МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
Сумська філія
Кафедра соціально-економічних дисциплін

ТЕКСТ ЛЕКЦІЇ

з навчальної дисципліни «Інформаційні та комунікаційні технології»
обов'язкових компонент
освітньої програми першого (бакалаврського) рівня вищої освіти
262 Правоохоронна діяльність (поліцейські)

за темою – «Єдина інформаційна система МВС України. Автоматизоване робоче місце працівника підрозділу "102" (АРМ "оператор "102") системи ІПНП. Автоматизоване робоче місце (АРМ) "диспетчер" системи ІПНП. Робота з базами даних, використання радіозв'язку та відео фіксації у роботі патрульного поліцейського»

Суми 2024

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 14.08.2024 № 8

СХВАЛЕНО
Вченою радою Сумської філії
Харківського національного
університету внутрішніх справ
Протокол від 08.07.2024 № 8

ПОГОДЖЕНО
Секцією Науково-методичної
ради ХНУВС з гуманітарних та
соціально-економічних дисциплін
Протокол від 13.08.2024 №7

Розглянуто на засіданні кафедри соціально-економічних дисциплін
Протокол від 25.06.2024 № 23

Розробник:
Доцент кафедри соціально-економічних дисциплін Сумської філії ХНУВС, кандидат економічних наук, доцент Виганяйло С.М.

Рецензенти:
1. Доцент кафедри протидії кіберзлочинності, факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ, канд.пед.наук, доцент Тетяна Петрівна Колісник
2. Доцент кафедри кібернетики та інформатики СНАУ, канд.екон.наук, доцент Олександр Борисович В'юненко

План лекції

1. Єдина інформаційна система МВС України.
2. Поняття системи централізованого управління нарядами поліції.
3. Автоматизоване робоче місце працівника підрозділу "102" (АРМ "оператор "102") системи ІПНП. Автоматизоване робоче місце (АРМ) "диспетчер" системи ІПНП.
4. Організація інформаційно-аналітичного забезпечення Національної поліції України.
5. Правила ведення радіоефіру під час патрулювання. Відеофіксація з допомогою персонального відеореєстратора під час патрулювання

Рекомендована література

Основна

1. Виганяйло С. М. Інформаційне забезпечення професійної діяльності: навч. посіб. Харків: ХНУВС, 2021. 110 с.
2. Клімушин, П. С. Інформаційні системи та технології в економіці : навчальний посібник / П. С. Клімушин, О. В. Орлов, А. О. Серенок; Нац. акад. держ. управління при Президентові України, Харк. регіон. ін-т держ. управління. - Харків : Вид-во ХарРІ НАДУ "Магістр", 2011. - 448 **c**http://dspace.univd.edu.ua/xmlui/handle/123456789/4730
3. Сезонова, І. К. Інформатика для правоохоронців: навч. посіб. / І. К. Сезонова; МВС України, Харк. нац. ун-т внутр. справ. - Харків, 2015. – 182 с. http://dspace.univd.edu.ua/xmlui/handle/123456789/1311
4. Інформаційні системи та технології: підруч. / кол. авт. ; за заг. ред. д.т.н., проф. В.Б. Вишні. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. 280с. URI: https://er.dduvs.in.ua/handle/123456789/7110
5. нформаційні технології: підруч. / В.Б. Вишня, К.Ю. Ісмайлов, І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро: Дніп-роп. держ. ун-т внутр.справ, 2021. 492с. URI: http://er.dduvs.in.ua/handle/123456789/6820
6. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. посіб. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 144с. URL: https://er.dduvs.in.ua/bitstream/123456789/5717/1/ПОСІБНИК%20ОУІБ%20.pdf
7. Гнусов Ю. В., Світличний В. А., Онищенко Ю. М. Спеціальна техніка Національної поліції України : навч. посіб. з дис. «Тактико-спеціальна підготовка» Харк. нац. ун-т внутр. справ, факультет № 4, каф. кібербезпеки. Харків: ХНУВС, 2017. 175 с.
8. Колісник Т. П, Сезонова І. К. Комп’ютерне діловодство для правоохоронців: навч. посіб. МВС України, Харк. нац. ун-т внутр. справ. Харків: НікаНова, 2015. 180 с. URL: https://core.ac.uk/download/pdf/187222413.pdf

Допоміжна

1. Вишня В. Б. Основи інформаційної безпеки: навч. посіб. / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро: ДДУВС, 2020. 128 с. http://er.dduvs.in.ua/handle/123456789/4206

2. Заплотинський Б.А. Інформаційні технології в юридичній діяльності. Посібник. Київський інститут інтелектуальної власності та права НУ “Одеська юридична академія”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2018.–108с.
3. Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів кругл. столу (м. Харків, 9 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020. – 132 с. http://dspace.univd.edu.ua/xmlui/handle/123456789/9984
http://dspace.onua.edu.ua/bitstream/handle/11300/11095/%D0%86%D0%A2%20%D0%B2%20%D0%AE%D0%94%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf?sequence=1&isAllowed=y
4. Інформаційне забезпечення юридичної діяльності : підручник / В.Б. Вишня, Л.В. Рибальченко, О.О. Косиченко та ін.; за заг. ред. В.Б. Вишні; МВС України, Дніпропетр. держ. ун-т внутр. справ.- Дніпро : ДДУВС, 2019.- 227 с. http://er.dduvs.in.ua/handle/123456789/3718
5. Інформаційне забезпечення діяльності Національної поліції України: зб. законодавчих та нормативних документів / уклад.:В.Б. Вишня та ін. Дніпро: ДДУВС, 2016. 476 с. http://er.dduvs.in.ua/handle/123456789/2043
6. Кормич Б.А., Федотов О.П., Аверочкіна Т.В. Правове регулювання інформаційної діяльності: навчально-методичний. Одеська юридична академія. 2018. 150 с.
https://pidruchniki.com/15931106/politologiya/pravove_regulyuvannya_informatsiynoyi_sferi_ukrayini
7. Краснобрижий І.В. Інформаційне забезпечення професійної діяльності : навч. посіб. Уклад: І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро : ДДУВС, 2018. 220 с. http://er.dduvs.in.ua/handle/123456789/2046
8. Методичні рекомендації щодо використання комп’ютерної програми «Навчальний ЄРДР» (для ролі «курсант») / [Розроб. Коршенко В. А., Демидов З. Г., Колмик О. О., Абламський С. Є.]; МВС України, Харків. нац. ун-т внутр. справ, Наук.-досл. лаб. з проблем розвитку інформац. технологій, Каф. крим. процесу та організації досуд. слідства ф-ту № 1. - Харків: ХНУВС, 2019. - 30 с. http://dspace.univd.edu.ua/xmlui/handle/123456789/6675
9. Мордвинцев М. В. Використання автоматизованих систем відеодокументування переміщень об'єкта для протидії торгівлі людьми / М. В. Мордвинцев, О. В. Хлєстков, С. П. Ницюк // Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 23 листоп. 2018 р.). – Дніпро: Дніпропетр. держ. ун-т внутріш. справ, 2018. – С. 52-54. http://dspace.univd.edu.ua/xmlui/handle/123456789/3953
10. Наказ МВС “Про затвердження Положення про Інтегровану інформаційно-пошукову систему ОВС України” від 12.10.2009 за № 436. http://tranzit.ltd.ua/nakaz/
11. Наказ МВС “Про затвердження Положення про систему Інтернет у телекомунікаційній мережі Національної поліції України” від 22.02.2017 № 141. http://tranzit.ltd.ua/nakaz/

12. Нелюбов В.О., Куруца О.С. Основи інформатики. Microsoft Word 2016: електронний навчальний посібник. Ужгород: ДВНЗ УжНУ, 2018. 96 с. https://dspace.uzhnu.edu.ua/jspui/handle/lib/18659

13. Про електронні довірчі послуги: Закон України від 5 жовтня 2017 р. № 2155-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2155-19/page

14. Проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції : методичні рекомендації / О.О. Акімова, О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков, Ю.І. Тюря. Дніпро: Дніпроп. держ. ун-т. внутр. справ, 2017. 37 с. https://dduvs.in.ua/wp-content/uploads/files/Structure/library/student/eib2.pdf

15. Ковальова О. В. Інформаційне забезпечення професійної діяльності: навч. посіб. Київ: «Дакор», 2021. 288 с.

16. Кормич Б.А., Федотов О.П., Аверочкіна Т.В. Правове регулювання інформаційної діяльності: навчально-методичний. Одеська юридична академія. 2018. 150 с. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/9530/Kormych%20Fedotov%20Averochkina%202018.pdf?sequence=1&isAllowed=y

17. Нелюбов В. О., Куруца О. С. Основи інформатики. Microsoft Word 2016: електронний навчальний посібник. Ужгород: ДВНЗ УжНУ, 2018. 96 с. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/18659

Інформаційні ресурси в Інтернеті

1. http://www.nau.kiev.ua
2. http://www.liga.kiev.ua
3. http://www.informjustr.kiev.ua
4. http://www.rada.gov.ua
5. https://zakon.rada.gov.ua
6. http://www.president.gov.ua
7. Інформаційно-пошукова правова система «Нормативні акти України» (НАУ): http://www.nau.ua
8. Офіційний сайт Національної поліції України: https://www.npu.gov.ua/
9. Офіційний сайт Єдиниго державного веб-порталу відкритих даних: https://data.gov.ua/
10. Офіційний сайт Міністерства внутрішніх справ України: https://www.mvs.gov.ua/
11. Бібліотека ХНУВС. URL: https://lib.univd.edu.ua/

Текст лекції

1. Єдина інформаційна система МВС України.

Єдина інформаційна система МВС України (ЄІС МВС) — це комплексна інформаційна платформа, створена для інтеграції та автоматизації різних підрозділів Міністерства внутрішніх справ України (МВС). Мета системи — оптимізувати обробку інформації, покращити координацію та управління діяльністю МВС, а також забезпечити прозорість, ефективність і захист даних.

