Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

О. В. Бочковий, Г. О. Блінова,
С. О. Прокопов, Є. А. Мамедова

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПАТРУЛЬНОЇ ПОЛІЦІЇ

Методичні рекомендації

Дніпро
2020

УДК 342.95
І-74

Рекомендовано до друку науково-методичною радою Дніпропетровського державного університету внутрішніх справ (протокол № 4 від 17.12.2020)

КОЛЕКТИВ АВТОРІВ:

Олексій Бочковий – завідувач навчально-наукової лабораторії з дослідження проблем превентивної діяльності факультету підготовки фахівців для підрозділів превентивної діяльності Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, старший науковий співробітник, майор поліції;

Ганна Блінова – професор кафедри адміністративного права, процесу та адміністративної діяльності факультету підготовки фахівців для підрозділів превентивної діяльності Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, доцент;

Сергій Прокопов – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ;

Ельміра Мамедова – ад'юнкт кафедри адміністративного права, процесу та адміністративної діяльності факультету підготовки фахівців для підрозділів превентивної діяльності Дніпропетровського державного університету внутрішніх справ.

РЕЦЕНЗЕНТИ:

Євген ЛЕГЕЗА – професор кафедри адміністративного та митного права Університет митної справи та фінансів, д.ю.н., професор;

Ігор ВОЙТУШЕНКО – інспектор тактико-оперативного реагування Управляння патрульной поліції в Дніпропетровській області.

І-74 **Інформаційне забезпечення діяльності патрульної поліції** : метод. рекомендації / О. В. Бочковий, Г. О. Блінова, С. О. Прокопов, Е. А. Мамедова. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2020. 104 с.

Висвітлено правові, організаційні, тактичні, технічні засади використання в роботі патрульної поліції засобів інформаційного забезпечення, технічних приладів, що мають функції фото- та кінозйомки, відеозапису, інформаційні системи та підсистеми, бази даних, автоматизовані робочі місця. Відображено деякі аспекти досвіду використання засобів інформаційного забезпечення та технічних приладів в роботі патрульних поліцейських, проблеми, що виникають в цьому процесі та шляхи їх вирішення

Призначено для використання працівниками підрозділів патрульної поліції, науково-педагогічними працівниками та здобувачами вищої освіти.

ЗМІСТ

СПИСОК СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце
ГРПП – група реагування патрульної поліції
ГУНП – Головне управління Національної поліції
ЄРДР – Єдиний реєстр досудових розслідувань
ІПНП – Інформаційний портал Національної поліції
КК України – Кримінальний кодекс України
КПК України – Кримінальний процесуальний кодекс України
КУпАП – Кодекс України про адміністративні правопорушення
МВС України – Міністерство внутрішніх справ України
СРПП – сектор реагування патрульної поліції
ст.– стаття

Передмова

Практика використання засобів інформаційного забезпечення працівниками поліції свідчить про складності організаційного, правового та технічного характеру, що супроводжують цей процес. Внаслідок реалізації ризиків зниження рівня інформаційного забезпечення, інформаційної безпеки та кібербезпеки підрозділів та працівників Національної поліції значно знижується їх ефективність.

Стратегія розвитку Міністерства внутрішніх справ України до 2020 року визначила, що недоліками у сфері інформаційного забезпечення підрозділів поліції є застарілі підходи до управління інформаційними ресурсами органів системи МВС, недостатній рівень використання ними інформаційно-комунікаційних технологій; відсутність системного вирішення проблеми авторизованого доступу користувачів, еталонної консолідації, перевірки актуальності і достовірності даних інформаційних ресурсів системи МВС; ступінь інтеграції в міжнародний інформаційний простір у сфері безпеки не відповідає сучасним викликам, які стоять перед системою МВС. Цією стратегією передбачено, що роль Міністерства внутрішніх справ України полягає у створенні умов розвитку безпечного середовища життєдіяльності, як основи безпеки на території України, а також сучасної системи внутрішньої безпеки. Цим документом приділяється значна увага у напрямку підвищенню ефективності роботи і взаємодії підрозділів поліції через максимальне використання інформаційно-комунікаційних технологій у реалізації завдань органами системи МВС. Основними кроками для реалізації цього завдання стратегія визначає : реалізацію концепції діяльності органів системи МВС, заснованої на використанні різних джерел інформації (Intelligence Led Policing); запровадження в системі МВС механізму приведення інформації про особу, що міститься у наявних державних та єдиних реєстрах, інших інформаційних базах, що перебувають у власності держави або підприємств, установ та організацій, та використовуються з метою проведення ідентифікації осіб, до єдиного ідентифікатора – унікального номеру запису в Єдиному державному демографічному реєстрі; об'єднання і захист відомчих інформаційних ресурсів органів системи МВС у рамках єдиного інтегрованого інформаційного середовища; упровадження сучасного авторизованого доступу користувачів до інформаційних ресурсів системи МВС та надання громадянам доступу до відкритих даних органів системи МВС і власних персональних даних; підгото-

