад легітимну програму.



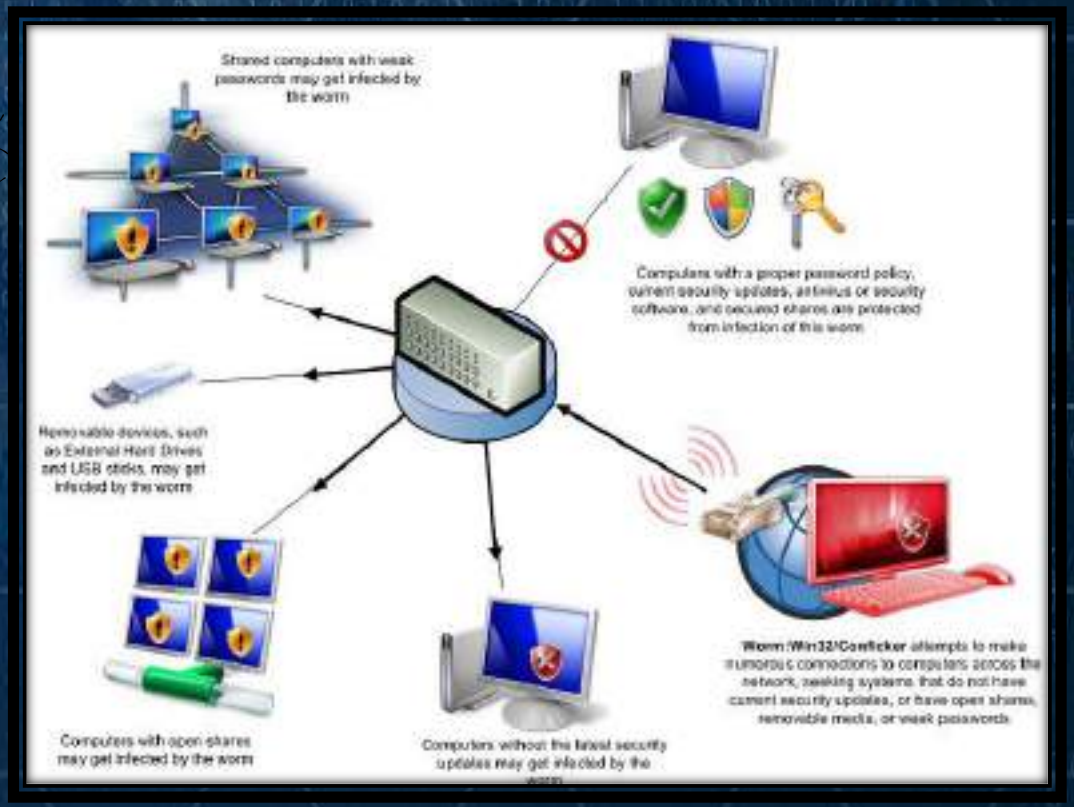
- Вірус приєднується до програми, файлу або дисків.
- Коли програма виконується, вірус активується та копіює себе.
- Вірус може бути доброякісним або злоякісним, але в певний момент виконує свою функцію.
- *Віруси можуть викликати збої комп'ютера та втрату даних.*
- Щоб відновити або запобігти вірусним атакам:
- *Уникайте потенційно ненадійних веб-сайтів/електронних листів.*
- *Перевстановіть операційну систему.*
- *Користуватися та підтримувати антивірусне програмне забезпечення.*

Хробаки

ХРОБАКИ - шкідливий код, який самостійно створює свої копії, використовуючи вразливість мережної інфраструктури.



Email лист:
Ann1994@gmail.com
TV|24@urk.net



Троянські коні / Логічні бомби

ТРОЯНСЬКІ КОНІ - програми, які здійснюють шкідливі операції під прикриттям, тихо знищуючи дані або пошкоджуючи вашу систему.

Наприклад: Завантажена гра чи програма може містити прихований код, який збирає особисту інформацію без відома користувача.

ЛОГІЧНА БОМБА - логіка шкідливого програмного забезпечення виконується за певних умов. Програма часто використовується з інших законних причин.

Наприклад: Програмне забезпечення, яке виходить з ладу, якщо плата за обслуговування не сплачена. Співробітник ініціює стирання бази даних, коли його звільняють.

Соціальна інженерія

СОЦІАЛЬНА ІНЖЕНЕРІЯ – атака, здійснення маніпуляції людьми з метою виконання дій або розголошення конфіденційної інформації, отримання доступу до комп'ютерних систем обманним шляхом.

Соціальний інженер:
Вітаю, це Тарас зі служби безпеки банку. Ваш банківський рахунок заблоковано, для його відновлення Вам необхідно повідомити ваш логін та пароль.

Довірливий клієнт:
Добре, мої логін та пароль …

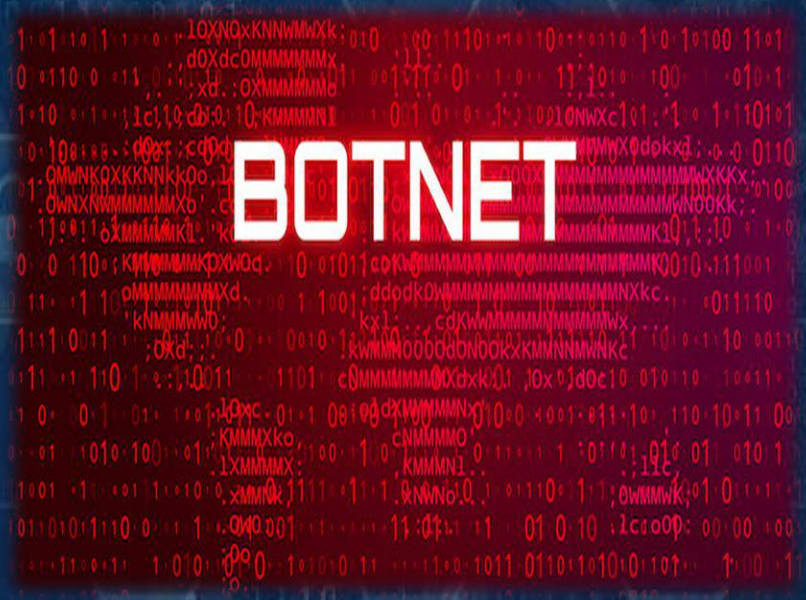
Руткіт

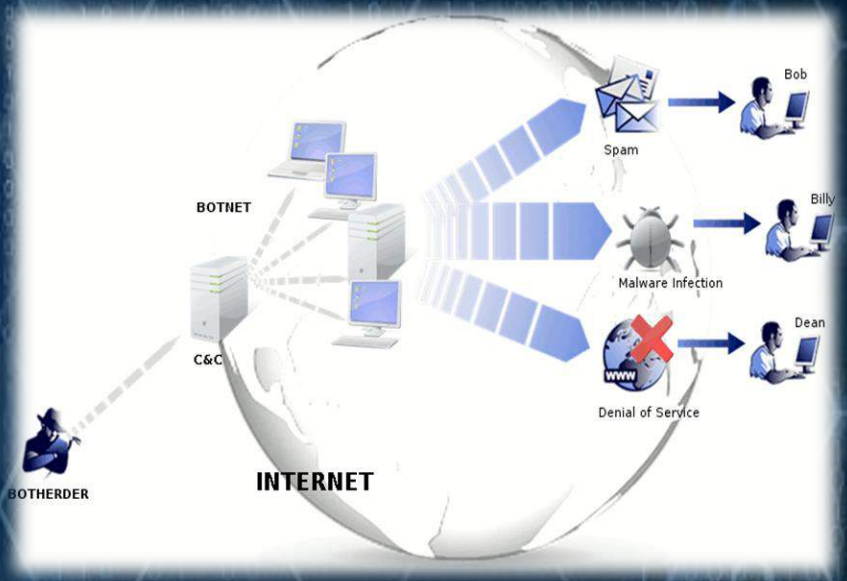
РУТКІТ – шкідливий код, який використовується для несанкціонованого доступу до пристрою через уразливі місця системи.

- Проникнувши на комп'ютер, хакер може встановити набір програм, який називається руткітом.
- Може увімкнути:
  - *Легкий доступ для хакера (та інших) до бази даних підприємства*
  - *Реєстратор натискань клавіш*
- Змінює операційну систему
- Усуває ознаки злому

Ботнет

БОТНЕТ – це ряд скомпрометованих комп'ютерів, які використовуються для створення та розсилки спаму чи вірусів, або для заповнення мережі повідомленнями у вигляді атаки «відмови в обслуговуванні».





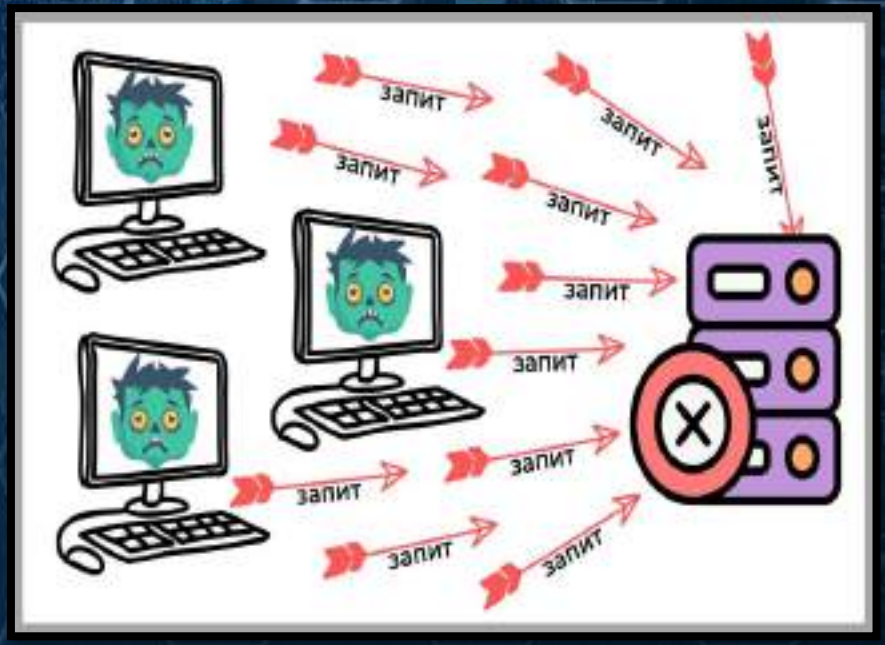
За допомогою Botnet можливо атакувати та відключати веб-сайти. При таких атаках кіберзлочинці перевантажують веб-сайт великою кількістю відправлених запитів (DDOS-атак), які сервер сайту не в змозі обробити.

Що означає DDoS?

Distributed	→	Розподілена
Denial	→	Відмова
of	→	в
Service	→	Обслуговуванні

DDoS-атака — це масоване бомбардування сервера одночасними сміттєвими запитами, які виснажують ресурси оперативної пам'яті та повністю забивають трафік. Наприклад, атака призводить до відмови в обслуговуванні через перевантаженість каналу веб-сайт перестає відповідати справжнім відвідувачам або зовсім відключається.

Кіберзлочинці можуть захопити мільйони електронних пристроїв по всьому світу для створення цифрової армії та здійснювати DDoS-атаки.



Виявлення загрози безпеки

Симптоми:

- Антивірусне програмне забезпечення виявляє проблему.
- Місце на диску несподівано зникає.
- Несподівано з’являються спливаючі вікна, іноді продають програмне забезпечення безпеки.
- З'являються файли або транзакції, яких там не повинно бути.
- Комп’ютер сповільнюється до повзання.
- Незвичайні повідомлення, звуки або зображення на моніторі.
- Вказівник миші рухається сам по собі.
- Комп’ютер спонтанно вимикається або перезавантажується.
- Часто нерозпізнані або ігноровані проблеми.

Основні правила кібергігієни

- **Перевірка безпеки активних акаунтів**

Перевірка безпеки вже існуючих облікових записів електронної пошти та акаунтів в соцмережах. Зокрема, такі веб-сайти, як haveibeenpwned.com та breachalarm.com допоможуть з'ясувати чи був пароль до електронної пошти викрадений зловмисниками

- **Аналіз програм**

Проаналізувати вже завантажені додатки, видалити непотрібні, та в подальшому контролювати встановлення кожної програми. Також під час завантаження кожного додатку варто звертати увагу на дозволи, які ви надаєте. Часто шкідливі програми надсилають запит на отримання великої кількості дозволів, які не відповідають їх функціоналу. Це дозволяє збирати багато інформації про користувача, з метою отримання прибутку.

- **Регулярне оновлення**

Для запобігання інфікуванню шкідливими програмами варто здійснювати своєчасне оновлення операційної системи та окремих додатків, які передбачають виправлення вразливостей та помилок в програмному забезпеченні.

- **Надійний пароль**

З метою запобігання несанкціонованому доступу до пристроїв, переконайтеся у надійності ваших паролів. Важливо створити складну комбінацію, яка міститиме не менше 10 символів, великі та малі літери, цифри та символи. Крім цього, для кожного акаунта варто використовувати унікальний пароль.

- **Додатковий рівень захисту**

Для покращення безпеки облікових записів, використовуйте двофакторну аутентифікацію, яка передбачає підтвердження особистості під час входу в певний акаунт. Найчастіше для цього використовуються SMS-повідомлення або окрема програма. Таким чином, у разі викрадення пароля зловмисники не зможуть отримати доступ до ваших даних.

- **Регулярне резервне копіювання**

Необхідним кроком для уникнення втрати важливих даних є регулярне резервне копіювання інформації на зовнішній жорсткий диск або хмару. Це допоможе відновити потрібні дані у разі їх шифрування програмою вимагачем або видалення шкідливим програмним забезпеченням.

- **Надійний захист**

Використання надійного рішення для захисту комп'ютера чи смартфона від шпигунських програм, фішинг атак, вірусів.

Антивірусне та антишпигунське програмне забезпечення

- Антивірусне програмне забезпечення виявляє певні типи зловмисного програмного забезпечення та може знищити його до того, як буде завдано будь-якої шкоди.
- Встановлення та обслуговування антивірусного та антишпигунського програмного забезпечення.
- Обов'язково оновлюйте антивірусне програмне забезпечення.
- Існує багато безкоштовних і комерційних варіантів.
- Зверніться по допомогу до свого спеціаліста з технічної підтримки.