Основні компоненти та функції ЄІС МВС:

Інтеграція баз даних: об'єднання різних реєстрів і баз даних МВС, таких як база даних громадян, реєстр автомобільного транспорту, дані про злочини та правопорушення, ідентифікація осіб тощо.

Автоматизація процесів: спрощення документообігу, управління запитами та зверненнями громадян, а також оперативне обслуговування правоохоронців.

Підвищення безпеки: система забезпечує високий рівень захисту даних через сучасні технології шифрування і контроль доступу.

Централізоване управління: ЄІС МВС надає єдиний інтерфейс для співробітників різних підрозділів, що сприяє покращенню взаємодії та оперативності прийняття рішень.

Моніторинг і аналітика: система дозволяє відстежувати діяльність підрозділів, аналізувати дані та створювати звіти для прийняття ефективних управлінських рішень.

ЄІС МВС допомагає спростити взаємодію між різними державними органами і громадянами, підвищуючи ефективність роботи та прозорість діяльності МВС України.

2. Поняття системи централізованого управління нарядами поліції.

ЦУНАМІ (Система централізованого управління нарядами поліції) — це інформаційно-аналітична система, призначена для оптимізації процесів управління патрульними нарядами поліції в Україні. Вона розроблена для того, щоб забезпечити ефективну координацію, контроль і управління ресурсами поліції в режимі реального часу.

Основні цілі системи ЦУНАМІ:

Оперативне управління нарядами поліції:

Забезпечення миттєвого отримання інформації про інциденти та надзвичайні ситуації.

Координація дій патрульних нарядів для швидкого реагування на події.

Моніторинг розташування патрулів:

Система використовує GPS-трекери, встановлені на поліцейських автомобілях та уніформах, для моніторингу їхнього місцезнаходження.

Це дозволяє диспетчерам ефективно розподіляти наряди в залежності від географічної близькості до місця події.

Автоматизація процесів розподілу завдань:

Алгоритми автоматично визначають найбільш оптимальні наряди для реагування на виклики, базуючись на місцезнаходженні, завантаженості та доступності нарядів.

Забезпечення прозорості і контролю:

Завдяки системі можна відслідковувати всі дії нарядів, їхні переміщення та час реагування.

Це підвищує рівень відповідальності серед правоохоронців і зменшує можливість зловживань.

Аналіз і звітність:

Система збирає дані про всі виклики, переміщення патрулів і виконання завдань, що дозволяє проводити детальний аналіз роботи підрозділів.

Це сприяє покращенню управління ресурсами та плануванню діяльності поліції.

Переваги ЦУНАМІ:

Швидке реагування на виклики завдяки оперативному розподілу завдань.

Оптимізація ресурсів, оскільки наряди розподіляються більш ефективно.

Підвищення безпеки як для громадян, так і для самих поліцейських завдяки відстеженню місцезнаходження нарядів.

Зменшення людського фактора в процесі прийняття рішень, оскільки система автоматизує частину процесів.

ЦУНАМІ є важливим інструментом для підвищення ефективності роботи поліції, а також для забезпечення безпеки та правопорядку на території України.

Система централізованого управління нарядами поліції (скорочено – система «ЦУНАМІ») являє собою комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами Національної поліції.

Дана система забезпечує користувачів необхідними інформаційними, технічними та аналітичними ресурсами для виконання функціональних обов’язків та прийняття ефективних управлінських рішень. Система фіксує, зберігає та робить доступними для аналізу та контролю повідомлення і результати реагування на них.

Мета впровадження системи «ЦУНАМІ» обумовлена необхідністю вдосконалення процесу організації діяльності з управління силами й засобами Національної поліції для ефективного реагування на повідомлення про злочини та події.

Організаційно система «ЦУНАМІ» складається з двох рівнів – міського та районного. До складу міського рівня організаційної структури входять ситуаційні центри, які діють у всіх обласних центрах України та м. Київ.

Ситуаційний центр – це підрозділ зі збору, опрацювання й аналізу інформації щодо рівня, структури і динаміки злочинності по всій Україні.

Основні компоненти системи “ЦУНАМІ”:

Організаційно-управлінський рівень

1.) Центр прийняття повідомлень – служба «102»

1.1. Служба «102»

1.2. Онлайн-сервіс 102kiev.com.ua

1.3. 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 (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).

Система централізованого управління нарядами поліції (скорочено – система «ЦУНАМІ») являє собою комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами Національної поліції.

Мета впровадження системи «ЦУНАМІ» обумовлена необхідністю вдосконалення процесу організації діяльності з управління силами й засобами Національної поліції для ефективного реагування на повідомлення про злочини та події.

Досягнення зазначеної мети забезпечується виконанням таких завдань:

– оптимізація роботи нарядів патрульної поліції, слідчо-оперативних груп чергових частин;

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

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

Скорочення часу реагування на повідомлення громадян про злочини та події відбувається за рахунок оптимізації відповідних інформаційних потоків.

Потоки інформації, які надходять в службу «102» по Україні, можна оцінити таким чином:

– загальне навантаження на службу «102» – близько 3 тис. викликів на добу;

– середній час дозвону заявника – 5–10 сек.;

– сумарний потік інформації на один пульт – до 280 звернень за добу.

Організаційно система «ЦУНАМІ» складається з двох рівнів – міського та районного.

До складу міського рівня організаційної структури входять ситуаційні центри, які діють у всіх обласних центрах України та м. Київ.

Створення системи ситуаційних центрів почалося разом зі створенням Національної поліції близько двох років тому. По-перше, було зрозуміло, що колишні чергові частини не відповідають сучасним вимогам, і, як результат, правоохоронці сильно програють у швидкості реагування. По-друге, збільшилася кількість звернень громадян. Ще кілька років тому протягом року до поліції зверталося близько 3 млн осіб, у 2017 році ця цифра перевалила за 7 млн. Свою роль зіграла патрульна поліція. Було створено патрульну поліцію, яка зараз працює в 33 містах. У сільських районах і невеликих містах розгорнуто групи реагування патрульної поліції, їх понад 1 тис. Також до системи реагування включено всю поліцію охорони, 450 нарядів, і всі слідчо-оперативні групи, які працюють у кожному відділі та відділку поліції. У зв'язку з цим виникла необхідність створення при Національній поліції ситуаційних центрів для відпрацювання всього масиву повідомлень та ефективного управління нарядами поліції.

Ситуаційний центр – це підрозділ зі збору, опрацювання й аналізу інформації щодо рівня, структури і динаміки злочинності по всій Україні. Є ситуаційний центр Нацполіції, де проводиться лише збір та опрацювання інформації, і ситуаційні центри в місті Києві та областях, у складі яких працює і служба «102».

3. Автоматизоване робоче місце працівника підрозділу "102" (АРМ "оператор "102") системи ІПНП. Автоматизоване робоче місце (АРМ) "диспетчер" системи ІПНП.

Розглянемо типову робочу зміну ситуаційного центру обласного рівня:

– оперативний черговий – старший зміни центру;

– диспетчер (помічник) - обробляє інформацію внесену до ІІПС ОНП забезпечує передачу спецповідомлень, контролює надходження електронної почти;

– 10 операторів лінії «102», які приймають повідомлення від громадян та вводять її до електронної картки;

– 4 інспектори керування нарядами забезпечують ефективне управління силами та засобами задіяними по ОГП в області, інспектор системи відеоспостереження контролює відеоінформацію з відеокамер та передає для реагування або веде спостереження за масовими заходами в зоні розміщення камер;

– 2 інспектори з аналітики обробляють отриману інформацію про події проводять аналіз, готують аналітичні довідки, працюють з електронною картою подій;

– інспектор стаціонарного пульта моніторингу поведінки за особами до яких застосовано електронні засоби контролю (ЕЗК).

До складу районного рівня організаційної структури входять наступні підрозділи:

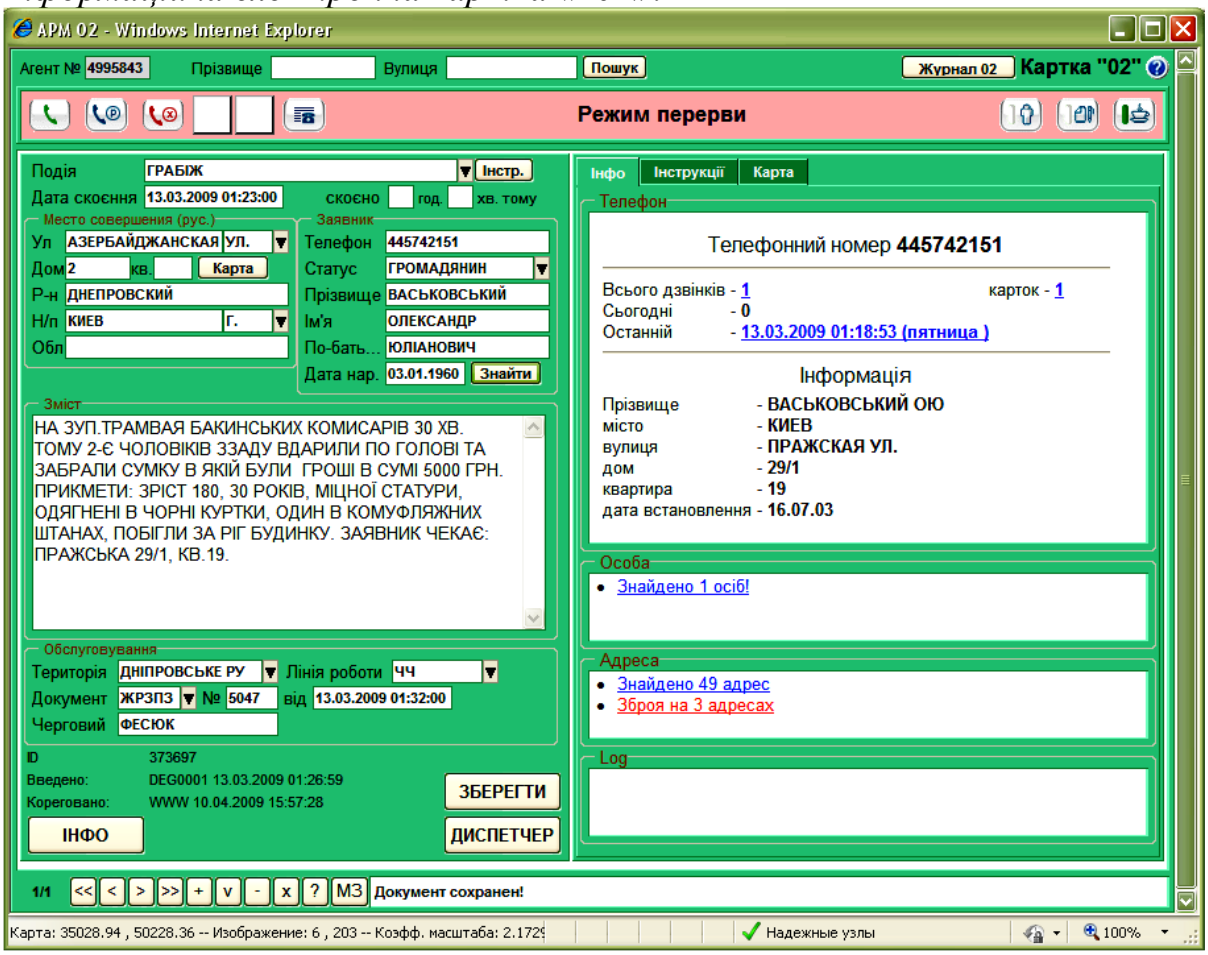
1. Чергові частини районних підрозділів Національної поліції.
2. Слідчо-оперативні групи.
3. Додаткові сили (дільничні інспектори поліції тощо).

У якості платформи для автоматизації служби «102» використовується сучасний цифровий call-центр (AWAYA), який інтегровано в існуючу інформаційну систему Національної поліції, що дозволило операторові одержувати інформацію про абонента ще до моменту підняття трубки, а саме:

– 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 тієї події, про яку повідомлено;
– попередження про дзвінки абонентів, які внесено до окремого списку: психічно хворі, телефонні хулігани та інше.

При випадковому обриві зв'язку оператор сам може передзвонити абоненту. У разі, якщо оператор «102» виходить на технічну перерву, всі дзвінки автоматично та рівномірно розподіляються на інших операторів.

Інформаційна електронна картка «102».



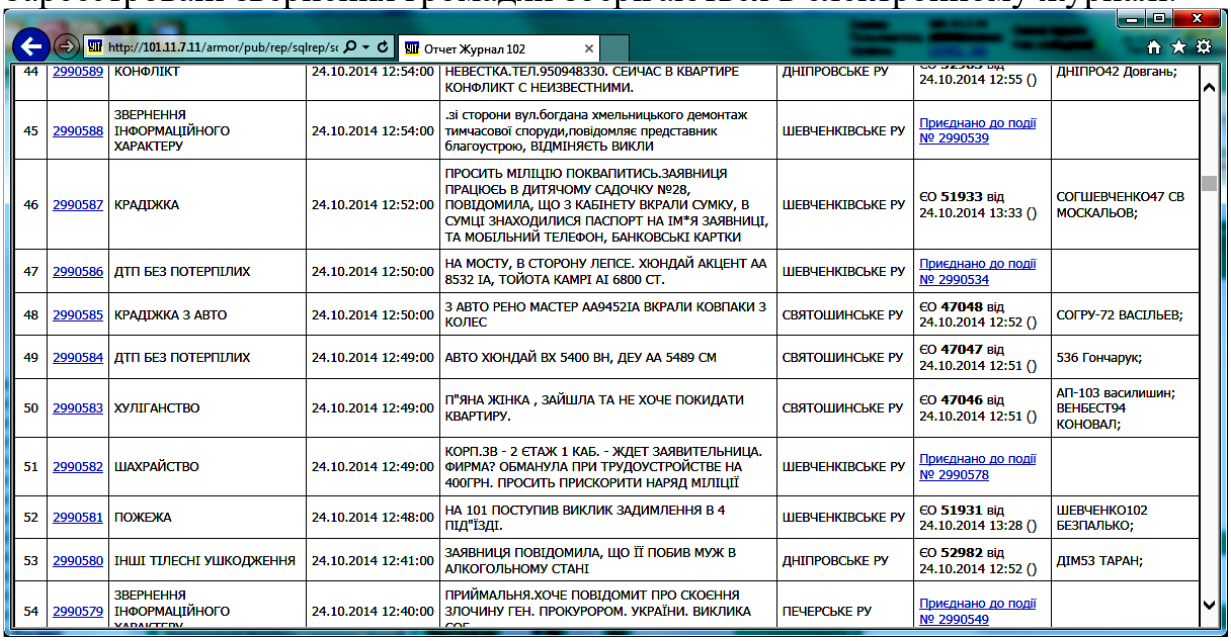
При заповненні електронної картки, оператор «102» здійснює попередню кваліфікацію події, про яку повідомлено. Заповнена оператором електронна картка відразу надходить до диспетчера-чергового відповідального за керування нарядами поліції в тому чи іншому районі міста.

Відповідне програмне забезпечення відображає інформацію про місце вчинення злочину на електронній карті міста.

Надалі електронна картка надходить до системи «ЦУНАМІ», і її обробленням займається диспетчер-черговий Головного управління (керує патрульними нарядами поліції для оперативного реагування на звернення) і оперативний черговий відповідного районного управління, до території якого відноситься звернення (реєструє звернення у журналі Єдиного обліку злочинів і правопорушень районного підрозділу Національної поліції).

Електронна картка, сформована оператором «102» одночасно відображається у чергового, що перебувають у диспетчерському центрі, та чергового відповідного райвідділу поліції на території якого відбувається подія (було вчинено правопорушення).

Зареєстровані звернення громадян зберігаються в електронному журналі.



44	2990589	КОНФЛІКТ	24.10.2014 12:54:00	НЕВЕСТКА.ТЕЛ.950948330. СЕЙЧАС В КВАРТИРЕ КОНФЛИКТ С НЕИЗВЕСТНИМИ.	ДНІПРОВСЬКЕ РУ	24.10.2014 12:55 ()	ДНІПРО42 Довгань;
45	2990588	ЗВЕРНЕННЯ ІНФОРМАЦІЙНОГО ХАРАКТЕРУ	24.10.2014 12:54:00	.зі сторони вул.богдана хмельницького демонтаж тимчасової споруди,повідомляє представник благоустрою, ВІДМІНЯЄТЬ ВИКЛИ	ШЕВЧЕНКІВСЬКЕ РУ	Приєднано до події № 2990539	
46	2990587	КРАДІЖКА	24.10.2014 12:52:00	ПРОСИТЬ МІЛІЦІЮ ПОКВАПИТИСЬ.ЗАЯВНИЦЯ ПРАЦЮЄЬ В ДИТЯЧОМУ САДОЧКУ №28, ПОВІДОМИЛА, ЩО З КАБІНЕТУ ВКРАЛИ СУМКУ, В СУМЦІ ЗНАХОДИЛИСЯ ПАСПОРТ НА ІМ*Я ЗАЯВНИЦІ, ТА МОБІЛЬНИЙ ТЕЛЕФОН, БАНКОВСЬКІ КАРТКИ	ШЕВЧЕНКІВСЬКЕ РУ	ЄО **51933** від 24.10.2014 13:33 ()	СОГШЕВЧЕНКО47 СВ МОСКАЛЬОВ;
47	2990586	ДТП БЕЗ ПОТЕРПІЛИХ	24.10.2014 12:50:00	НА МОСТУ, В СТОРОНУ ЛЕПСЕ. ХЮНДАЙ АКЦЕНТ АА 8532 ІА, ТОЙОТА КАМРІ АІ 6800 СТ.	ШЕВЧЕНКІВСЬКЕ РУ	Приєднано до події № 2990534	
48	2990585	КРАДІЖКА З АВТО	24.10.2014 12:50:00	З АВТО РЕНО МАСТЕР АА9452ІА ВКРАЛИ КОВПАКИ З КОЛЕС	СВЯТОШИНСЬКЕ РУ	ЄО **47048** від 24.10.2014 12:52 ()	СОГРУ-72 ВАСІЛЬЄВ;
49	2990584	ДТП БЕЗ ПОТЕРПІЛИХ	24.10.2014 12:49:00	АВТО ХЮНДАЙ ВХ 5400 ВН, ДЕУ АА 5489 СМ	СВЯТОШИНСЬКЕ РУ	ЄО **47047** від 24.10.2014 12:51 ()	536 Гончарук;
50	2990583	ХУЛІГАНСТВО	24.10.2014 12:49:00	П"ЯНА ЖІНКА , ЗАЙШЛА ТА НЕ ХОЧЕ ПОКИДАТИ КВАРТИРУ.	СВЯТОШИНСЬКЕ РУ	ЄО **47046** від 24.10.2014 12:51 ()	АП-103 василишин; ВЕНБЕСТ94 КОНОВАЛ;
51	2990582	ШАХРАЙСТВО	24.10.2014 12:49:00	КОРП.3В - 2 ЄТАЖ 1 КАБ. - ЖДЕТ ЗАЯВИТЕЛЬНИЦА. ФИРМА? ОБМАНУЛА ПРИ ТРУДОУСТРОЙСТВЕ НА 400ГРН. ПРОСИТЬ ПРИСКОРИТИ НАРЯД МІЛІЦІЇ	ШЕВЧЕНКІВСЬКЕ РУ	Приєднано до події № 2990578	
52	2990581	ПОЖЕЖА	24.10.2014 12:48:00	НА 101 ПОСТУПИВ ВИКЛИК ЗАДИМЛЕННЯ В 4 ПІД"ЇЗДІ.	ШЕВЧЕНКІВСЬКЕ РУ	ЄО **51931** від 24.10.2014 13:28 ()	ШЕВЧЕНКО102 БЕЗПАЛЬКО;
53	2990580	ІНШІ ТІЛЕСНІ УШКОДЖЕННЯ	24.10.2014 12:41:00	ЗАЯВНИЦЯ ПОВІДОМИЛА, ЩО ЇЇ ПОБИВ МУЖ В АЛКОГОЛЬНОМУ СТАНІ	ДНІПРОВСЬКЕ РУ	ЄО **52982** від 24.10.2014 12:52 ()	ДІМ53 ТАРАН;
54	2990579	ЗВЕРНЕННЯ ІНФОРМАЦІЙНОГО	24.10.2014 12:40:00	ПРИЙМАЛЬНЯ.ХОЧЕ ПОВІДОМИТ ПРО СКОЄННЯ ЗЛОЧИНУ ГЕН. ПРОКУРОРОМ. УКРАЇНИ. ВИКЛИКА	ПЕЧЕРСЬКЕ РУ	Приєднано до події № 2990549	