Norton from symantec
McAfee
KASPERSKY lab
AVG Anti-Virus
avast! be free
AVIRA
NOD32 antivirus
bitdefender secure your every bit
TREND MICRO
F-Secure
eset
G DATA

Використання надійних паролів

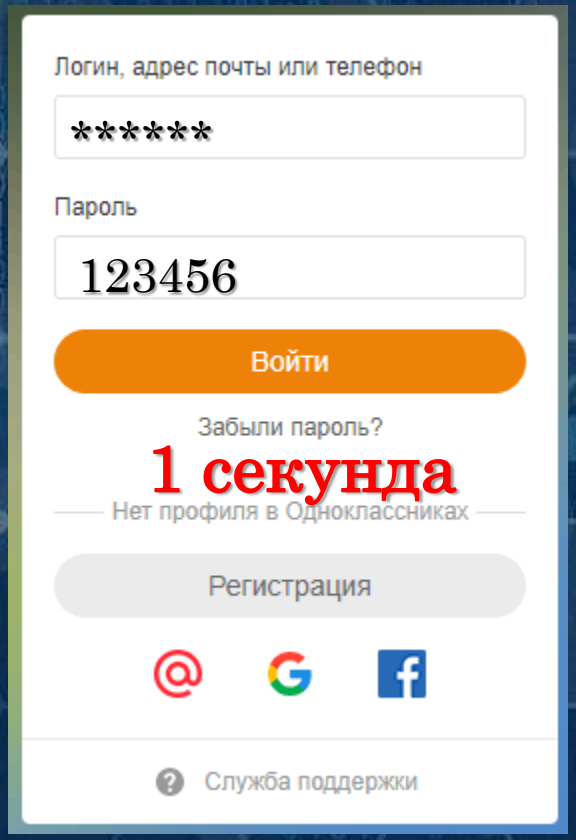
Стандарти створення паролів:

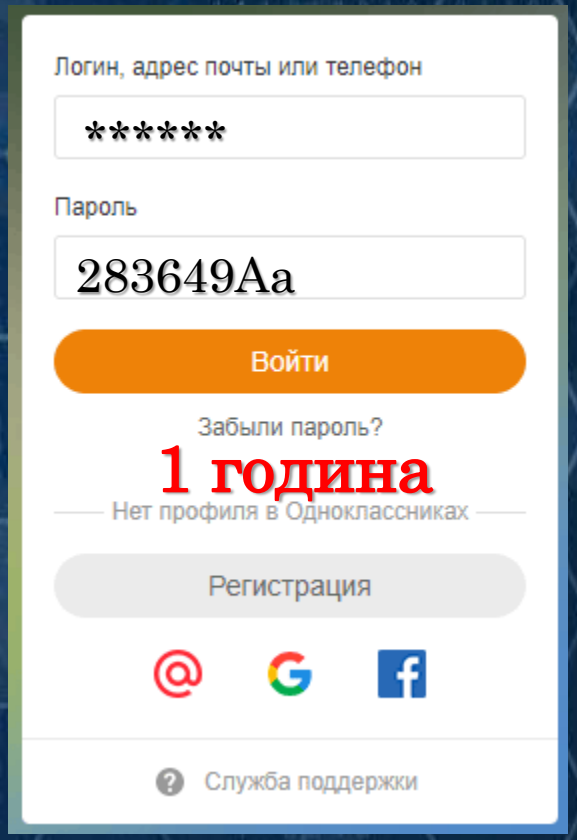
- Довжина не менше 10-ти символів
- Повинен містити символи принаймні двох із наступних чотирьох типів символів:
  - Англійська верхній регістр (A-Z)
  - англійська нижній регістр (a-z)
  - Цифри (0-9)
  - Спеціальні символи ($, !, %, ^, …)
- Не повинен містити ім’я користувача або частину імені користувача
- Не повинен містити легкодоступну або вгадувану особисту інформацію про користувача або сім’ю користувача, наприклад, дні народження, імена родичів, адреси тощо
- Регулярно змінюйте, чим частіше, тим краще!

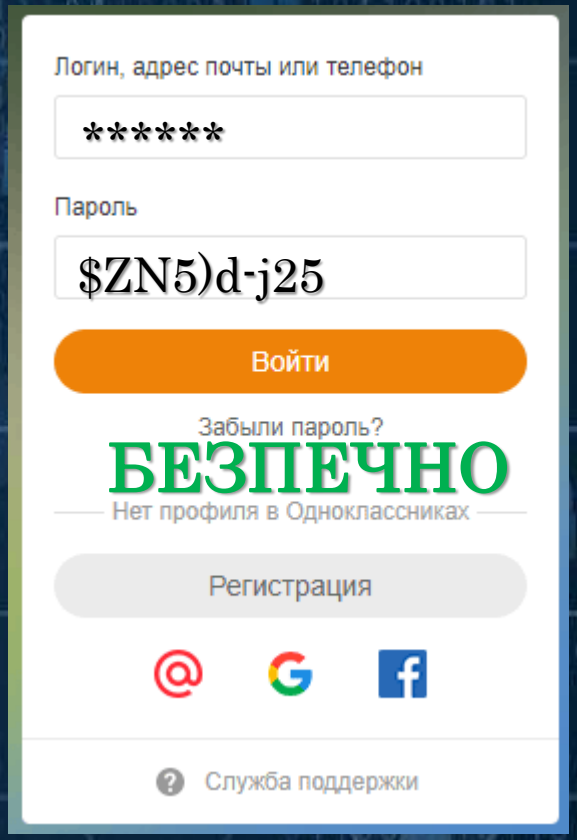
БУДЬТЕ КРЕАТИВНИМИ ПІД ЧАС СТВОРЕННЯ ПАРОЛІВ!

Скільки часу потрібно хакеру для зламування паролів?

Приклад підбору паролів





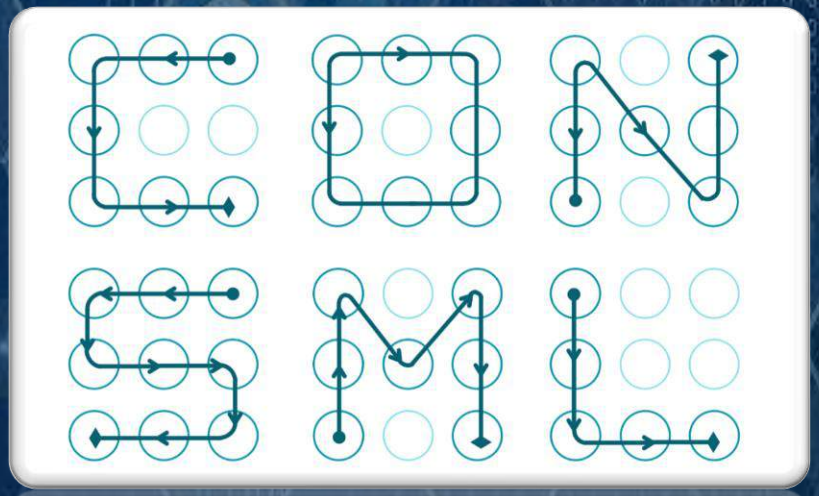


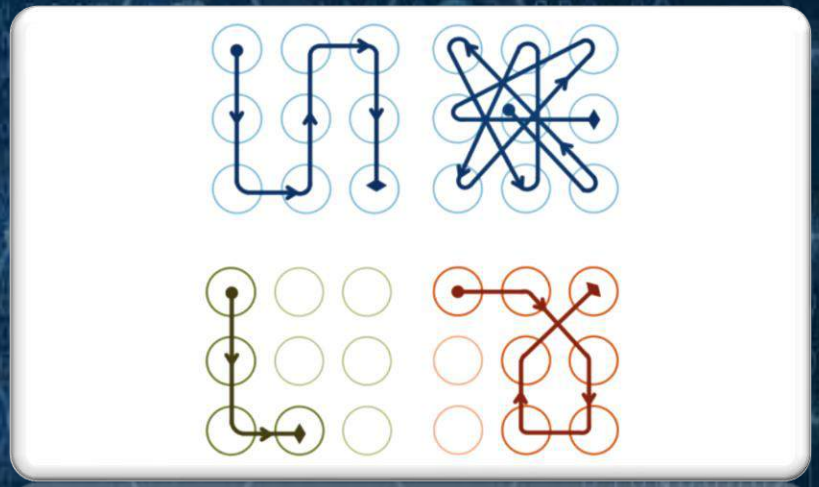
Сервіс для перевірки надійності паролю:
www.passwordmonster.com

Графічні паролі

Серед найбільш популярних способів захисту мобільних пристроїв є графічний ключ

Графічний пароль – це тип пароля, при якому користувач повтрює деякий малюнок із заздалегідь вибраними жестами.

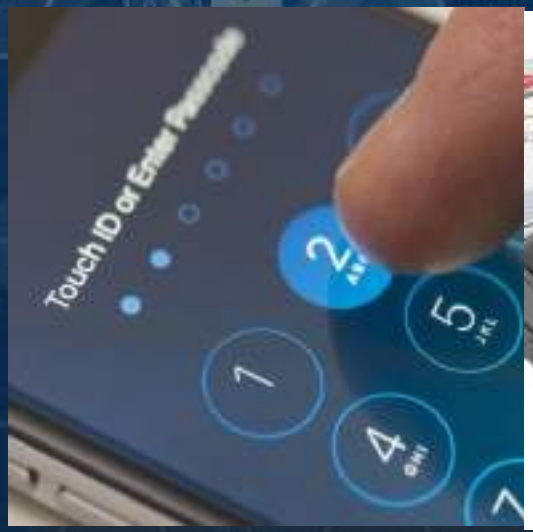




Цифрові паролі

Цифрові паролі або пінкод – це пароль, який складається тільки з цифр.

Часто використовується там, де використання повноцінної клавіатури технічно ускладнене або недоречне.



Тактильні паролі

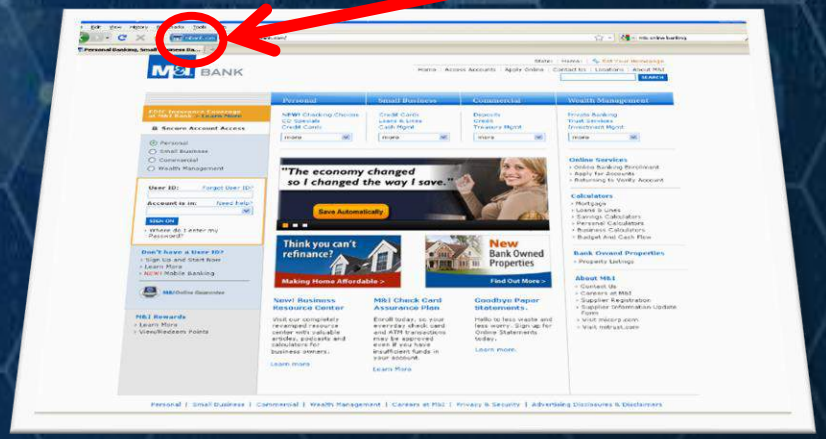
В якості пароля використовується відбиток пальця.

Відбитки пальців людини є детальними, майже унікальними, складними до змінювання та стійкими впродовж життя людини, що робить їх придатними для використання у якості ідентифікатора особи.

Зчитування пароля здійснюється спеціальним сенсором.

Безпека користування Wi-Fi

- ✓ Вимкнути автоматичне підключення до мережі
- ✓ Не робити грошових операцій у публічних місцях
- ✓ Не вимикати брандмауер або фаєрвол
- ✓ Використовувати безпечний протокол з'єднання HTTPS
- ✓ Вимкнути загальний доступ до файлових папок
- ✓ Використовувати сервіси VPN
- ✓ Використовувати антивірусні програми

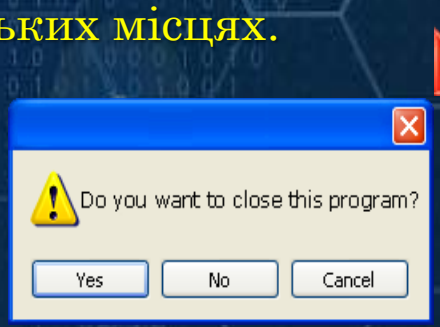


Правила Wi-Fi безпеки

Висновки

«Не піддавайтеся на провокації!»

- Обов'язково встановіть хороший брандмауер або блокувальник спливаючих вікон
- Блокувальники спливаючих вікон не завжди блокують УСІ спливаючі вікна, тому завжди закривайте спливаючі вікна, використовуючи «Х» у верхньому куті.
- Ніколи не натискайте «так», «прийняти» чи навіть «скасувати»
- Заражені USB–накопичувачі часто залишають без нагляду хакерами у громадських місцях.



ONLINE-ТЕСТУВАННЯ

Тема 2. Безпека роботи з інформацією.

Практичне заняття: «Фейк чи маніпуляція?»

Завдання 1. З наведених нижче випадків виявіть різницю між фейком та маніпуляцією.

Випадок 1

Російські ЗМІ повідомили: ЗСУ цілеспрямовано б'ють по дитсадках, коледжах, школах і дитячих лікарнях.

ЗМІ РФ заявили: «компоненти цивільної інфраструктури в космосі, що надаються Україні у військових цілях, можуть стати законною мішенню для удару у відповідь».

Випадок 2

Російські ЗМІ повідомили: «Корупція в Україні викликає серйозне занепокоєння у представників Міноборони США. Київ неналежним чином використовує американську військову допомогу. Частину західної зброї вже знаходили в Африці, куди вони потрапили через контрабанду».

Україна сама спровокувала «спеціальну воєнну операцію», яку проводить Росія на її території.

Випадок 3

Російські ЗМІ повідомили: Українські війська розстріляли групу медиків, які прямували до Вугледара для евакуації поранених.

Посол РФ в Аргентині заявив: «Без накачування України зброєю, «сво» давно б завершилося. Сума військової допомоги Україні вже досягла щонайменше $50 млрд. Постачання не сприяють врегулюванню конфлікту, а лише додатково його розпалюють».

Випадок 4

Луганський колаборант А. Марочко заявив, що «військовослужбовці ЗСУ, дислоковані в населеному пункті Часів Яр, влаштували стрілянину між своїми підрозділами. У цьому районі немає російських військ, там знаходяться лише українські бойовики та найманці».