Диспетчер системи «ЦУНАМІ» є оперативним черговим і куратором кожного конкретного райуправління поліції, відповідальним за організацію реагування на злочини та пригоди в районах. До функцій чергових-диспетчерів входить:

– управління нарядами поліції;

– отримання інформації з служби «102» та відстеження на електронній карті місць учинення правопорушень;

– передача даних про правопорушення на планшет конкретного патруля поліції;

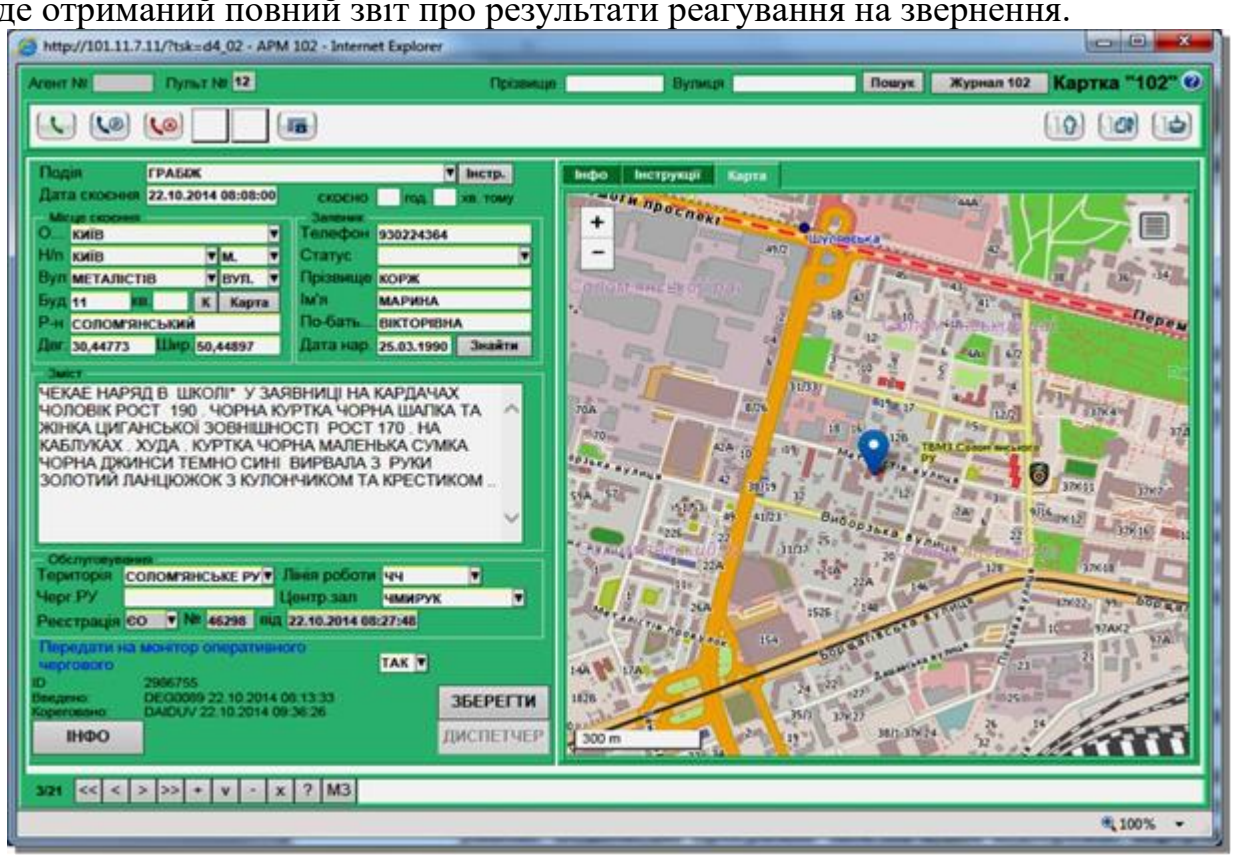
– забезпечення відповідного патруля всією наявною інформацією, що знаходиться у відомчих інформаційних масивах, про заявника та адресу виїзду;

– 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 наряд)' та відстеження результатів реагування на заяви та повідомлення громадян про злочини, прийняті рішення тощо.

Патруль одержує від диспетчера у формі електронного повідомлення основні дані із заяви, у тому числі номер заявника.

За результатами реагування диспетчер ставить відповідні відмітки. Інформаційна електронна картка залишається у диспетчера на контролі, поки не буде отриманий повний звіт про результати реагування на звернення.



При здійсненні планування розстановки сил та засобів, задіяних для охорони громадського порядку, в системі використовується криміналістичний аналіз, який відображає оперативну обстановку на території обслуговування Національної поліції в різних розрізах та геоінформаційною прив’язкою до місцевості.

В системі використовуються звіти та аналітичні форми наступного характеру:

– аналіз реєстрації подій та правопорушень в розрізі підрозділів Національної поліції;

– аналіз реєстрації подій та правопорушень в розрізі видів злочинів;

– аналіз реєстрації подій та правопорушень по часу скоєння;

– відомості про час призначення та час прибуття нарядів з моменту отримання повідомлення службою «102»;

– відомості про час прибуття СОГ на місце події;

– список завдань по часу прибуття/відпрацювання патрулів;

– кількість повторних викликів за період тощо.

Автоматизоване робоче місце диспетчера міського управління патрульної поліції забезпечує управління нарядами для реагування на прийняті злочини та події, а саме:

– відображає перелік подій, прийнятих оператором «102», які були вчинені в районі обслуговування;

– відображає дислокацію та стан роботи патрульних нарядів;

– інформує, у кольоровій гаммі, про послідовність реагування на подію;

– сигналізує про перевищення часових нормативів окремих етапів виконання завдання;

– в разі визначення телефонного номера заявника відображає накопичені дані по цьому номеру (за якою адресою встановлено, кількість та зміст попередніх звернень);

– надає можливість зв’язатись з оператором «102», який прийняв виклик;

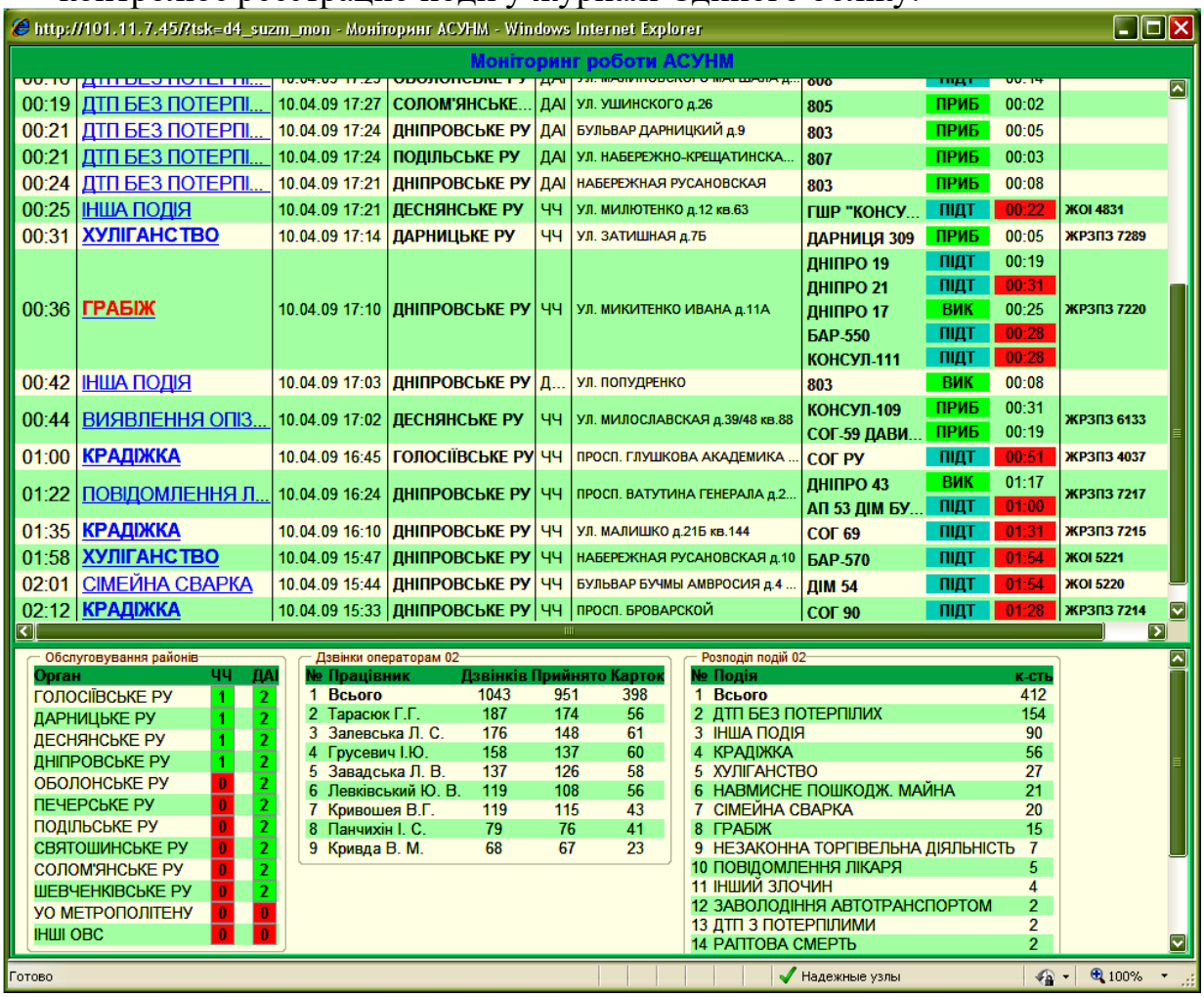
– надає можливість зв’язатись з заявником для уточнення даних по події;

– в разі отримання ПІБ заявника надає всю наявну інформацію про особу з інтегрованого банку даних «АРМОР»;

– надає повну інформацію на адресу з інтегрованого банку даних «АРМОР»;

– інформує про повторність надходження інформації про подію;

– контролює реєстрацію події у журналі Єдиного обліку.



Система в автоматичному режимі на протязі 30 хв. (якщо черговий самостійно не здійснить реєстрацію раніше) проводить реєстрацію звернення з

картки «102» в електронний журнал «Єдиного обліку» (ЄО) та приєднує картку «102» до картки ЄО як джерело початкової інформації, що перешкоджає укриттю злочинів на стадії їх кваліфікації в районних управліннях, оскільки оператор «102» та диспетчер відокремлені від впливу керівників територіальних органів.

Наряди патрульної поліції:

– відпрацьовують завдання, що надійшли від чергового-диспетчера;

– фіксують виконання етапів завдання за допомогою логістичного мобільного пристрою;

– надають короткий рапорт про виконання завдання (про результати реагування на звернення);

– взаємодіють з іншими патрулями з метою розкриття злочинів по «гарячих слідах».

Геоінформаційна система (електронна карта міста) використовується для візуального відображення на електронній карті міста місць учинення злочинів, усіх мобільних патрульних нарядів, оснащених GPS-приймачами, які в цей період часу виконують службові обов'язки.

Геоінформаційна система з відповідним програмним забезпеченням допомагає вирішити наступні завдання:

– планування і розміщення сил та засобів Національної поліції на підлеглій території, маршрутів та зон патрулювання (на підставі накопиченої статистики стосовно місць скоєння злочинів - CrimeAnalytics);

– контроль за діяльністю нарядів поліції з використанням системи супутникового позиціонування GPS;

– організація взаємодії нарядів поліції;

– при необхідності надає інтерактивну рекомендацію-підказку щодо призначення патрулів на подію для реагування;

– інтерактивний аналіз і розбір дій підрозділів Національної поліції при реагуванні на правопорушення;

– можливість відображення маршруту (треку) руху автопатруля;

– виявлення патрулів, треки яких перетинали визначену територію у визначений час;

– графічне відображення стану оперативної обстановки та статистичного аналізу по видах злочинів.

Система супутникового GPS-позиціювання та мобільного комунікаційного обладнання. Необхідною складовою системи є оснащення патрулів системою супутникового GPS-позиціювання та мобільного комунікаційного обладнання з можливістю підключення до інформаційних обліків Національної поліції. Таке обладнання дозволяє відслідковувати місцезнаходження патруля, напрямки його руху та статус на даний час (зайнятий, вільний, на перерві).

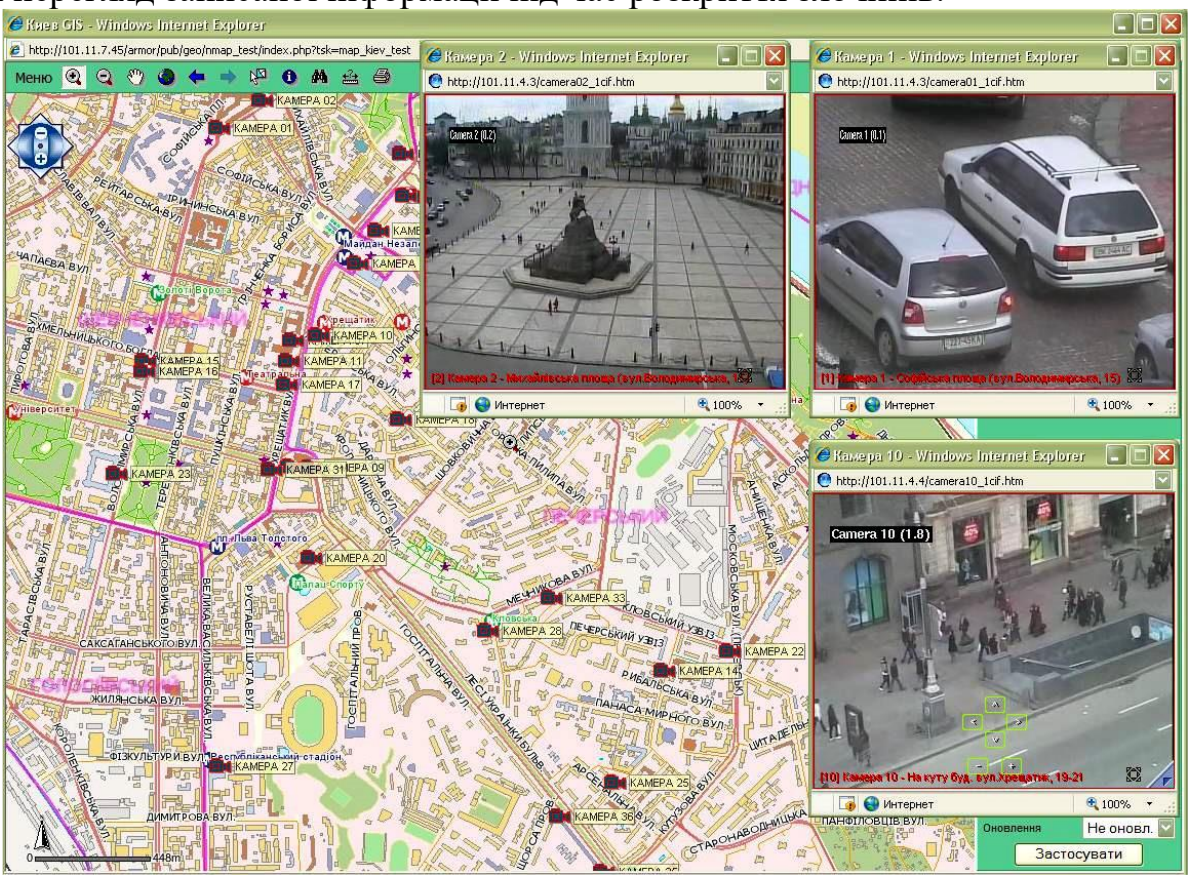
В салоні автопатруля встановлюється спеціальний блок керування та відображення. Цей пристрій фактично є портативним комп’ютером, який дозволяє отримувати завдання від диспетчера-чергового в електронному вигляді, автоматично прокладати маршрут до місця скоєння, надає можливість інформувати диспетчера, що наряд приступив до виконання завдання, прибув на місце пригоди, виконав завдання або завершив патрулювання. Також цей пристрій забезпечує доступ до інформаційної системи «АРМОР», що дозволяє працівнику поліції безпосередньо на місці при необхідності отримати інформацію з інформаційних обліків Національної поліції.

З моменту підтвердження прийому завдання система розпочинає супроводження руху наряду до місця події. В разі значного відхилення від нормативів часу реагування на той чи інший злочин система автоматично повідомляє про це чергового та пропонує додатково направити на місце події інший патруль.

З моменту підтвердження прийому завдання система розпочинає супроводження руху наряду до місця події. В разі значного відхилення від нормативів часу реагування на той чи інший злочин система автоматично

повідомляє про це чергового та пропонує додатково направити на місце події інший патруль.

Система відеоспостереження. Метою впровадження такої системи є необхідність оперативного візуального контролю за основними криміногенними місцями, вулицями, площами, транспортними потоками, а також перегляд записаної інформації під час розкриття злочинів.



Таким чином, телекомунікаційна мережа доступу системи ІПНП є 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 Міністерства внутрішніх справ України, а при використанні відкритих каналів - засоби захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

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.

Контроль за дотриманням вимог законодавства України в сфері захисту інформації під час використання ІПНП здійснює керівник підрозділу, де експлуатується центральний програмно-технічний комплекс системи.

3. Організація інформаційно-аналітичного забезпечення Національної поліції України

З метою організації інформаційно-аналітичного забезпечення поліції було розроблено Положення про інформаційно-телекомунікаційна систему «Інформаційний портал Національної поліції України». Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (далі - система ІПНП) - сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення.

Розглянемо *основні завдання системи «Інформаційний портал Національної поліції України»*, до них належать:

– інформаційно-аналітичне забезпечення діяльності Національної поліції України;

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

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

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

Система «Інформаційний портал Національної поліції України» призначена для:

– формування інформаційних ресурсів ЄІС МВС;

– обробки інформації, яка утворена в процесі діяльності поліції; □ надання безпосереднього оперативного доступу до інформаційних ресурсів ЄІС МВС;

– генерації інтерфейсів та оброблення тимчасових наборів даних для здійснення інформаційної взаємодії органів (підрозділів) поліції з іншими органами державної влади, органами правопорядку іноземних держав, міжнародними організаціями;

– здійснення пошукових та аналітичних функцій для використання інформації з інформаційних ресурсів (баз даних) поліції, МВС та інших органів державної влади в межах службової діяльності відповідно до рівня доступу і повноважень за запитом або регламентом;

– використання програмних компонентів геоінформаційних підсистем для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об'єкта в залежності від зміни його характеристик, зміни масштабу та деталізації картографічної інформації в інформаційних ресурсах;

– забезпечення автоматизації процесів управління силами та засобами поліції;

– забезпечення електронного документообігу в органах (підрозділах) поліції, обміну електронними документами з МВС;

– комплексного захисту інформації та розмежування доступу до інформації, що зберігається в базах даних системи «Інформаційний портал Національної поліції України».