В МЗС РФ заявили: «Київ неодноразово визнавав, що всі його дії йдуть зі схвалення та підтримки США й інших країн НАТО, вбивства в Брянській області були скоєні з натовської зброї. У зв'язку з цим виникає питання про кваліфікацію цих держав як співучасників таких злочинів та спонсорів тероризму».

Випадок 5

Російські ЗМІ повідомили: полонених захисників «Азовсталі» в Оленівці наприкінці липня обстріляли з РСЗО HIMARS з території України.

Донецький колаборант В. Павлов заявив, що «українські формування під виглядом перевірки документів вриваються до будинків мешканців населеного пункту Лиман, щоб знайти «шпигунів» або тих, хто дотримується проросійських поглядів».

Завдання 2. Враховуючи проаналізовані випадки вигадайте власні варіанти фейкової інформації та маніпуляції.

Тема 3. Безпека роботи з інформацією.

Практичне заняття: «Використання нейромереж для підготовки проєкту»

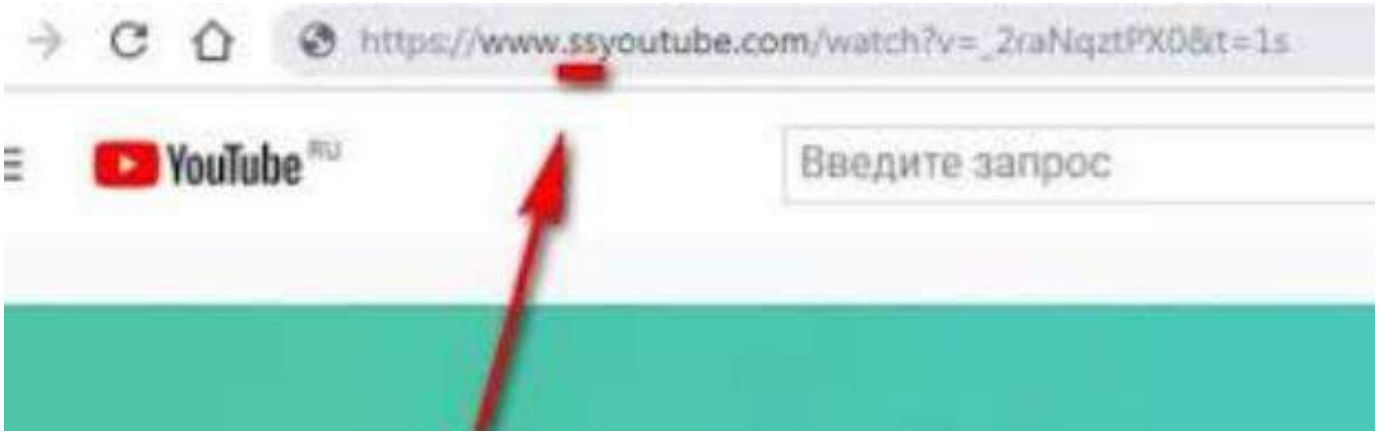
Використовуючи сучасні інноваційні технології підготуйте навчальний проєкт.

Крок 1. Обрання спікерів лекції

Визначте одного із запропонованих спікерів обравши матеріали до проєкту.

Крок 2. Завантаження відеоматеріалів

Обране відео завантажте на власний ПК для подальшого опрацювання, як наведено на прикладі нижче.



Крок 3. Монтаж відеоматеріалів

Змонтуйте та збережіть відео використовуючи сучасні інноваційні технології перейшовши за вказаним посиланням https://online-video-cutter.com

Примітка: відео повинно містити англійські субтитри та не перевищувати загальний хронометраж 15 хвилин спікерського тексту (без вступів/завершень, супроводження звукового ряду тощо).

Крок 4. Переклад відеоматеріалів на державну мову

Використовуючи сучасні інноваційні технології (нейромережу) здійсніть переклад відеоматеріалів на українську мову слідуючи підказкам зазначеного сервісу https://neurodub.ai

Крок 5. Обробка аудіоматеріалів

Здійсніть відокремлення аудіо матеріалів на державній мові у форматі MP3 від відео за допомогою сучасних інноваційних технологій слідуючи підказкам зазначеного сервісу https://mp3cut.net

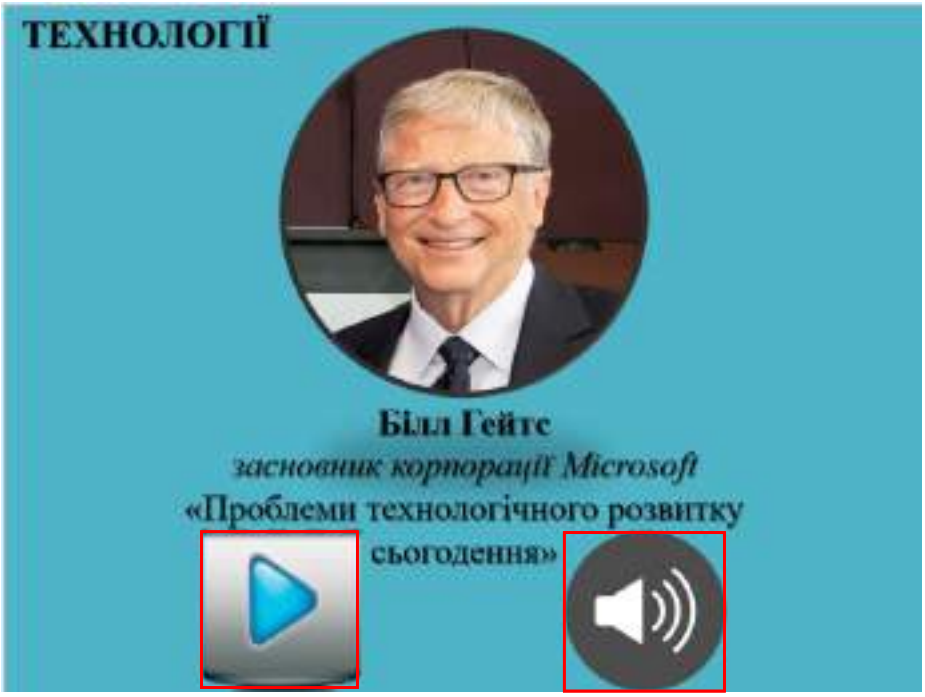
Крок 6. Опрацювання зібраних матеріалів

Прослухайте уважно зібрані матеріали та визначте тему та категорію лекції.

Крок 7. Презентація лекції

Збережіть зібрані матеріали на хмарному сервері Google Drive для переходу за гарячими посиланнями презентація лекції. Презентувати результати роботи.

Примітка: якщо виконана робота зроблена правильно та з виконанням встановлених вимог, то проєкт має виглядати наступним чином:



НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки ННІ № 1

Мультимедійна презентація

Тема: ВИКОРИСТАННЯ ПОЛІЦІЄЮ МОЖЛИВОСТЕЙ ІТС «ІНФОРМАЦІЙНИЙ ПОРТАЛ НПУ» ТА ВЕБ-РЕСУРСУ «РОЗШУК» МВС УКРАЇНИ, ЄРДР У БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ

Тема 4:
Використання поліцією можливостей ІТС «Інформаційний портал НПУ», експертних систем тощо у боротьбі зі злочинністю

Питання:

1. Призначення та структура Інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України»
2. Використання Інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» у боротьбі зі злочинністю
3. Задачі та алгоритми роботи центру прийняття повідомлень «102»

Нормативно-правові акти

Основна література:

1. Конституція (ст. 3, 19, 31, 32, 34)
2. Про Національну поліцію (ст. 25, 26, 27, 28)
3. Про інформацію (ст. 1, 9-21)

Додаткова література:

1. Про Національну програму інформатизації.
2. Про захист персональних даних.
3. Про державну таємницю.
4. Про електронні комунікації.
5. Про доступ до публічної інформації.
6. Про електронні документи та електронний документообіг
7. Про електронні довірчі послуги.
8. Про захист інформації в ІКС.
9. Кодекси: КК, КПК, КУАП тощо.

Відомчі нормативні документи:

1. Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події, затвердженого наказом МВС від 08 лютого 2019 року № 100, зареєстрованого в Міністерстві юстиції України 05 березня 2019 року за № 223/33194;

2. Положення про інформаційно-комунікаційну систему Інформаційний портал Національної поліції України», затвердженого наказом МВС від 03 серпня 2017 року № 676, зареєстрованого в Міністерстві юстиції України 28 серпня 2017 року за № 1059/30927;

3. Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення, затвердженого наказом Генеральної прокуратури України від 30.06.2020 № 298

Питання:

1. Призначення та структура Інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України»

Єдиний облік (далі - ЄО) - прийняття та реєстрація органами (підрозділами) поліції заяв і повідомлень про кримінальні правопорушення та інші події;

Прийняття та реєстрація заяв (повідомлень) - отримання заяв і повідомлень про кримінальні правопорушення та інші події та присвоєння їм порядкового номера уповноваженими службовими особами органів (підрозділів) поліції;

Уповноважена службова особа - працівник чергової служби, у разі відсутності в структурі органу (підрозділу) поліції відповідної чергової служби - інший визначений керівництвом органу (підрозділу) поліції працівник, якого уповноважено на прийняття та реєстрацію заяв і повідомлень про кримінальні правопорушення та інші події.

Джерелом інформації про кримінальні правопорушення та інші події, зокрема, є:

1) заяви (повідомлення) осіб, які надходять до органу (підрозділу) поліції, особи, уповноваженої на здійснення досудового розслідування, або службової особи, уповноваженої на прийняття та реєстрацію заяв (повідомлень);

2) самостійно виявлені слідчим або іншою посадовою особою органу поліції з будь-якого джерела обставини кримінального правопорушення;

3) повідомлення осіб, які затримали підозрювану особу під час учинення або замаху на вчинення кримінального правопорушення чи безпосередньо після вчинення кримінального правопорушення, чи під час безперервного переслідування особи, яка підозрюється в його вчиненні;

4) інше.

Прийняття заяв (повідомлень) незалежно від місця і часу їх учинення, повноти отриманих даних, особи заявника здійснює цілодобово, безперервно та невідкладно орган (підрозділ) поліції, до якого надійшла така інформація.

Заяви (повідомлення) можуть бути усні або письмові:

- усні заяви (повідомлення) від осіб уповноважена службова особа органу (підрозділу) поліції або інший поліцейський, до повноважень якого це належить, вносить до протоколу прийняття заяви про кримінальне правопорушення та іншу подію;
- під час особистого звернення заявника до органу (підрозділу) поліції із письмовою заявою (повідомленням) уповноважена службова особа органу (підрозділу) поліції її (його) приймає і реєструє.

Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» затверджена Наказам МВС від 03.08.2017 № 676.

ІПНП знаходиться за адресом: http://101.11.1.10 Доступ до ІПНП надається авторизованим користувачам, посадовим особам НПУ, які пройшли процедури реєстрації на порталі. Для реєстрації на порталі потрібно заповнити заявку на реєстрацію, зобов’язання та направити з супровідним листом до підрозділів інформаційно-аналітичної підтримки.

ІТС ІПНП – це сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності НПУ та її інформаційно-аналітичного забезпечення. Система ІПНП є складовою частиною єдиної інформаційної системи МВС.

Основними завданнями ІТС ІПНП є:

• інформаційно-аналітичне забезпечення діяльності Національної поліції України;

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

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

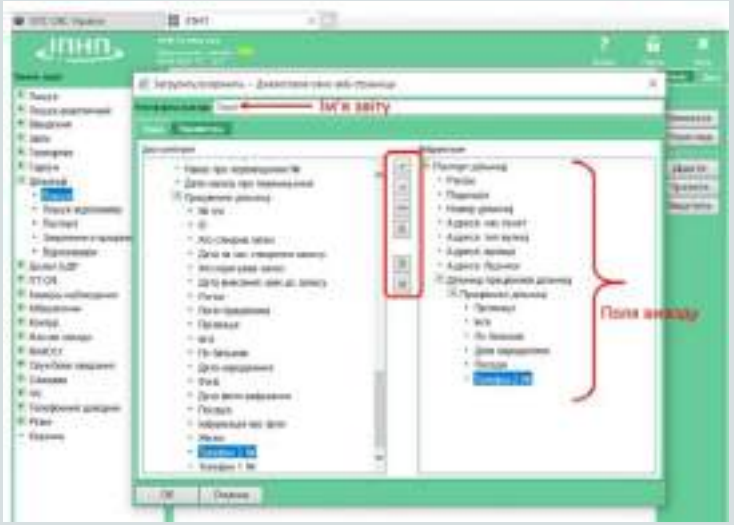
• забезпечення електронної взаємодії з МВС та іншими органами державної влади.

Телекомунікаційна мережа доступу системи ІПНП - сукупність технічних і програмних засобів, призначених для обміну інформацією між складовими системи.

Для захисту інформації, що обробляється органами (підрозділами) поліції в системі ІПНП, використовуються канали Єдиної цифрової відомчої телекомунікаційної мережі МВС, а при використанні відкритих каналів - засоби захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Структура системи ІПНП є:

- центральний програмно-технічний комплекс;
- автоматизовані робочі місця користувачів;
- телекомунікаційна мережа доступу;
- комплексна система захисту інформації.



Центральний програмно-технічний комплекс системи ІПНП – це сукупність технічних і програмних засобів, призначених для обробки інформації, які забезпечують:

- введення, записування, зберігання, видалення, знищення, приймання та передавання інформації та формування баз даних у системі ІПНП;
- формування тимчасових наборів даних для наповнення та підтримки в актуальному стані інформаційних ресурсів баз (бланків) даних ЄІС МВС;
- моніторинг стану інформаційного обміну між складовими системами ІПНП, а також системних журналів аудиту роботи користувачів, технічних і програмних засобів;
- захист інформації під час її обробки.

До складу центрального програмно-технічного комплексу ІПНП входять:

- центральне сховище даних;
- сервери додатків;
- шлюзові сервери;
- автоматизоване робоче місце адміністратора безпеки.

Автоматизовані робочі місця користувачів - 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 ІПНП і призначені для автоматизації службової діяльності, реалізації повноважень обробляти інформацію відповідно до наданого рівня доступу в системі ІПНП.

Комплексна система захисту інформації 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 ІПНП 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.


ЦУНАМІ
ВІДЕОКАМЕРИ
ДТП
ДРАГЕРИ
ТРАФІК
СПОВІЩЕННЯ
ГАРПУН
АТРІУМ
АДМІНПРАКТИКА
HOTLINE
АДМІНПРАКТИКА - ШТРАФИ
ІНТЕГРАЦІЯ ПРОГРАМНОГО КОМПЛЕКСУ «CALLWAY»
ІНФОРМАЦІЙНИЙ ПОРТАЛ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
АСТРА
СТВОРЕНО НАВЧАЛЬНИЙ КЛАС
СКЛАД
ДОЗВІЛ «БДР»
УЗПЛ «HUMAN RIGHTS»
ІТТ «CUSTODY RECORDS»
ІНСПЕКТОР
РЕЄСТР АТП

ІП «Особа»

автоматизований облік відомостей щодо осіб, які вчинили правопорушення, в тому числі тих відносно, яких поліцейські здійснюють профілактичну роботу

Категорії обліку

- яким повідомлено про підозру, досудове розслідування закінчено та направлено з обвинувальними актом до суду (категорія ***«підсудні»)***;
- звільнених з місць позбавлення волі, які відбували покарання за умисний злочин і в яких судимість не знято та не погашено (категорія ***«раніше судимі»)***;
- раніше судимі, яким установлено адміністративний нагляд (категорія ***«адміністративний нагляд»)***;
- раніше судимі, засуджені до позбавлення волі за тяжкі, особливо тяжкі злочини або засуджені два і більше разів до позбавлення волі за умисні злочини (категорія ***«формальний нагляд»)***;
- діти, які перебувають на профілактичному обліку та відносно яких заведено обліково-профілактичні справи (категорія ***«дитина правопорушник»)***;
- особи, які вчиняють домашнє насильство у будь-якій формі (категорія ***«сімейний насильник»)***.

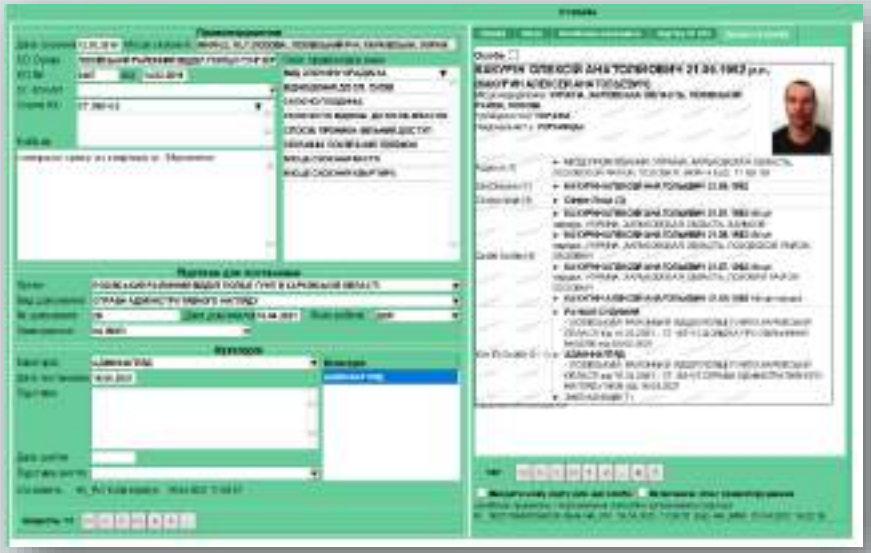
ІП «Особа» категорія «підсудні»

Інформація про обвинувачених, обвинувальний акт щодо яких направлено до суду, вноситься до ІП «Особа» слідчими, які здійснювали досудове розслідування кримінального провадження відносно цих осіб, упродовж доби з часу внесення до ЄРДР відомостей про закінчення досудового розслідування, або працівниками слідчих підрозділів, на яких покладено обов'язки щодо формування зазначеного обліку

Зняття такої інформації з ІП «Особа» здійснюється працівниками підрозділів ІАП НПУ на підставі рішення суду згідно з даними ЄРДР або персонально-довідкового обліку ЄІС МВС із зазначенням підстави та дати.

Інформація про осіб, щодо яких судом ухвалено виправдувальний вирок, невідкладно видаляється з ІП «Особа».

ІП «Особа» категорія «адміністративний нагляд»



Превентивний облік осіб, звільнених з місць позбавлення волі, які відбували покарання за умисний злочин і в яких судимість не знята або не погашена в установленому законом порядку та осіб, які вчинили домашнє насильство у будь-якій формі здійснюється дільничними офіцерами поліції.

Унесення зазначених відомостей до ЄІС МВС покладається на начальника сектору превенції територіального (відокремленого) підрозділу поліції або працівника цього сектору, до обов'язків якого входить організація роботи з особами, які перебувають на превентивному обліку.

Профілактичний облік осіб, що вчинили домашнє насильство, які не досягли вісімнадцятирічного віку, здійснюється працівниками підрозділів ювенальної превенції Національної поліції України.

Питання:

2. Використання Інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» у боротьбі зі злочинністю

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

- тимчасових наборів даних, що створюються в процесі діяльності поліції та використовуються для наповнення та підтримки в актуальному стані баз (бланків) даних, які входять до ЄІС МВС та визначені у статті 26 Закону України «Про Національну поліцію»;
- баз даних у сфері управлінських відносин, необхідних для виконання покладених на поліцію повноважень;
- баз даних, необхідних для забезпечення щоденної діяльності поліції, у сфері трудових відносин, фінансового забезпечення, документообігу.

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

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

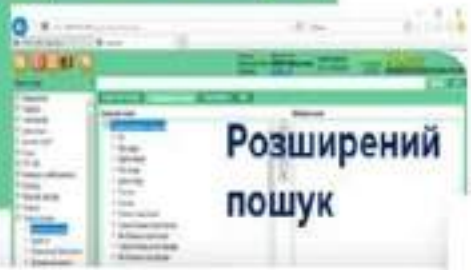
- повідомлень про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, що надійшли технічними каналами зв'язку;
- щодобових переліків та складу нарядів поліції та слідчо-оперативних груп, що заступають на чергування;
- завдань та орієнтувань, що доводились до нарядів поліції для реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події;
- звітування нарядів поліції за результатами реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, виявлення додаткових обставин на місці пригоди;
- пересувань нарядів поліції, які отримані і з планшетних комп'ютерів (мобільних терміналів) та засобів GPS.

ОСНОВНІ ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ІПНП

Введення інформації

Пошук

Короткий пошук



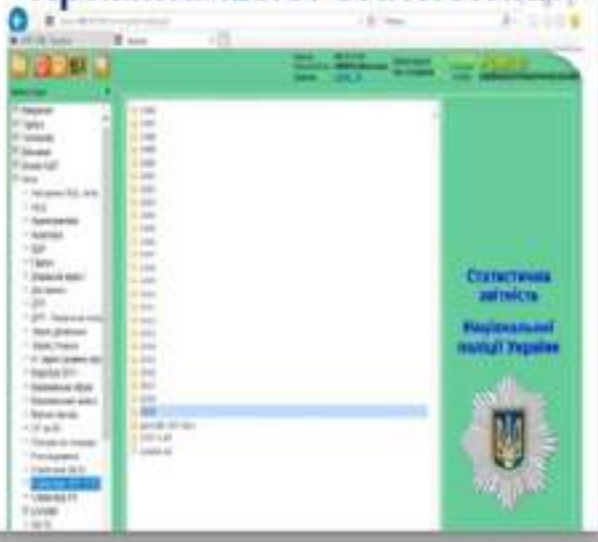
Розширений пошук

Аналітичне досьє

Геопортал

Розрахунок звітів

Архів звітів «Кримінальної статистики»



РОЗРОБЛЕНІ ТА ВПРОВАДЖЕНІ НФОРМАЦІЙНІ ПІДСИСТЕМИ ІНФОРМАЦІЙНОГО ПОРТАЛУ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

ЦУНАМІ

комплекс апаратних та програмних засобів, а також переозлу, призначений для управління силами й засобами органів та підрозділів Національної поліції України

ГАРПУН

облік транспортних засобів, що перебувають в розшуку, на які накладено арешт органами Державної виконавчої служби Міністерства юстиції України та стосовно яких є орієнтування правоохоронних органів щодо можливої причетності до скоєння правопорушень

АДМІНПРАКТИКА

автоматизований облік адміністративних правопорушень призначений для здійснення перевірки особи на наявність (відсутність) даних про повторне вчинення однорідного правопорушення, аналізу застосування адмінзаконодавства та формування звітності, у тому числі у сфері безпеки дорожнього руху. Дозволяє введення інформації на місці вчинення правопорушення поліцейським з планшету

АДМІНПРАКТИКА-ШТРАФИ

облік відомостей щодо обробки платежів по штрафам, а саме обмін даними про виписки з рахунків надходжень державного бюджету щодо адмін штрафів між бюджетною установою «Парус» та Інформаційним порталом НП України

АСТРА

комплекс оброблення інформації, що надходить з камер автоматичної фіксації порушень ПДР. Дозволяє відстежувати виявлені порушення та автоматично формувати постанову про притягнення до адміністративної відповідальності

СКЛАД

облік номерної бланкової продукції: протоколів про адміністративні правопорушення та постанов, тимчасових дозволів на право керування транспортними засобами, бланки протоколів про адмін. затримання

ДОЗВІЛ «БДР»

облік відомостей щодо виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів на рух окремих категорій транспортних засобів. Дозволяє здійснювати автоматичне формування та роздруківку дозвільних документів

ВІДЕОКАМЕРИ

оперативне отримання інформації щодо наявності відеокамер на місці вчинення кримінального правопорушення

ДТП

фіксування та облік основних даних про дорожньо-транспортні пригоди для узагальнення та аналізу стану безпеки дорожнього руху. Також система забезпечує автоматичне формування відповідної довідки для надання до страхових компаній. Створено 19 форм звітності

ДРАГЕРИ

облік використання пристроїв встановлення стану алкогольного сп'яніння підрозділами патрульної поліції НПУ

ТРАФІК

автоматизований облік відомостей щодо осіб, причетних до торгівлі людьми та осіб, причетних до нелегальної міграції із зазначенням характеристики вчинених ними кримінальних правопорушень

СПОВІЩЕННЯ

облік сповіщень про осіб, які засуджені за вчинення злочинів або притягуються до кримінально відповідальності, що надходять з установ Державної пенітенціарної служби України

АТРІУМ

ведення криміналістичного обліку (реєстру судимості), зареєстрованих кримінальних проваджень, осіб які їх вчинили, результатів розгляду в суді, а також осіб звільнених з місць позбавлення волі, у т.ч. по Закону Савченко

ІНТЕГРАЦІЯ ПРОГРАМНОГО КОМПЛЕКСУ «CALLWAY»

інтеграція програмно-апаратного комплексу Callway та підсистеми оброблення викликів за скороченим номером поліції 102 працівниками контактних центрів з служби "102"

УЗПЛ «HUMAN RIGHTS»

облік скарг на порушення прав людини поліцейськими та заходів реагування на них, перевірка за якими здійснюється працівниками Управління захисту прав людини Національної поліції України

ІТТ «CUSTODYRECORDS»

відстеження в режимі реального часу порядку тримання осіб в ІТТ для здійснення реагування на випадки порушення їх прав, протиправних дій працівників поліції стосовно них, а також формування та ведення статистичних даних

HOTLINE

облік звернень жителів України на телефонну «гарячу» лінію Національної поліції України та контролю вжитих заходів реагування

СТВОРЕНО НАВЧАЛЬНИЙ КЛАС

З'явилась можливість проведення навчання операторів служби «102» та диспетчерів, які здійснюють керування нарядами поліції, з метою підвищення рівня їх професійної майстерності та навиків спілкування з громадянами

ІНСПЕКТОР

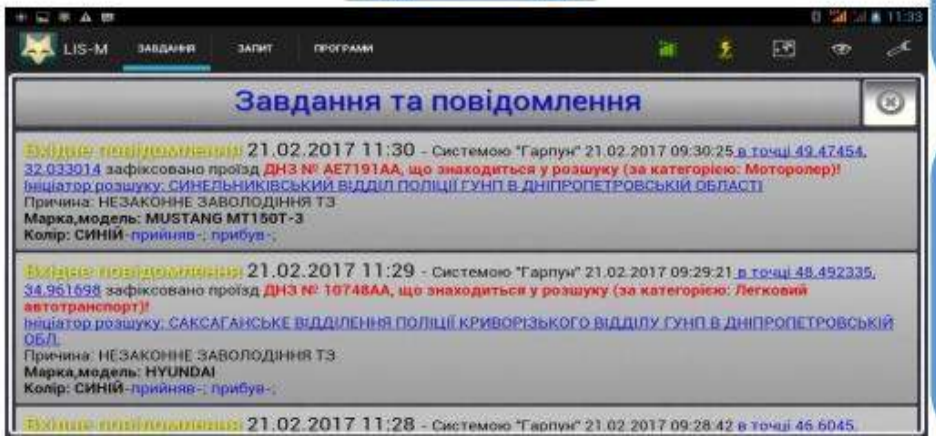
електронний облік виявлених порушень законності, допущених працівниками поліції під час прийняття, реєстрації та розгляду заяв і повідомлень про вчинені кримінальні правопорушення та інші події

РЕЄСТР АТП

реєстр адміністративно – територіального поділу України (область, район, населений пункт, вулиця, будинок) з можливістю виведення на мапу та редагування геоданих (редактор полігонів)

ІП «ГАРПУН»

Метою є накопичення, зберігання, захист, облік, пошук, узагальнення даних про транспортні засоби, які розшукуються з будь-яких підстав у рамках кримінального або виконавчого провадження, стали засобом або предметом учиненого кримінального чи адміністративного правопорушення, та інші відомості про транспорт, які можуть становити службовий інтерес



Орієнтування

- Орієнтування про незаконне заволодіння
- Орієнтування зникнення з місця скоєння ДТП
- Орієнтування про інше правопорушення
- Оперативне орієнтування
- Евакуювання авто

Розшук

- Розшук ТЗ у зв'язку з незаконним заволодінням
- Розшук ТЗ, що зник з місця скоєння ДТП
- Розшук ТЗ іншими правоохоронними органами України
- Розшук майна боржника за даними ДВС

Контроль за незаконним обігом номерних знаків

- Розшук викраденого номерного знаку
- Розшук підробленого номерного знаку
- Втрачений номерний знак
- Знищений номерний знак

ІП «АДМІНПРАКТИКА»

Метою створення ІП «Адмінпрактика» є облік відомостей щодо зареєстрованих адміністративних правопорушень, осіб, які їх учинили та результатів розгляду цих правопорушень

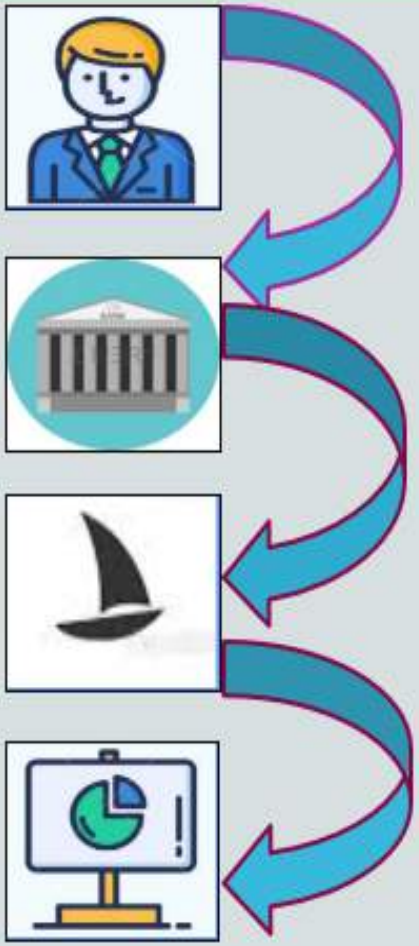
З 01.08.2016 до інформаційної системи внесено **1068369** адміністративних протоколів (постанов), а з 01.01.2017 – **145843**.