В інформаційних ресурсах системи «Інформаційний портал Національної поліції України» обробляється інформація, яка належить до державних інформаційних ресурсів. Така інформація не підлягає поширенню та передачі іншим особам, крім випадків, передбачених законодавством. Інформаційними ресурсами системи ІПНП є інформація, що утворена в процесі діяльності поліції та використовується для формування:

– тимчасових наборів даних, що створюються в процесі діяльності поліції та використовуються для наповнення та підтримки в актуальному стані баз (банків) даних, які входять до ЄІС МВС та визначені статтею 26 Закону України «Про Національну поліцію»;

– баз даних у сфері управлінських відносин, необхідних для виконання покладених на поліцію повноважень;

– баз даних, необхідних для забезпечення щоденної діяльності поліції, у сфері трудових відносин, фінансового забезпечення, документообігу.

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

– повідомлень про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, що надійшли технічними каналами зв’язку;

– щодобових переліків та складу нарядів поліції та слідчо-оперативних груп, що заступають на чергування; □ завдань та орієнтувань, що доводились до нарядів поліції для реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події;

– звітування нарядів поліції за результатами реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, виявлення додаткових обставин на місці пригоди;

– пересувань нарядів поліції, які отримані із планшетних комп’ютерів (мобільних терміналів) та засобами GPS. Поліція може створювати інші бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, відповідно до статті 25 Закону України «Про Національну поліцію».

Розпорядником системи «Інформаційний портал Національної поліції України» є Національна поліція України, який вживає заходів із організації матеріально-технічного та кадрового забезпечення, що необхідні для ефективного функціонування системи. Адміністратором системи ІПНП є уповноважений структурний підрозділ апарату центрального органу управління Національної поліції України, який забезпечує:

– вирішення організаційних питань щодо забезпечення функціонування системи;

– ведення обліку користувачів та надання їм доступу до інформації, що в ній обробляється;

– захист інформації від несанкціонованого доступу, знищення, модифікації та блокування доступу до неї шляхом здійснення організаційних і технічних заходів, впровадження засобів та методів технічного захисту інформації;

– вжиття заходів стосовно розвитку і вдосконалення системи;

– координацію функціонування складових системи.

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

Складові системи «Інформаційний портал Національної поліції».

Складовими системи «Інформаційний портал Національної поліції України» є:

– центральний програмно-технічний комплекс;

– автоматизовані робочі місця користувачів;

– телекомунікаційна мережа доступу;

– комплексна система захисту інформації.

Центральний програмно-технічний комплекс системи «Інформаційний портал Національної поліції України» - 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 «Інформаційний портал Національної поліції України»;

– формування тимчасових наборів даних для наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних ЄІС МВС;

– моніторинг стану інформаційного обміну між складовими системи ІПНП, а також системних журналів аудиту роботи користувачів, технічних і програмних засобів;

– захист інформації під час її обробки.

До складу центрального програмно-технічного комплексу системи «Інформаційний портал Національної поліції України» входять:

– центральне сховище даних - програмно-технічний комплекс, який складається із серверів, систем керування базами даних та іншого програмного

забезпечення, призначених для безперервного виконання операцій, записування, зберігання, знищення, приймання та передавання інформації, зберігання системних журналів аудиту роботи користувачів та системних журналів реєстрації роботи програмних засобів;

– сервери додатків - програмно-технічний комплекс, який складається із серверів та програмного забезпечення, призначених для безперервного виконання операцій з інформаційного обміну між складовими системи ІПНП, функціонування програмних засобів генерації інтерфейсів користувачів для оброблення інформації, записування та зберігання системних журналів аудиту приймання та передавання інформації, реєстрації роботи програмних засобів;

– шлюзові сервери - програмно-технічний комплекс, який складається із серверів, призначених для забезпечення захисту інформації під час здійснення обміну інформацією між підсистемами, взаємодії з інформаційними системами МВС та інших центральних органів виконавчої влади;

– автоматизоване робоче місце адміністратора безпеки - складова комплексної системи захисту інформації в системі ІПНП, обладнана технічними засобами та програмним забезпеченням, призначеними для моніторингу системних журналів реєстрації роботи програмних та технічних засобів, аналізу порушень в роботі системи ІПНП, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів, визначення повноважень користувачів системи ІПНП.

Центральний програмно-технічний комплекс системи «Інформаційний портал Національної поліції України» розміщується в спеціалізованих службових приміщеннях Національної поліції України.

Розглянемо 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 «Інформаційний портал Національної поліції України» і призначені для автоматизації службової діяльності, реалізації повноважень обробляти інформацію відповідно до наданого рівня доступу в системі ІПНП.

Телекомунікаційна мережа доступу системи «Інформаційний портал Національної поліції України» - 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 Міністерства внутрішніх справ України, а при використанні відкритих каналів - засоби захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

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

«Інформаційний портал Національної поліції України» 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.

До складу Єдиної інформаційної системи Міністерства внутрішніх справ входять:

Інтегрована інформаційно-пошукова система Національної поліції.

Система централізованого управління нарядами патрульної поліції «ЦУНАМІ»

ДБД Арсенал – відомості щодо зброї, яка перебуває на озброєнні МВС, МО, МНС, АДПС, СБУ, ДПА, ДМС, ДДПВП, УДО.

ІС Оріон – єдині оперативні обліки, які передбачені Законом України „Про оперативно-розшукову діяльність”.

ОДК – оперативно-довідкова картотека, в який розміщено відомості щодо притягнення осіб до кримінальної відповідальності та судимості осіб.

АДІС "ДАКТО"- автоматична дактилоскопічна інформаційна система.

Складові центрального ПТК ІПНП повинні забезпечити генерацію інтерфейсів, оброблення тимчасових наборів та формування інформаційних ресурсів ЄІС МВС для наступних підсистем:

1) ІП «*Єдиний облі*к» – автоматизований облік заяв і повідомлень про вчинені кримінальні правопорушення та інші події, зареєстрованих органами Національної поліції України, у тому числі їх структурними (відокремленими) підрозділами (управліннями, відділами, відділеннями), а також організація контролю за дотриманням порядку веденням цього обліку відповідно до Інструкції (п.1.4.3.2);

2) ІП «*Кримінальна статистика*» – автоматизований облік відомостей про кримінальні правопорушення, осіб, які їх учинили або підозрюються в їх учиненні, досудове розслідування за якими здійснюється слідчими органів поліції. Ведення обліку регламентовано Положенням (п. 1.4.3.3);

3) ІП «*Адміністративна практика*» – автоматизований облік відомостей щодо зареєстрованих в органах поліції адміністративних правопорушень, осіб, які їх учинили, результатів розгляду цих правопорушень та виконання накладених стягнень у вигляді штрафів та обмін даними про виписки з рахунків надходжень державного бюджету щодо адміністративних штрафів між інформаційною підсистемою «бюджетна установа МВС» та системою ІПНП. Ведення обліку регламентовано інструкціями (п.п. 1.4.3.14, 1.4.3.15, 1.4.3.16);

4) ІП «*Корупція*» – автоматизований облік даних стосовно всіх зареєстрованих кримінальних та адміністративних корупційних правопорушень, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах. Ведення обліку регламентовано Інструкцією (п.1.4.3.4);

5) ІП «*Особа*» («Правопорушник» та «Підсудний») – автоматизований облік інформації про осіб, щодо яких поліцейські здійснюють профілактичну роботу, а також про обвинувачених осіб, обвинувальний акт щодо яких направлено до суду;

6) ІП «Розшук» – автоматизований облік відомостей щодо розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання, безвісно зниклих та інших категорій осіб, які розшукуються відповідно до Інструкції (п.1.4.3.5);

7) ІП «*Пізнання*» – автоматизований облік інформації у тому числі біометричних даних щодо осіб, які переховуються від органів влади, безвісно зниклих осіб, невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком. Ведення обліку регламентовано Інструкцією (п.1.4.3.5. та 1.4.3.13);

8) ІП «*Гарпун*» – автоматизований облік даних про транспортні засоби, які пересуваються шляхами загального користування та номерні знаки, які розшукуються з будь-яких підстав у рамках кримінального або виконавчого провадження, стали засобом або предметом учиненого кримінального правопорушення, та інші відомості про транспорт, які можуть становити службовий інтерес для правоохоронних органів при з'ясуванні об'єктивних обставин у разі встановлення або запобігання факту порушень прав та свобод людини, гарантованих державою;

9) ІП «*Номерні речі*» – автоматизований облік відомостей щодо речей, викрадених, вилучених з ознаками підробки, заборонених або обмежених в обігу у фізичних осіб, безгосподарних, знайдених або вилучених із камер схову вокзалів, аеропортів, зданих до органів поліції, які мають індивідуальні заводські (фабричні) номери;

10) ІП «*Культурні цінності*» – автоматизований облік даних щодо викрадених, вилучених культурних цінностей, що належать до об'єктів матеріальної і духовної культури та мають художнє, історичне, етнографічне та наукове значення, матеріали щодо яких зареєстровано органами поліції;

11) ІП «Кримінальна зброя» – автоматизований облік відомостей про викрадену, втрачену, вилучену, знайдену зброю, а також добровільно здану зброю із числа тієї, що незаконно зберігалася, незалежно від її технічного стану, що має індивідуальні заводські (фабричні) номери або номери деталей: нарізної, комбінованої, гладкоствольної, газової, пневматичної, стартової, сигнальної, під патрон Флобера, холодної, пристроїв для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями метальними снарядами несмертельної дії. Ведення обліку регламентовано Інструкцією (п.1.4.3.6); 12) ІП «Зареєстрована зброя» – автоматизований облік відомостей стосовно зброї, що має індивідуальні заводські (фабричні) номери, перебуває в користуванні громадян, підприємств, установ, організацій, господарських об'єднань, яким надано, відповідно до законодавства, дозвіл на її придбання, зберігання, носіння, перевезення, та яка обліковується органами поліції: нарізної, комбінованої, гладкоствольної, газової, пневматичної, холодної, пристроїв вітчизняного виробництва для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями метальними снарядами несмертельної дії. Ведення обліку регламентовано Інструкцією (п.1.4.3.6);

13) ІП «*Домашній арешт*» – автоматизований облік даних стосовно підозрюваних, обвинувачених, щодо яких застосовано запобіжний захід у

вигляді домашнього арешту. Ведення обліку регламентовано Інструкцією, зазначеною у п.1.4.3.7;

14) ІП «*Документ*» – автоматизований облік відомостей про викрадені (втрачені) паспортні документи, інформацію щодо яких зареєстровано органами поліції за зверненнями громадян;

15) ІП «*Атріум*» – автоматизований облік даних стосовно осіб, звільнених з місць позбавлення волі, засуджених та тих, які притягаються до кримінальної відповідальності;

16) ІП «*Дактилоскопічний облік*» – автоматизований облік відомостей про дактилоскопічні карти, складені щодо осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученням органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт), а також невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв’язку з хворобою або неповнолітнім віком;

17) ІП «*Аналітика*» – програмний комплекс аналітичних засобів забезпечує роботу генератора запитів та генератора звітів. Генератор запитів - уніфікована система пошукових та аналітичних сервісів для використання інформації з інформаційних ресурсів (тимчасових наборів даних, баз даних) поліції, МВС та інших органів державної влади для забезпечення службової діяльності працівників поліції відповідно до їх повноважень та наданого рівня доступу.