Особливостями ІП є:

- автоматизований облік для здійснення перевірки осіб, які вчинили адміністративні правопорушення на наявність (відсутність) вчинення однорідних правопорушень протягом року;
- механізм перевірки належності протоколу/постанови певному працівникові;
- можливість автоматичного заповнення реквізитів щодо транспортних засобів (державний номер, марка, власник АМТ) та даних про водійські посвідчення та їх власників з НАІС МВС ;
- автоматичне заповнення найменувань юридичних осіб при заповнені ідентифікаційних кодів ЄДРПОУ;
- сервіс «Рух протоколу» для відслідкування місця перебування протоколу на кожному етапі прийняття рішення щодо нього;
- складання адмінпротоколів та постанов на мобільних планшетних пристроях працівниками патрульної поліції;
- сервіс друку постанови, протоколу та супровідного листа ДВС України.

ІП «АДМІНПРАКТИКА - ШТРАФИ»

Метою створення ІП «Адмінпрактика - штрафи» є облік відомостей щодо результатів обробки платежів про штрафи, а саме обмін даними про виписки з рахунків надходжень державного бюджету щодо адміністративних штрафів між бюджетною установою «Парус» та Інформаційним порталом Національної поліції України.



Особливості надходження інформації.

- Після надходження до бюджетної установи «Парус» інформації про поповнення рахунків державного бюджету щодо адміністративних штрафів, зазначені відомості стають доступними для вивантаження до ІПНП.
- Завантаження інформації в ІПНП виконується автоматично у пакетному режимі за розкладом та за наявності інформації для обміну.
- До електронної картки в ІП «Адмінпрактика» автоматично вноситься значення стягнутої суми і дата стягнення відповідно до номеру протоколу.

ІП «ДТП»

Метою створення ІП «ДТП» є забезпечення повного обліку дорожньо-транспортних пригод в Україні.

Паперовий вигляд ІК «ДТП» заповнюється в разі відсутності планшетів

Особливості ІП є :

- наповнення електронної картки даними про детальні умови скоєння ДТП;
- GPS-прив'язка ДТП до місця скоєння та одночасного перегляду на мапі країни;
- внесення фото-відеозображень з місць подій щодо кожного ДТП;
- передбачено можливість надання доступу уповноваженим представникам МОЗ та МТСБУ;
- екранна форма мапи з розташуванням місць ДТП

Електронна картка ІП «ДТП» заповнюється безпосередньо на місці дорожньо-транспортної пригоди

Мапа розташування місць ДТП

Паперовий вигляд довідки Ф. 2.0. для надання до страхової компанії

Фотозображення з місця ДТП

Відповідно до доручення керівництва НПУ на ІПНП з **01.08.2016** внесено **80723** відомостей про ДТП.
З **01.01.2017** – **11774**.

ІП «ДРАГЕР»

Мета створення інформаційної підсистеми

Облік спеціальних технічних засобів, якими здійснюється проведення огляду водіїв транспортних засобів на стан алкогольного сп'яніння (Drager)

Облік інформації про осіб, які тестуються із зазначенням результатів тестування

Відомості до інформаційної підсистеми про спеціальні технічні засоби (Drager), якими здійснюється проведення огляду водіїв транспортних засобів на стан алкогольного сп'яніння та осіб, які підлягали тестуванню вносяться працівниками патрульної поліції.

Внесення відомостей до інформаційної підсистеми «ДРАГЕР» здійснюється з автоматизованого робочого місця або через мобільний планшетний пристрій.

Увага! Огляд на стан алкогольного сп'яніння за допомогою спеціальних технічних засобів поліцейським проводиться тільки особам та водіям, які керують транспортними засобами!

ІП «ДОЗВІЛ - БДР»

Метою створення інформаційної підсистеми «Дозвіл-БДР» є автоматизація процесу видачі та обліку дозволів на рух окремих категорій транспортних засобів, у тому числі небезпечних та негабаритних вантажів.

Додатковою можливістю ІП «Дозвіл-БДР» є перевірка оригінальності дозвільного документа за допомогою QR – коду, який розміщено на паперовому вигляді дозволу, за адресою http://www.sai.gov.ua/ - WEB сайту Управління безпеки дорожнього руху Департаменту превентивної діяльності НПУ із застосуванням будь – якого гаджету

Дозвільний документ має QR – код

Відповідно до доручення керівництва Національної поліції України на ІПНП з **01.01.2017** видано **1813** дозволів.

Електронний вигляд паперового дозволу, який роздруковується з ІП «Дозвіл-БДР»

"Затверджую"
Начальник відділу УБДР ДПД Національної поліції України
С.К. Мізін
«25» серпня 2016 р.

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ДЕПАРТАМЕНТ ПРЕВЕНТИВНОЇ ДІЯЛЬНОСТІ
УПРАВЛІННЯ БЕЗПЕКИ ДОРОЖНЬОГО РУХУ

термін дії: з 26.08.2016 по 30.09.2016

ПОГОДЖЕННЯ № 1300-13 НВ
МАРШРУТУ РУХУ ТРАНСПОРТНОГО ЗАСОБУ ПІД ЧАС ДОРОЖНЬОГО ПЕРЕВЕЗЕННЯ НЕБЕЗПЕЧНИХ ВАНТАЖІВ

1. ЗА МАРШРУТОМ: ПП «Ягодин» виїзд на М07 – М07 – об'їзна Ковеля виїзд на М19 - М19 - об'їзна Луцька - М19 - виїзд на М06 - М06 - об'їзна Рівне - М06 - об'їзна Новоград-Волинського - М06 - об'їзна Житомира - М06 - об'їзна Коростишева - М06 - виїзд на Т06-08 - Т06-08 - Мала Рача - Велика Рача - Межирічка. 1) ПП «Ягодин» виїзд на М07 – М07 – об'їзна Ковеля виїзд на М19 - М19 - об'їзна Луцька - М19 - виїзд на М06 - М06 - об'їзна Рівне - М06 - об'їзна Новоград-Волинського - М06 - об'їзна Житомира - М06 - об'їзна Коростишева - М06 - виїзд на Т06-08 - Т06-08 - Мала Рача - Велика Рача - Межирічка. 2) ПП

ІП «ITT-CUSTODY RECORDS»

Метою створення ІП «ITT-custody records» є забезпечення автоматизованого обліку осіб, утримуваних в ізоляторах тимчасового тримання Головних управлінь Національної поліції України

Доступ до адвоката

Комфортні умови утримання

Зустріч з родичами

ПРАВА ЗАТРИМАНОГО

Медична допомога

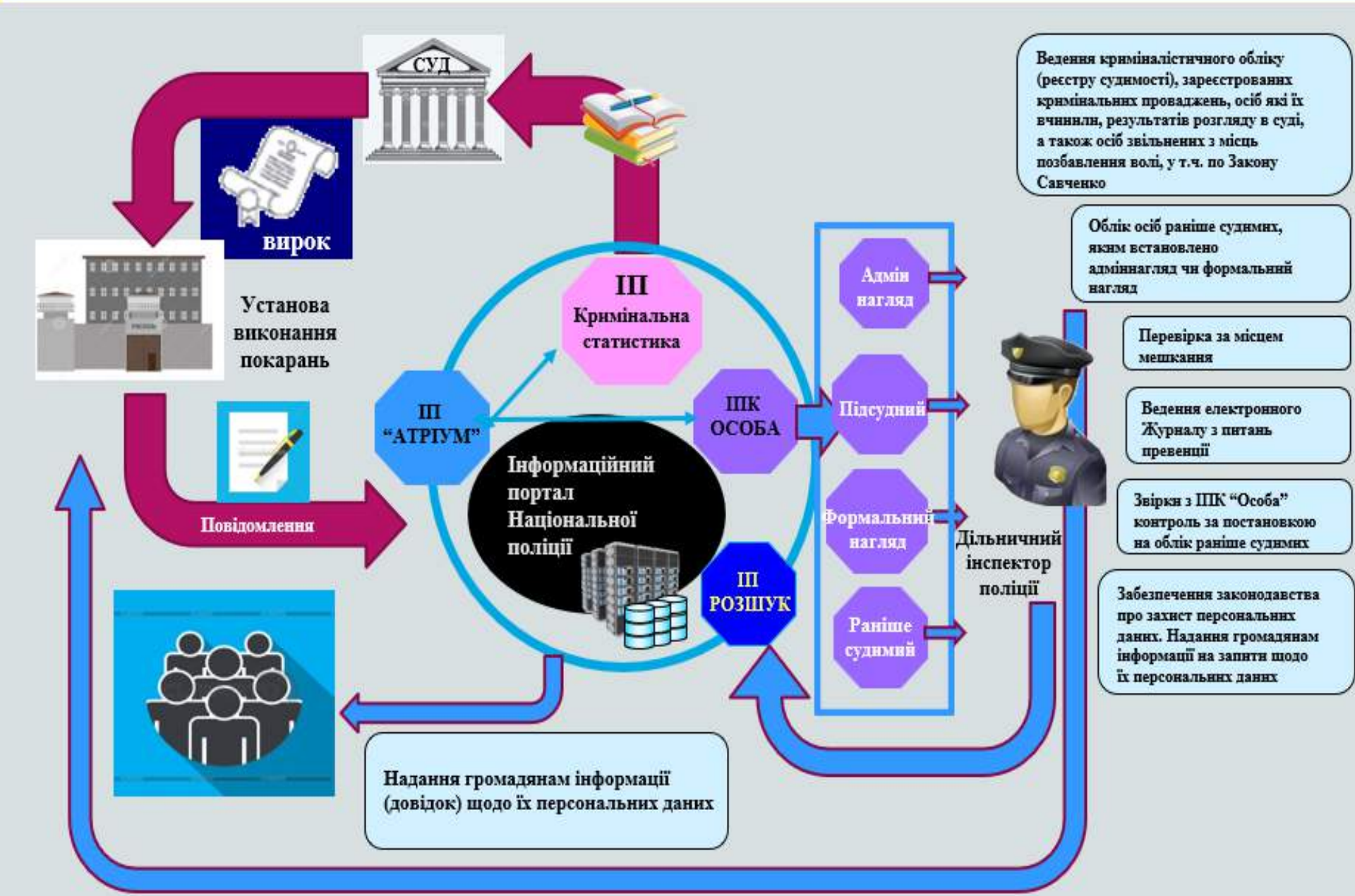
Харчування

Оскарження дій поліції

Метою створення ІП є забезпечення відстеження порядку тримання осіб в ІТТ ГУНП НПУ для здійснення оперативного реагування на випадки порушення їх прав і законних інтересів та протиправних дій працівників поліції стосовно них. Також, використовується для розроблення та формування статистичних звітів.

Відповідно до доручення керівництва НПУ на ІПНП з 25.03.2016 внесено відомості щодо **18987** осіб, з 01.01.2017 – **3001**.

ІП «АТРІУМ»


СУД
вирок
Установа виконання покарань
Повідомлення
ІП "АТРІУМ"
ІП Кримінальна статистика
ІПК ОСОБА
Інформаційний портал Національної поліції
ІП РОЗШУК
Адмін нагляд
Підсудний
Формальний нагляд
Раніше судимий
Дільничний інспектор поліції
Надання громадянам інформації (довідок) щодо їх персональних даних
Ведення криміналістичного обліку (реєстру судимості), зареєстрованих кримінальних проваджень, осіб які їх вчинили, результатів розгляду в суді, а також осіб звільнених з місць позбавлення волі, у т.ч. по Закону Савченко
Облік осіб раніше судимих, яким встановлено адміннагляд чи формальний нагляд
Перевірка за місцем мешкання
Ведення електронного Журналу з питань превенції
Звірки з ІПК "Особа" контроль за постановкою на облік раніше судимих
Забезпечення законодавства про захист персональних даних. Надання громадянам інформації на запити щодо їх персональних даних

Питання:

3. Задачі та алгоритми роботи центру прийняття повідомлень «102»

Система централізованого управління нарядами поліції (система “ЦУНАМІ”)

– комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами органів та підрозділів Національної поліції України.

Мета впровадження системи «ЦУНАМІ» – вдосконалення процесу організації діяльності з управління силами й засобами НПУ для ефективного реагування на заяви та повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події.

Завдання впровадження системи “ЦУНАМІ”:

– оптимізація роботи нарядів поліції, задіяних для забезпечення публічної безпеки в системі єдиної дислокації, слідчо-оперативних груп чергових частин;

– скорочення часу реагування на повідомлення громадян про злочини та події, попередження правопорушень й затримання злочинців по «гарячих слідах»;

– здійснення оперативного контролю за своєчасністю і якістю реагування нарядами поліції на правопорушення та інші події, дотримання законності під час виконання службових обов'язків працівниками поліції.

Основні компоненти системи “ЦУНАМІ”

Організаційно-управлінський рівень

1) Центр прийняття повідомлень – служба «102»
1.1. Служба «102»
1.2. Чергова служба (чергові частини Головних управлінь, апарату Національної поліції)
2) Диспетчерський центр управління
3) Інформаційно-технічний супровід системи.
3.1. Геоінформаційна система (електронна карта міста).
3.2. Система супутникового GPS-позиціювання та мобільного комунікаційного обладнання.
3.3. Система відеоспостереження.
3.4. Система колективного відображення.

Виконавчий рівень

1) Наряди управління патрульної поліції.
2) Групи реагування патрульної поліції (далі - ГРПП).
3) Слідчо-оперативні групи.
4) Наряди управління поліції охорони.
5) Чергові частини управлінь, відділів поліції (а також УПО, УПП).
6) Додаткові сили (дільничні офіцери поліції, працівники управління захисту економіки, кіберполіції, вибухотехнічної служби, кінологічного центру, спеціалісти НДЕКЦ тощо).

Чергова служба відповідні підрозділи та окремі посадови особи органів і підрозділів Національної поліції, які в безперервному режимі забезпечують координацію підрозділів поліції при оперативному реагуванні на заяви і повідомлення громадян про правопорушення та події.

До чергової служби відносяться:

- чергові частини;
- чергові ситуаційних відділів;
- чергові секторів реагування патрульної поліції;
- чергові відділів чергової служби управлінь патрульної поліції.

Центр прийняття повідомлень

Служба «102» – відділи «102» УІПКП «102» Головних управлінь Національної поліції в областях та м. Києві, працівники яких у цілодобовому режимі здійснюють прийняття, реєстрацію та організацію реагування на повідомлення про правопорушення та інші події за допомогою АРМ «оператор «102» та АРМ «диспетчер» ІТС «Цунамі».

Оператор служби «102» – посадова особа відділу «102» УІПКП «102» Головних управлінь Національної поліції в областях та м. Києві, 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 ІТС «Цунамі».

Центр прийняття повідомлень

Диспетчер – старший інспектор, інспектор-черговий відділу «102» управлінь інформаційної підтримки та координації поліції «102» Головних управлінь Національної поліції в АР Крим та м. Севастополі, областях та м. Києві, уповноважений на здійснення керування нарядами поліції за допомогою АРМ «диспетчер» в ІТС «Цунамі» з метою оперативного реагування на заяви та повідомлення про правопорушення та інші події.

Функції диспетчерів:

- ✓ управління нарядами поліції, у тому числі підрозділів патрульної служби, поліції охорони, які працюють у районі його обслуговування;
- ✓ отримання інформації з служби «102» та відстеження на електронній карті місць учинення правопорушень;
- ✓ передача даних про правопорушення на планшет конкретного патруля поліції;
- ✓ забезпечення відповідного патруля всією наявною інформацією, що знаходиться у відомчих інформаційних масивах, про заявника та адресу виїзду;
- ✓ координація роботи найближчих вільних нарядів поліції, які залучаються до розкриття злочину по «гарячих слідах», виїзду до заявника, на місце пригоди або в напрямку вірогідного переховування злочинця;
- ✓ контроль часу виїзду наряду та відстеження результатів реагування на заяви та повідомлення громадян про правопорушення, прийняті рішення тощо.

Автоматизація служби “102” дозволила оператору одержувати інформацію про абонента ще до моменту підняття слухавки:

- дані про власника телефонного номера;
- кількість дзвінків, які раніше надходили із цього номера та щодо яких подій;
- відстеження повторних викликів по вже зареєстрованій події;
- географічне місце (адресу) на електронній карті міста Києва тієї події, про яку повідомлено;
- попередження про дзвінки абонентів, які внесено до окремого списку: психічно хворі, телефонні хулігани та інше.

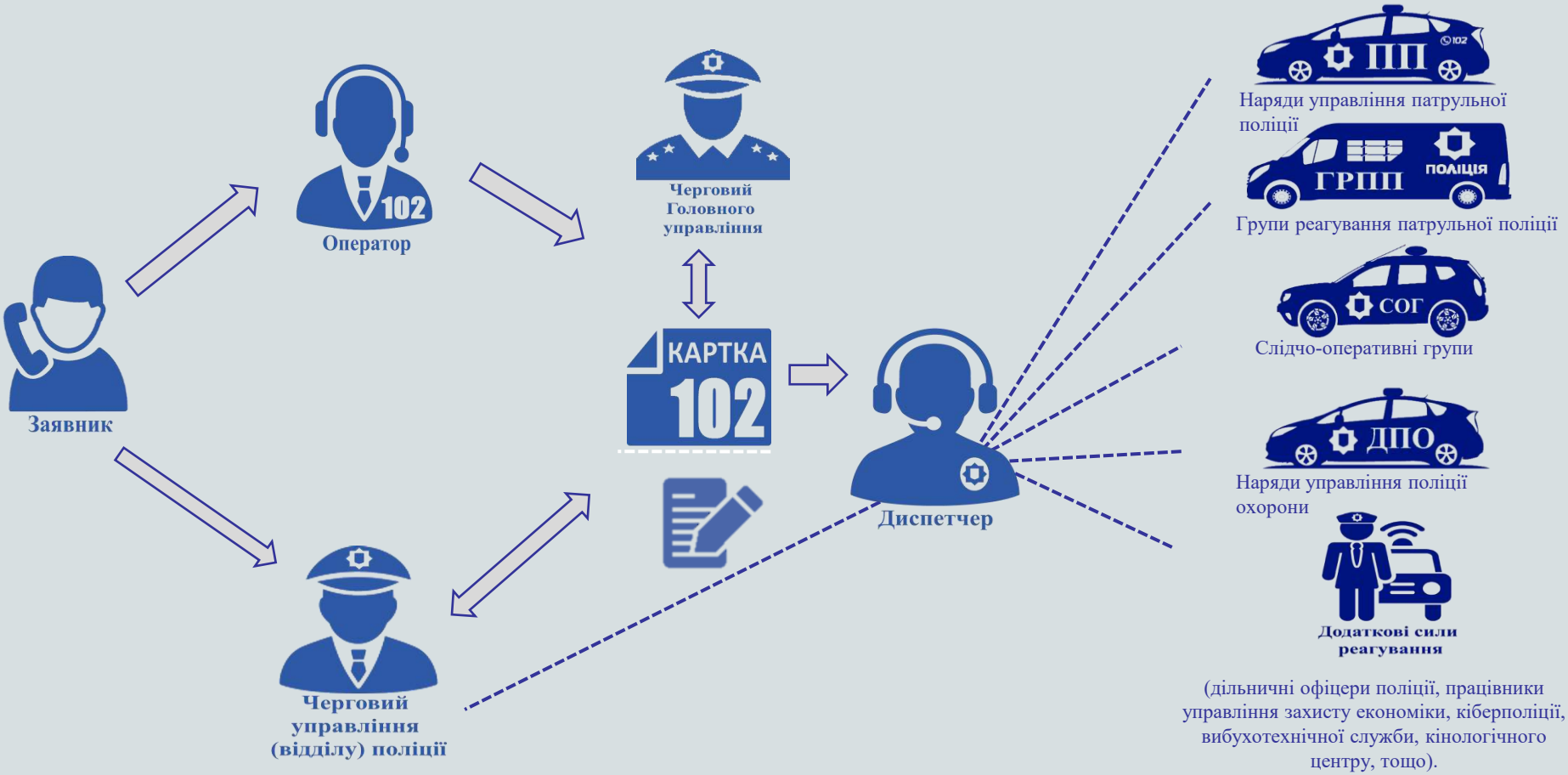
Оператор здійснює первинну кваліфікацію події

Заповнена оператором електронна картка відразу надходить до диспетчера відповідального за керування нарядами поліції в тому чи іншому районі, області (столиці).

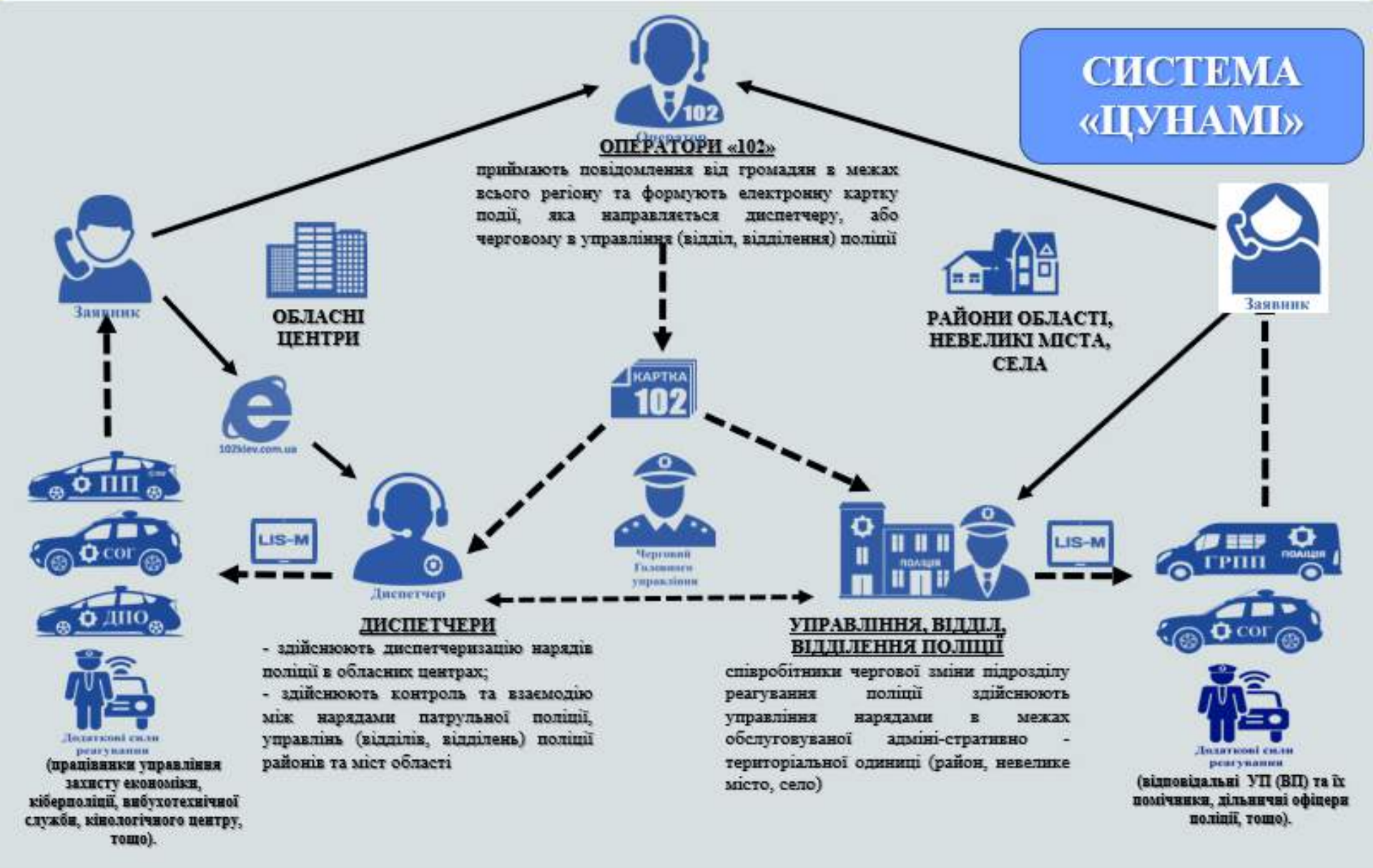
Програмне забезпечення відображає інформацію про місце вчинення злочину на електронній карті міста Києва.

Інформація з електронної картки «102» одночасно відображається у оперативного чергового ГУНП.

Схема реагування на заяви та повідомлення громадян



ЗАПРОВАДЖЕННЯ В ГУНП АВТОМАТИЗОВАНОЇ СИСТЕМИ ЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ НАРЯДАМИ ПОЛІЦІЇ «ЦУНАМІ»



ДИСПЕТЧЕРИ

- здійснюють диспетчеризацію нарядів поліції в обласних центрах;
- здійснюють контроль та взаємодію між нарядами патрульної поліції, управлінь (відділів, відділень) поліції районів та міст області