18) *Підсистема підтримки електронних цифрових підписів* – це програмні засоби, що розміщуються та функціонують на програмно-технічних потужностях ІПНП та забезпечують можливості накладання електронного цифрового підпису на документи, утворені в процесі оперативно-службової діяльності поліції в електронному вигляді та внесені до ІПНП, контролю за автентифікацією дій користувачів, які вносять будь-які зміни до системи ІПНП, використання ЕЦП для засобів криптографічного захисту інформації, взаємодії з центрами сертифікації ключів;

19) *ІП Аналітика ситуаційних центрів* – сукупність програмних модулів для формування узагальнених автоматизованих відомостей, інформаційно-аналітичних матеріалів з питань протидії злочинності, у тому числі за окремими видами кримінальних правопорушень та на території окремих регіонів, забезпечення публічного порядку та безпеки, протидії терористичній діяльності, ліквідації наслідків стихійного лиха тощо. Забезпечує узагальнення та моніторинг відомостей про кримінальні правопорушення, надзвичайні ситуації та інші події, які надходять з різних джерел за визначеними або пов’язаними параметрами – ознаками, джерелами, фактами, об’єктами, особами, які необхідні для підготовки та прийняття управлінських рішень у сфері забезпечення охорони прав і свобод людини, публічної безпеки і порядку, протидії злочинності та терористичній діяльності, надання відповідної інформації керівництву Національної поліції України та органам і підрозділам поліції. Функціонування підсистеми регламентовано Положенням (п.1.4.3.12);

20) *ІП ведення користувачів ІПНП* – забезпечує реалізацію таких функцій:

– реєстрація користувачів центрального ПТК;

– надання користувачам центрального ПТК прав доступу до програмних комплексів та інформаційних підсистем з відповідними «привілеями»;

– блокування, видалення (відміна), зміна «привілеїв» та редагування запису користувача центрального ПТК;

– перегляд системних журналів стосовно дій користувачів;

– підтвердження зміни повноважень користувача відповідно до підсистеми управління персоналом.

21) *ІП Кримінальна аналітика* – забезпечує доступ (інформаційну взаємодію) до інформаційних ресурсів окремим програмним засобам або формує необхідні інтерфейси, що використовуються для функціонування моделі поліцейської діяльності, керованої аналітикою «Intelligence Led Policing»;

22) *ІП Ведення класифікаторів* – призначена для редагування набору типових записів, що використовуються в інформаційних підсистемах та програмних комплексах центрального ПТК;

23) *ІП Конвертації інформації* – забезпечує перенесення та модифікацію даних між наявною та модернізованою системою ІПНП.

Формування у складі центрального ПТК ІПНП власних баз даних у сфері управлінських відносин, необхідних для виконання покладених на поліцію повноважень, а також забезпечення щоденної діяльності поліції у сфері трудових, фінансових відносин, відносин документообігу:

1) *ІП фінансово-господарською діяльності* – автоматизована підсистема обліку однострою, службового автотранспорту та майна органів та структурних підрозділів Національної поліції;

2) ІП «*Рекрутинг*» – автоматизована система підбору кадрів, яка призначена забезпечувати проведення конкурсу на вакантні посади в НПУ та його інформаційне супроводження (окрім вакантних посад до підрозділів патрульної поліції);

3) ІП «*Кадри*» – автоматизована підсистема обліку персоналу НПУ;

4) ІП «*Архів*» – автоматизований облік відомостей про склад, зміст і місцезнаходження архівних фондів і (або) архівних документів, створених під час діяльності органів і підрозділів поліції;

5) *ІП СЕДО* (Система електронного документообігу) – призначена для документального забезпечення процесів управління та автоматизації діловодства та документообігу, здійснення контролю за виконавською дисципліною, забезпечення обробки електронних документів та за необхідності, документів у паперовому вигляді в діяльності Національної поліції та МВС. Ведення системи регламентовано Вимогами (п. 1.4.3.11);

6) *ІП Система електронної взаємодії державних електронних інформаційних ресурсів* – це окремий абонентський програмний модуль, що розміщується та функціонує на програмно-технічних потужностях ІПНП,

призначений для автоматизації та технологічного забезпечення обміну електронними даними між суб’єктами владних повноважень з державними електронними інформаційними ресурсами під час надання адміністративних послуг та здійснення інших повноважень відповідно до покладених на них завдань шляхом використання сервіс-орієнтованої архітектури, що є інтерфейсами прикладного програмування доступу до державних електронних інформаційних ресурсів, побудованими згідно з єдиними вимогами, а також шляхом використання єдиних форматів, протоколів, довідників, шаблонів та класифікаторів. Функціонування підсистеми регламентовано Постановою (п.1.4.2.2);

7) *Call-центр Національної поліції* – автоматизована система прийому повідомлень на «гарячу» телефонну лінію 0800-500202. Забезпечує прийняття, фіксацію, оброблення та реєстрацію звернень громадян щодо питань, пов'язаних з діяльністю поліції (довідкова інформація, скарги на дії чи бездіяльність працівників поліції та повідомлення про правопорушення);

8) *ІП «102»* – автоматизована підсистема прийому повідомлень «102» за допомогою телекомунікаційних мереж. Забезпечує прийняття, фіксацію, оброблення та реєстрацію повідомлень про правопорушення та інші події, передачу інформації про них відповідним оперативно-диспетчерським службам для організації реагування на такі повідомлення. Функціонування підсистеми регламентовано Інструкцією (п. 1.4.3.2);

9) *ІП «Цунамі»* – автоматизована підсистема централізованого управління нарядами поліції. Забезпечує управління силами й засобами органів та підрозділів поліції для реагування на повідомлення про правопорушення та інші події. Підсистема забезпечує інтеграцію прийнятих формалізованих повідомлень про правопорушення та інші події, інформацію про наявні сили поліції для здійснення реагування та їх статуси, їх взаємної геоінформаційної прив’язки, обміну інформацією з мобільними терміналами, що використовуються патрулями та іншими силами, інтерфейсів, аналітичних засобів для прийняття ефективних управлінських рішень диспетчерською службою. Функціонування підсистеми регламентовано Інструкцією (п. 1.4.3.9);

10) *Програмний модуль інтеграційної платформи ІПНП* для взаємодії інформаційних підсистем Національної поліції з регіональними сегментами систем забезпечення публічної безпеки і порядку (в рамках реалізації проектів «Безпечне місто»), інформаційними підсистемами та реєстрами інших ЦОВВ, у тому числі для здійснення розшуку осіб, транспортних засобів, забезпечення безпеки дорожнього руху та відеоаналізу інформації;

11) *Підсистема картографічної інформації* – програмні компоненти геоінформаційних підсистем, що необхідні для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об’єкта залежно від зміни його характеристик, масштабу та деталізації картографічної інформації для відображення даних;

12) *ІП «ДТП»* – автоматизований облік відомостей про дорожньо-транспортні пригоди, у тому числі фото-відеозображення з місця події, фіксування координат події на карті регіону (країни);

13) *ІП «Дозвіл БДР»* – автоматизований облік відомостей щодо дозволів на рух окремих категорій транспортних засобів, у тому числі небезпечних та негабаритних вантажів. Особливістю ІП є сервіси друку паперового вигляду дозвільного документа та перевірки оригінальності дозвільного документа за допомогою QR-коду із застосуванням будь-якого пристрою з функцією розпізнавання цього коду. Функціонування підсистеми регламентовано Правилами (п.1.4.3.17);

14) *ІП «ITT-Custody records»* – автоматизована підсистема, що забезпечує відстеження порядку тримання осіб в ізоляторах тимчасового тримання головних управлінь Національної поліції (ІТТ) для здійснення оперативного реагування на випадки порушення їх прав і законних інтересів, протиправних дій працівників поліції стосовно них, а також формування та ведення статистичних даних. Підсистема створюється відповідно до Меморандуму (п. 1.4.4);

15) *Сегмент порталу взаємодії з ресурсами в мережі Інтернет* – програмний комплекс, що забезпечує підтримку мобільних додатків, призначених для інформування підрозділів поліції про правопорушення та події, поліпшення комунікації між органами поліції і громадськістю.

Розвиток програмного комплексу необхідно здійснювати на основі експериментального проекту мобільного додатку «Моя поліція» (здійснює опрацювання повідомлень та звернень громадян, які надійшли із застосуванням технологій для мобільних телефонних пристроїв (смартфонів).