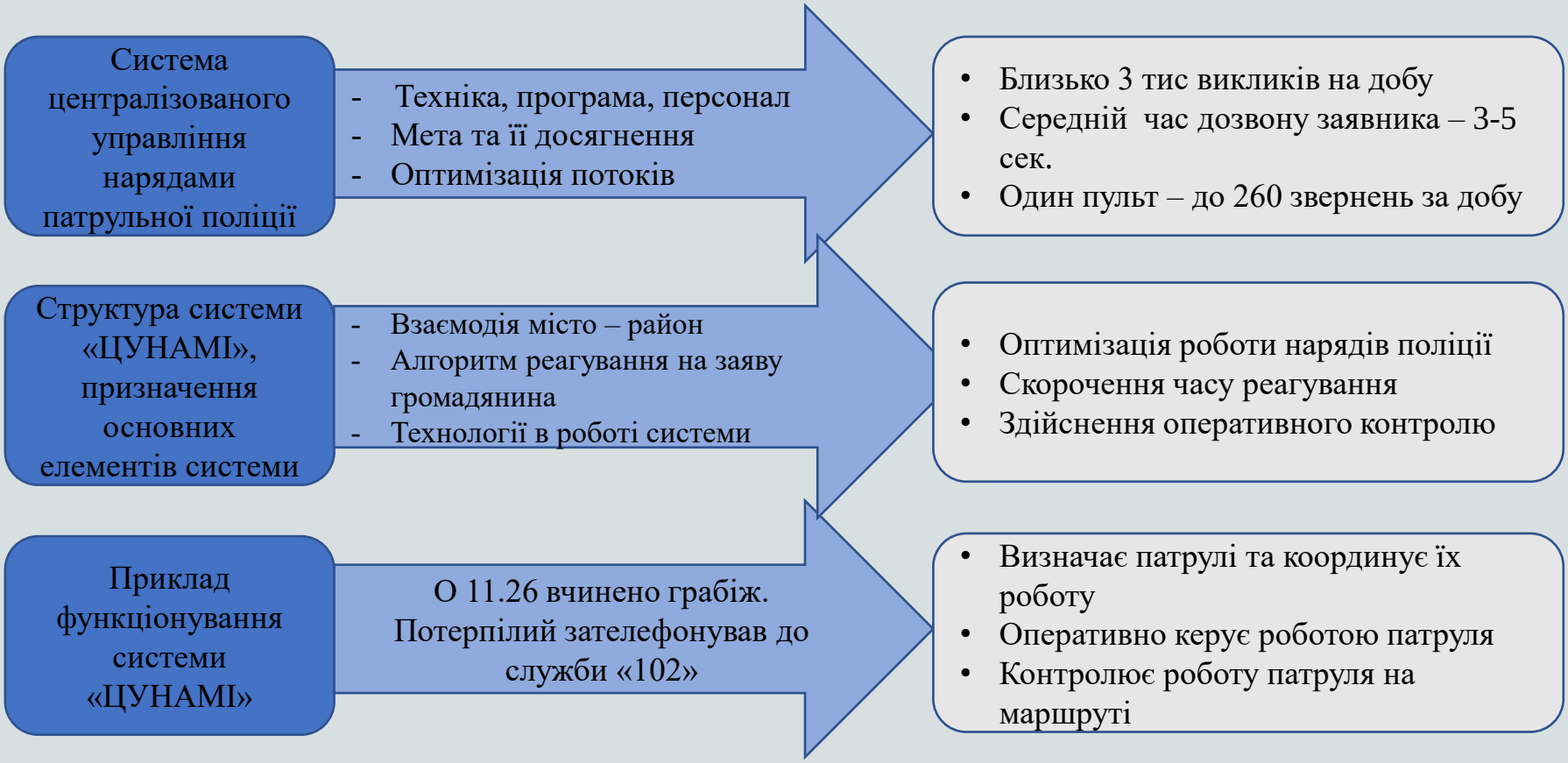
УПРАВЛІННЯ, ВІДДІЛ, ВІДДІЛЕННЯ ПОЛІЦІЇ

співробітники чергової зміни підрозділу реагування поліції здійснюють управління нарядами в межах обслуговуваної адміні-стративно - територіальної одиниці (район, невелике місто, село)

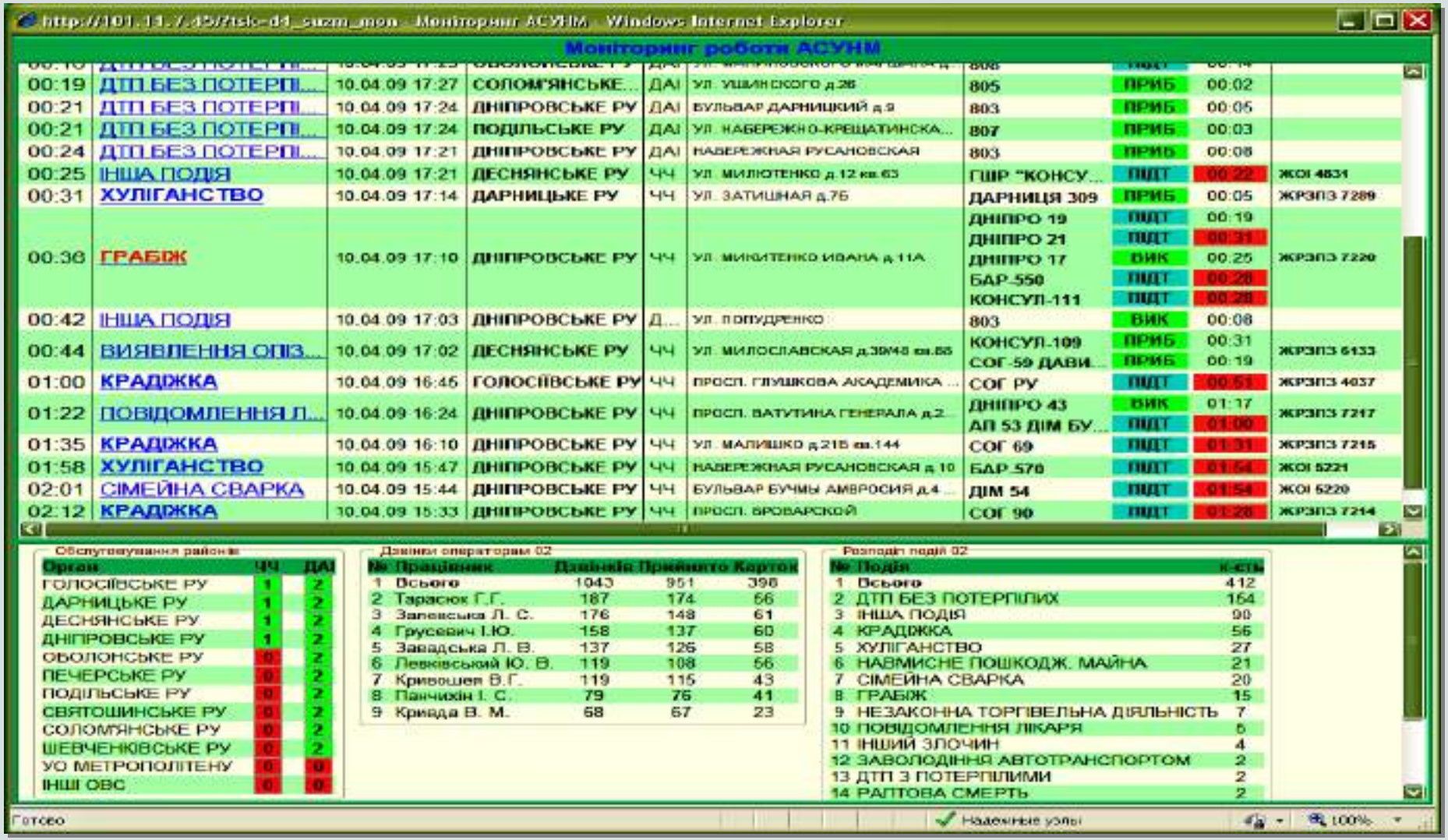
(працівники управління захисту економіки, кіберполіції, вибухотехнічної служби, кінологічного центру, тощо).

(відповідальні УП (ВП) та їх помічники, дільничні офіцери поліції, тощо).

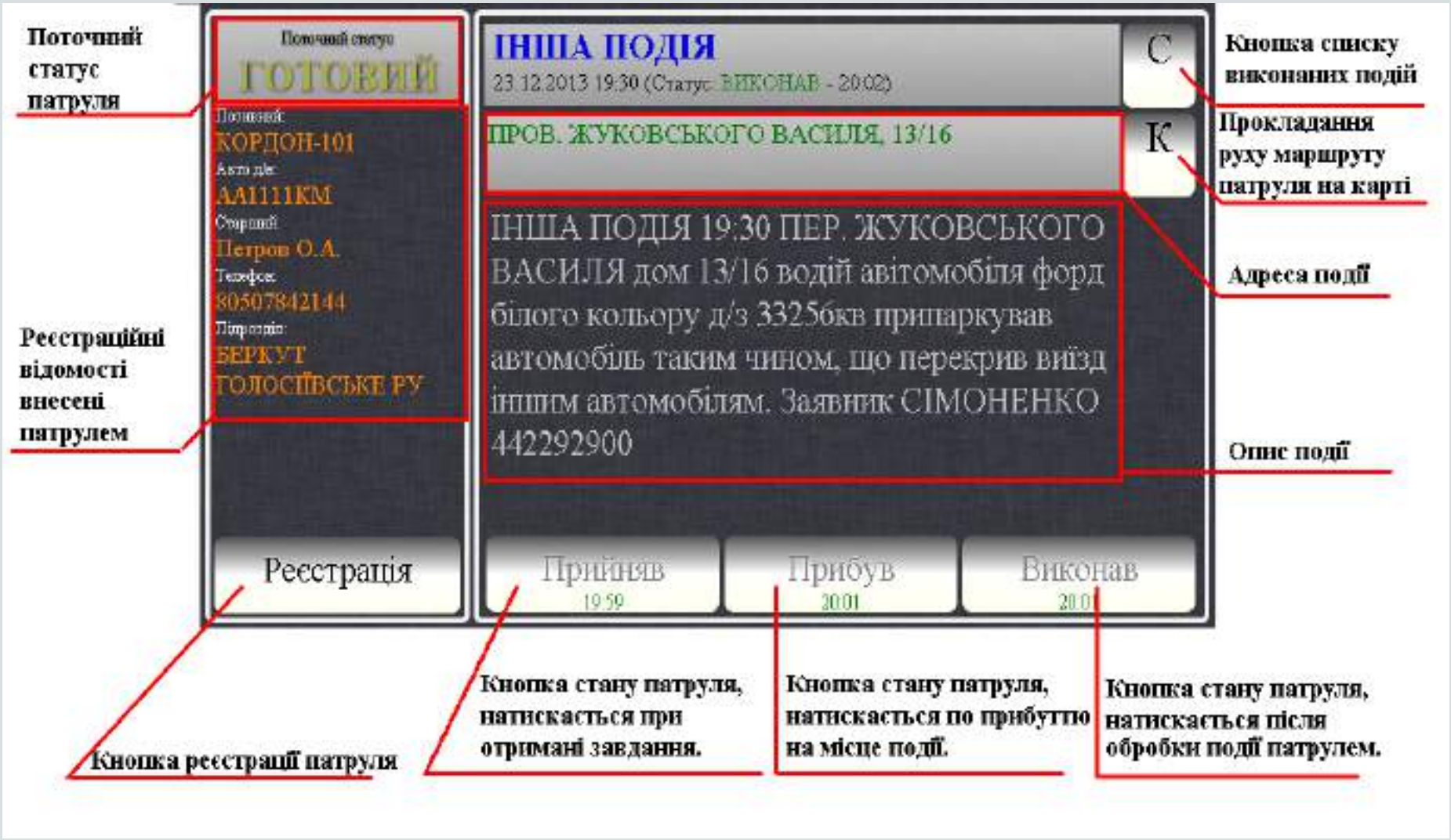
Система централізованого управління нарядами патрульної поліції «ЦУНАМІ»



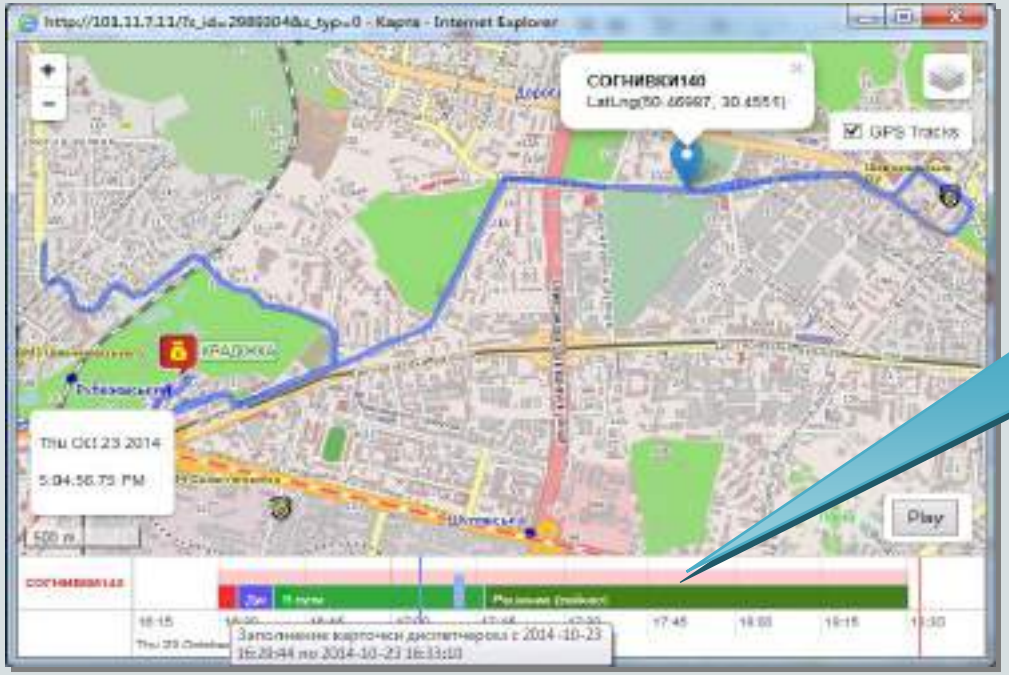
Моніторинг роботи патрулів



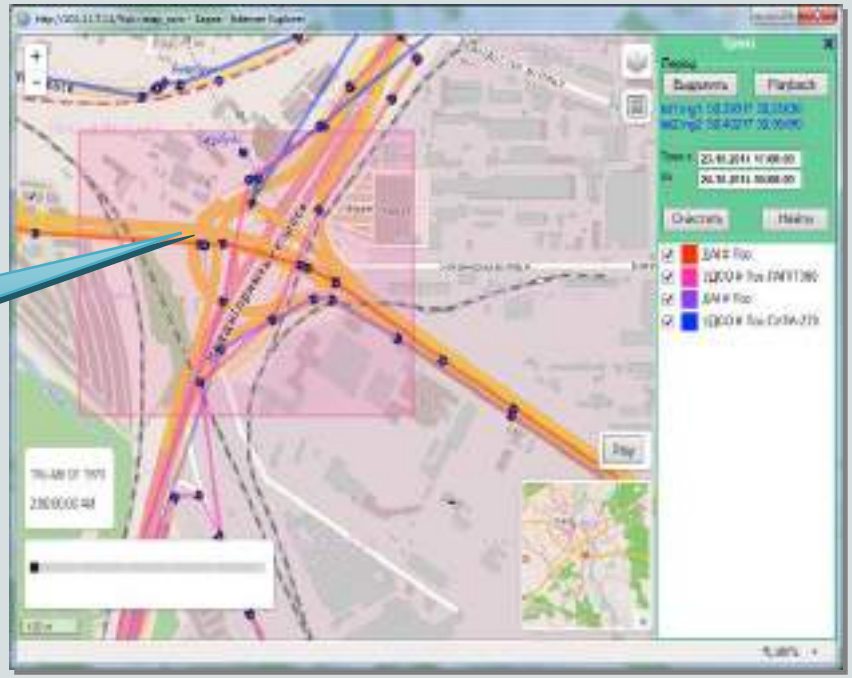
Планшетний комп'ютер в автомобілях нарядів поліції



Можливості системи “ЦУНАМІ”