За допомогою мобільного додатку передбачено опрацювання наступних основних функціональних можливостей:

– кнопка «SOS» використовується для відправлення екстреного виклику на спецлінію «102»;

– повідомлення про правопорушення (у тому числі з фото-, відео- та аудіофайлами);

– push-сповіщення – отримання користувачами важливої інформації від поліції (у тому числі про надзвичайні новини, орієнтування, перекриття руху під час проведення масових заходів тощо);

– «активний свідок» – дозволяє швидко знаходити свідків правопорушення, використовуючи потенціал мобільних платформ;

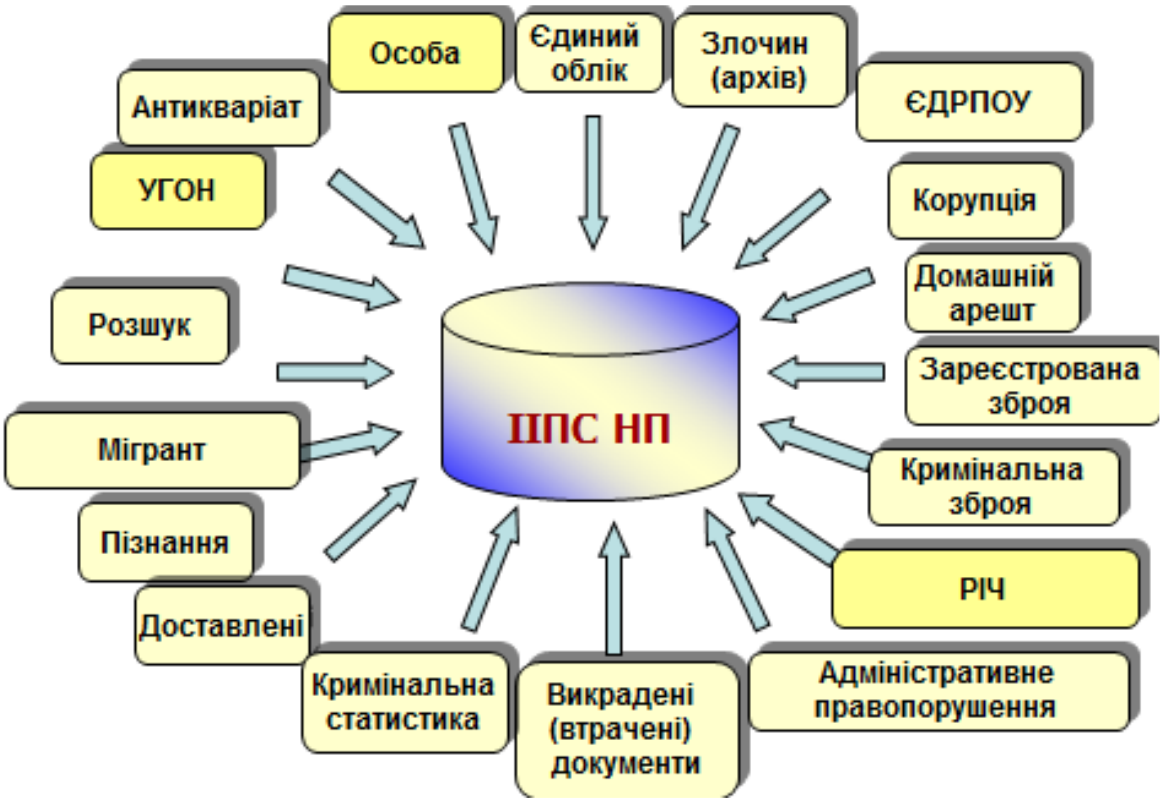
– карта відділень поліції та медичних закладів – можливість відшукати найближче відділення, куди можна звернутися за допомогою;

– інструкція спілкування з поліцейськими – як правильно діяти у тій чи іншій ситуації, а також як мають поводитися поліцейські;

– моніторинг роботи поліцейських – користувачі програми мають змогу оцінити роботу поліцейського за п’ятибальною шкалою, а також залишити анонімний відгук;

– актуальні новини поліції – можливість користувачів ознайомитися з новинами поліції.

Інтегрована інформаційно-пошукова система Національної поліції складається з наступних інформаційних підсистем (мал. 1)



Мал. 1. Інтегрована інформаційно-пошукова система Національної поліції

5. Правила ведення радіоефіру під час патрулювання. Відеофіксація з допомогою персонального відеореєстратора під час патрулювання. Правила ведення радіообміну (радіоефіру) під час патрулювання поліцейськими є важливою складовою ефективної комунікації та координації дій між патрулями і диспетчерськими службами. Дотримання цих правил дозволяє уникнути непорозумінь, зменшити час реагування на інциденти та підвищити безпеку правоохоронців.

Основні правила ведення радіоефіру під час патрулювання:

Короткість і чіткість повідомлень:

Повідомлення повинні бути короткими, інформативними і конкретними, без зайвих деталей.

Необхідно уникати розмов, що не стосуються службових завдань, щоб не перевантажувати радіоканал.

Структура повідомлення

Повідомлення повинно мати чітку структуру: адресат, передача інформації та завершення.

Спочатку називається позивний патрульного або наряду, який передає повідомлення, потім зазначається суть події чи запиту.

Позивні:

Використання позивних є обов’язковим для ідентифікації підрозділів або окремих патрулів. Використання реальних імен під час радіообміну не допускається.

Диспетчер і патрульні мають чітко знати позивні один одного для уникнення плутанини.

Дотримання черговості:

У радіоефірі важливо дотримуватися черговості передачі повідомлень і не перебивати інших учасників, якщо вони вже ведуть радіообмін.

Перед передачею повідомлення необхідно переконатися, що радіоефір вільний.

Заборона використання некоректних або нецензурних висловів:

У радіообміні суворо забороняється використання нецензурної лексики або будь-яких слів чи фраз, які можуть ввести в оману.

Використання кодів і спеціальних термінів:

Поліцейські під час радіообміну використовують службові коди та спеціальні терміни для скорочення часу передачі інформації та забезпечення конфіденційності.

Наприклад, використовуються коди для позначення типів правопорушень, місцезнаходження або статусу патруля ("10-4" — підтвердження отримання повідомлення, "10-20" — місцезнаходження і т. д.).

Використання фраз для підтвердження отримання інформації:

Для підтвердження отримання повідомлення використовується стандартна фраза "Прийняв" або кодове "10-4".

У разі нерозуміння повідомлення варто перепитати за допомогою фрази "Повторіть".

Оперативне інформування про зміну ситуації:

Поліцейські повинні одразу повідомляти диспетчера про будь-які зміни в ситуації на місці події (наприклад, зміна місцезнаходження, зміна характеру інциденту).

Безпека передачі даних:

Передавати конфіденційну інформацію по відкритому радіоканалу слід обережно або через зашифровані канали, щоб уникнути її перехоплення сторонніми особами.

Закінчення радіообміну:

Після завершення радіообміну варто вживати стандартні фрази, наприклад, "Кінець зв’язку" або "На зв’язку", що означає готовність до подальшого обміну інформацією.

Дотримання цих правил допомагає забезпечити оперативну і чітку координацію дій під час патрулювання, що сприяє підвищенню ефективності поліцейських операцій і безпеки як самих правоохоронців, так і громадян.

Відеофіксація за допомогою персонального відеореєстратора під час патрулювання є важливим інструментом для забезпечення прозорості, дотримання законності та безпеки як поліцейських, так і громадян. Персональні відеореєстратори (також відомі як боді-камери) дозволяють документувати дії поліцейських у реальному часі та фіксувати всі взаємодії з громадянами під час виконання службових обов’язків.

Основні принципи використання персональних відеореєстраторів:

1. **Обов'язковість носіння**:
   - Під час патрулювання поліцейські зобов’язані носити персональні відеореєстратори на видимій частині форми (зазвичай на грудях), щоб камера могла охоплювати повне поле зору.
2. **Активація відеозапису**:
   - Поліцейські повинні вмикати відеореєстратор перед початком взаємодії з громадянами, зокрема під час затримання, перевірки документів, проведення операцій чи реагування на інциденти.
   - У деяких ситуаціях (наприклад, коли діяти потрібно негайно) відеозапис може починатися автоматично завдяки передбаченим функціям відеореєстратора.
3. **Інформування громадян**:
   - Поліцейські повинні повідомляти громадян про ведення відеозапису, щоб забезпечити прозорість взаємодії.
   - Винятки становлять випадки, коли інформування про відеозапис може негативно вплинути на безпеку чи оперативність дій.
4. **Безперервність запису**:
   - Після початку запису поліцейські не мають права вимикати відеореєстратор до завершення події або взаємодії, якщо тільки це не суперечить службовим вимогам або законодавству.
   - Вимкнення камери до завершення дії або інциденту допускається лише за певних умов (наприклад, з метою захисту конфіденційності або безпеки).
5. **Заборона редагування або видалення записів**:
   - Поліцейські не мають права редагувати або видаляти записи з відеореєстратора. Всі записи повинні зберігатися в оригінальному вигляді для подальшого аналізу або використання як доказу.
6. **Збереження і доступ до записів**:
   - Всі відеозаписи повинні автоматично завантажуватися в захищені сховища даних після завершення зміни. Термін зберігання записів залежить від характеру інциденту (звичайний запис може зберігатися короткий час, тоді як записи, пов'язані з правопорушеннями або скаргами, можуть зберігатися довше).
   - Доступ до відеозаписів регламентується законодавством. Їх можуть переглядати лише уповноважені особи або використовувати у судових процесах.
7. **Використання записів як доказу**:
   - Відеозаписи з персональних відеореєстраторів можуть використовуватися як докази у кримінальних чи адміністративних справах, що підвищує об’єктивність розгляду ситуацій.
8. **Захист конфіденційності**:
   - Поліцейські повинні враховувати питання конфіденційності, особливо коли відеофіксація ведеться у приватних місцях або стосується неповнолітніх осіб, свідків або потерпілих.

Переваги використання відеореєстраторів:

- **Прозорість**: Громадяни можуть бути впевнені, що дії поліцейських фіксуються, що зменшує ризики неналежної поведінки з обох сторін.
- **Захист прав поліцейських**: У випадках конфліктних ситуацій або скарг на дії поліцейських відеозапис допомагає відновити об’єктивну картину подій.
- **Документування доказів**: Записи можуть слугувати цінними доказами для суду та розслідувань, сприяючи більш справедливому розгляду справ.
- **Підвищення довіри громадян**: Використання персональних камер сприяє покращенню довіри до роботи поліції та їхньої готовності діяти згідно із законом.

Персональні відеореєстратори є ефективним інструментом для підвищення прозорості, зменшення конфліктних ситуацій і забезпечення безпеки всіх учасників взаємодії під час патрулювання