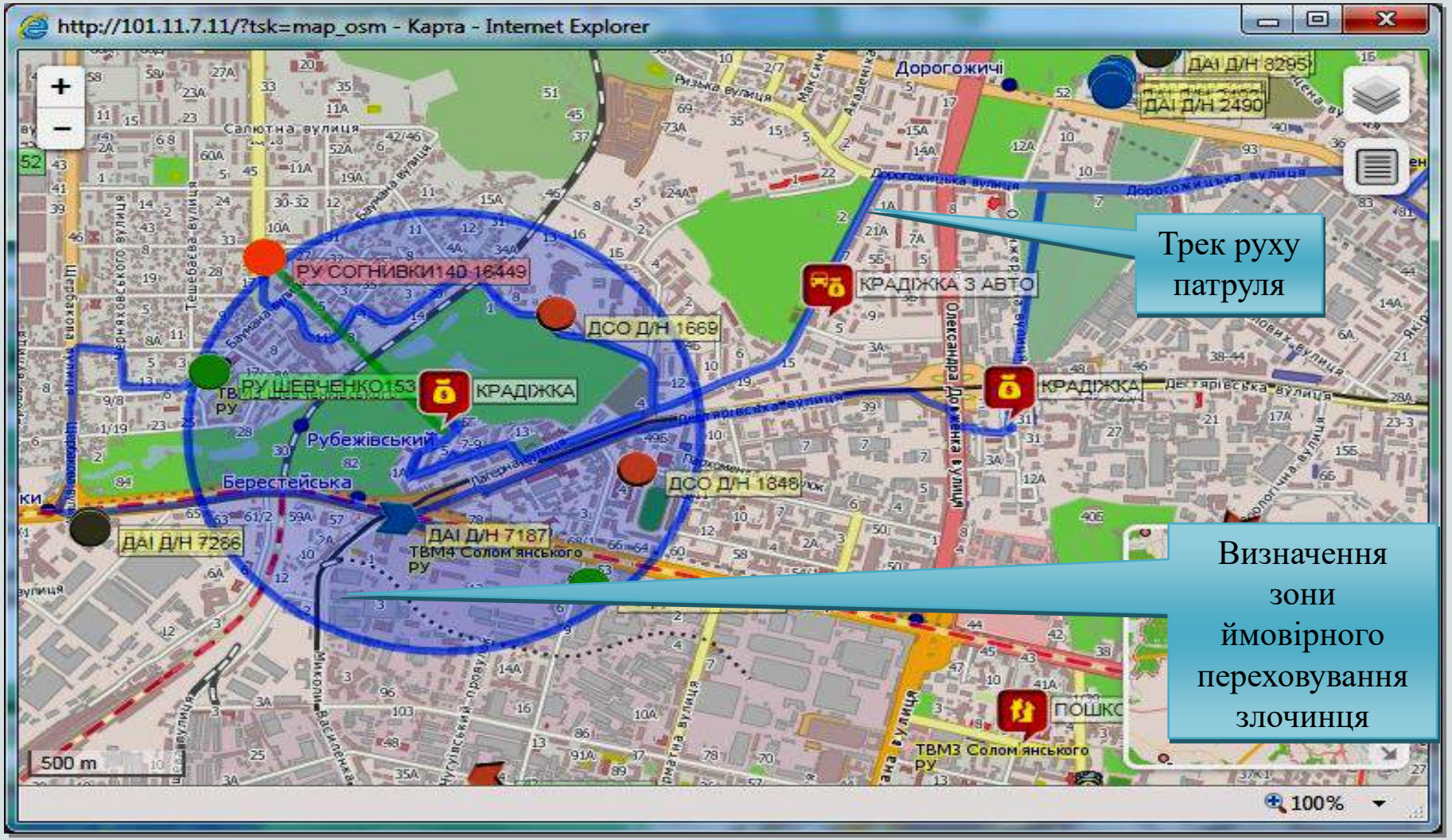


Інтерактивна хронологічна шкала відтворення етапів реагування на подію



Контроль проїзду вибраної території у визначений час

Можливості системи “ЦУНАМІ”



Можливості системи “ЦУНАМІ”

Інтерактивне визначення скупчення місць правопорушень

Автоматизоване визначення патруля для призначення, з урахуванням спеціалізації наряду

ВИСНОВКИ

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.

Розпорядником системи ІПНП є Національна поліція України.

Адміністратором системи ІПНП є уповноважений структурний підрозділ апарату центрального органу управління Національної поліції України.

Користувачами системи ІПНП є посадові особи органів (підрозділів) поліції, яким в установленому порядку надано право доступу до інформації в цій системі.

Online-тестування

Тема 3. «Використання поліцією можливостей ІТС «Інформаційний портал НПУ» та веб-ресурсу «Розшук» МВС України, ЄРДР у боротьбі зі злочинністю

Крок 1. Ознайомтесь з навчальними матеріалами проведення навчально-ділової гри «Лінія 102» та рекомендаціями щодо виконання завдання (наведені нижче).

Крок 2. По результатам вивчених матеріалів перейдіть за наступним посиланням http://102.dduvs.in.ua та ознайомитись з емулятором навчально-ділової гри «Лінія 102», а також з окремою роботою оператора служби «102», диспетчера, патруля, чергового щодо відпрацювання інформації про подію.

- ОПЕРАТОР (*логін: 002_к; пароль: 200_к*);
- ДИСПЕТЧЕР (*логін: dis_к; пароль: sid_к*);
- ПАТРУЛЬ (*логін: patrol_к; пароль: lortap_к*);
- ЧЕРГОВИЙ (*логін: rovd; пароль: 111*).

Примітка: *під час проведення навчально-ділової гри «Лінія 102» не надавати стороннім особам логіни та паролі доступу до акаунтів. Введена інформація зберігається на сервері і може бути переглянута адміністратором, тому необхідно ставитися з великою відповідальністю до виконання завдання.*

ПЕРЕЛІК ПОДІЙ

Подія №1

До лінії 102 звернувся гр. Колинько В.А. та повідомив наступне, що мешканці м. Києва, а саме гр. Солопіга Степан Степанович 12.05.1985 р.н. та гр. Кобиняка Клим Карпович 20.02.1979 р.н. приблизно об 23 год. 10 хв. 19 листопада 2022 року, перебуваючи в стані алкогольного сп'яніння, здійснили розбійний напад на гр. Федорину Олега Олександровича 08.02.1988 р.н. Під час бійки гр. Солопіга С.С. завдав гр. Федорині О.О. удару фінським ножем під ліву лопатку, внаслідок чого останній помер на місці вчинення злочину. Відомо, що гр. Солопіга С.С. та гр. Кобиняка К.К. заволоділи шапкою та гаманцем потерпілого.

Подія №2

До лінії 102 звернувся гр. Здоренко З.А. та повідомив наступне, що увечері 30 жовтня 2022 року гр. Здоренко О.І. і Воляк В.В., будучи в нетверезому стані, в підземному переході залізничної станції Київ-Пасажирський м. Києва, з хуліганських мотивів розбили п'ять електричних світильників. При виході з підземного переходу гр. Воляк В.В. зірвав з поручнів пластмасове покриття.

Подія №3

До лінії 102 звернулась гр. Старокваша С.С. та повідомила наступне, що гр. Вереска В.В. будучи в нетверезому стані, в ніч на 05 грудня 2022 року намагався здійснити угон автомобіля. Проходячи по вул. Жилянській, б. 25, в м. Києві побачивши автомобіль «Феррарі», який належав заявниці, гр. Вереска В.В. розбив скло, заліз у машину й намагався її завести. Останній свій злочинний намір не довів до кінця, бо в цей час до автівки підійшла охорона приватної фірми «Січ», які й затримали гр. Вереска В.В. на місці скоєння злочину.

Подія №4

До лінії 102 звернулась гр. Захарченко В.І. та повідомила наступне, що гр. Верба Л.Т. 31 грудня 2022 року приблизно об 11 год. з метою крадіжки індивідуального майна проник у квартиру гр. Захарченка В.І., що знаходиться за адресою м. Києві, вул. Блакитна, б. 21, кв. 8. Останній викрав майна на загальну суму 115 тис. грн., де і був затриманий мешканцями під'їзду по вищевказаній адресі.

Подія №5

До лінії 102 звернулась гр. Кабан К.К. та повідомила наступне, що 19 січня 2023 року об 12 год. 15 хв. поблизу буд. 16 по вул. Соборній в м. Київ гр. Рясний Роман Іванович в належному йому автомобілі «Шкода Октавія», д.н. ВС 0001 ВА перевозив у пластиковій тарі речовину рожевого кольору, яка згідно висновку експерта за явними ознаками схожа з наркотичним засіб «метадон».

Рекомендації щодо виконання завдання

1. Перейдіть на сайт за наступним посиланням: http://102.dduvs.in.ua
2. Відкрити піктограму НАВС та ввести логін та пароль *оператора*.
3. Натиснути кнопку «Далі».
4. Заповнити всі реквізити картки.
5. Натиснути кнопку «Зберегти».
6. Натиснути кнопку «Авторизація».
7. Ввести логін та пароль *диспетчера*.
8. Натиснути кнопку «Далі».
9. Подія повинна набути статусу «Нове».
10. Натиснути на Вашу подію. Відкриється інформація, яка була введена оператором.
11. Натиснути кнопку «Авторизація».
12. Ввести логін та пароль *патруля*.
13. Натиснути кнопку «Далі».
14. Натиснути на Вашу подію. Відкриється інформація, яка була введена оператором.
15. Натиснути кнопку «Прийняти».
16. Натиснути кнопку «Авторизація».
17. Ввести логін та пароль *диспетчера*. Натиснути кнопку «Далі».
18. Подія повинна набути статусу «В обробці».
19. Натиснути кнопку «Авторизація».
20. Ввести логін та пароль *патруля*. Натиснути кнопку «Далі».
21. Натиснути на Вашу подію.
22. Натиснути кнопку «Прибув».
23. Натиснути кнопку «Авторизація».
24. Ввести логін та пароль *диспетчера*. Натиснути кнопку «Далі».
25. Подія повинна набути статусу «Прибув».
26. Натиснути кнопку «Авторизація».
27. Ввести логін та пароль *патруля*. Натиснути кнопку «Далі».
28. Натиснути на Вашу подію.
29. Надрукувати звіт про виконану патрулем роботу.
30. Натиснути кнопку «Зберегти звіт».
31. Натиснути кнопку «Авторизація».
32. Ввести логін та пароль *диспетчера*. Натиснути кнопку «Далі».
33. Подія повинна набути статусу «Виконано».
34. Натиснути на Вашу подію.
35. Необхідно побачити повну інформацію про подію.
36. Натиснути на рядок «Розшукові обліки МВС + Патруль».
37. Перевірити по обліках осіб та/або транспортні засоби з Вашої події.
38. Натиснути кнопку «Авторизація».
39. Ввести логін та пароль *чергового*.
40. Натиснути кнопку «Далі».
41. Натиснути на рядок «Розшукові обліки МВС + Патруль».
42. Натиснути кнопку «Розшук».
43. Закрити екран «Розшук».
44. Закрити екран «Патруль».
45. Повідомити викладача про виконане завдання.

Тема 3. «Використання поліцією можливостей ІТС «Інформаційний портал НПУ» та веб-ресурсу «Розшук» МВС України, ЄРДР у боротьбі зі злочинністю»

Пам'ятайте

Під час виконання практичних завдань пам'ятай про правила безпеки життєдіяльності при роботі з комп'ютером!

Крок 1. У рамках курсу навчальної дисципліни пройдіть online-тестування з удосконалення уміння правильного та швидкого набирання тесту (Typing test) за вказаним посиланням або скануйте QR-code:
https://monkeytype.com

Крок 2. У відкритому вікні налаштуйте наступні параметри: мова – українська; час виконання вправи – 60 с.

Крок 3. Створити новий документ Word виконавши команду *Файл-Створити-Новий документ* або необхідно виконати команду *Ctrl + N*.

Примітка: *Зазначені службові документи додаються на окремому аркуші (зразок). Усі зазначені у зразку документи оформлювати згідно з вимогами наказу МВС України від 29.07.2019 №630.*

Крок 4. Замість особистого підпису у службовому документі необхідно вставити QR-код, який містить інформацію про прізвище та ім'я, контактний телефон, E-mail, номер навчальної групи, посаду підписанта.

Примітка: *QR-код можна створити за допомогою Generator QR Code або скористатися будь-якою доступною програмою у мережі Інтернеті.*

Крок 5. Встановити пароль на документ, виконавши команду *Файл- Відомості-Захист документа-Зашифрувати та встановити пароль.*

Крок 6. Зберегти документ як «Ваше Прізвище – П.з. 6.1» у папці «Тема 6», виконавши команду *Файл-Зберегти як*.

Т.в.о. завідувача кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС капітану поліції
Кирилу ЯРОВОМУ

ДОПОВІДНА ЗАПИСКА

Щодо результатів виконання вправи зі швидкісного набору тексту

З метою виконання практичного завдання навчальної дисципліни «Інформаційне забезпечення професійної діяльності» мною виконана вправа зі швидкісного набору тексту з використанням програми «Monkeytype», що за посиланням (https://monkeytype.com) та отримані такі результати, а саме:

1) кількість набраних слів – ____;
2) витрачений час – ____;
3) кількість набраних символів за хвилину – ____;
4) кількість помилок – ____ .

Висновок: мої навички швидкісного набору тексту протягом року (покращились/погіршились/не змінились).

Додаток: скріншот результатів виконання вправи на 1 арк. в 1 прим.

Слідчий слідчого відділу
Васильківського РУП
ГУНП в Київській області
лейтенант поліції
____._____.2024

Ірина КРАВЧУК

Додаток

(Скріншот результатів виконання вправи)

ПІДСУМКОВЕ ТЕСТУВАННЯ

АВТОРСЬКІ МАТЕРІАЛИ

Кібергігієна. Основи захисту персональних даних

Основи кібербезпеки. Система захисту інформації

Стратегії протидії дезінформації у мережі Інтернет

Основи програмування. Сучасні мови програмування

Основні техніки збору інформації за допомогою OSINT-інструментів

Можливості сучасних інноваційних технологій (криптовалюта, Метавсесвіт)

Основні поняття апаратно-програмного забезпечення інформаційних технологій

Інтерактивний квест «Детективне розслідування»