вка належних інформаційних систем МВС до приєднання до Шенгенської інформаційної системи; розширення та оновлення знань, умінь та навичок працівників у роботі з відомчими інформаційними системами. Таким чином питання інформаційного забезпечення та кібербезпеки Національної поліції України мають стратегічне значення для ефективної діяльності Міністерства внутрішніх справ України.

Теоретична невизначеність понять інформаційного забезпечення та кібербезпеки, низький рівень моніторингу стану інформаційного забезпечення патрульної поліції, проблем, що виникають при використанні засобів відео та фото фіксації, планшетних пристроїв, програмного забезпечення, недоліків чинного законодавства у цій сфері діяльності Національної поліції загалом, та патрульної поліції, зокрема, є причинами визначених у Стратегії розвитку Міністерства внутрішніх справ України до 2020 року недоліків у сфері інформаційного забезпечення підрозділів поліції.

1. Загальні засади інформаційного забезпечення діяльності патрульної поліції

В останні роки Україна неодноразово стикалася з актуалізацією загроз інформаційній безпеці органів публічної влади. Серед них недавнє поширення шкідливого програмного забезпечення Petya, вимагача WannaCry, атаки 2015-2016 років на енергетичний сектор, атака на президентські вибори у 2014 році, різні інциденти, пов'язані з інформаційними системами та мережами державних органів і держкомпаній у 2016 році, інциденти, пов'язані з Євромайданом у 2013-2014 роках, а також низка профільних кіберзлочинів. Інший напрям негативного зовнішнього інформаційного впливу, що здійснюється із використанням новітніх інформаційних технологій, це зміна свідомості громадян, спрямована на розпалювання міжнаціональної та релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу або будь-яке порушення суверенітету, територіальної цілісності України, громадського порядку та безпеки. Загрози можуть бути різної природи, результатом дій різних суб'єктів, що мають великий спектр мотивів. Вони можуть бути націлені на багато об'єктів, мати різну величину, атакувати велике коло жертв і приносити безліч шкідливих наслідків. Відповідно, потрібен ефективний алгоритм оцінки якості кожної загрози, що визначатиме поєднання заходів і можливостей різних правоохоронних структур для протидії ним.

Дослідженням питань інформаційного забезпечення, інформаційної безпеки та кібербезпеки суб’єктів публічної влади та правоохоронних органів, опікувались такі вчені як Є.Д. Бондаренко, В.В. Бухарев, В.О. Єльцов, Д.П. Кисленко, В.В. Лушер, Г.М. Шорохова та інші. Проте на сьогодні відсутня сучасна концепція кібербезпеки Національної поліції загалом та патрульної поліції зокрема.

Проблема реалізації кіберзагроз та негативного зовнішнього інформаційного впливу характерна не тільки для України [19]. Європейський парламент для протидії таким негативним сучасним викликам прийняв ряд документів, серед яких Резолюція «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» [69; 26], Директива Європейського Парламенту і Ради «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» [52], Регламент Європейського парламенту і Ради «Про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» [70] та інші. Своєю чергою Україна створила такі нормативно правові документи як страте-

гії, доктрини, програми, які спрямована на визначення національних інтересів України в інформаційному просторі, ідентифікацію загроз їх реалізації, напрямів й пріоритетів державної політики в інформаційному просторі.

Документами, що місять принципи формування та реалізації державної інформаційної політики, у тому числі, пов'язаних з протидією деструктивному зовнішньому інформаційному впливу є Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та плану заходів щодо її реалізації, затверджені Розпорядженнями Кабінету Міністрів України від 20.09.2017 № 649-р , від 8 листопада 2017 р. № 797-р та від 17 січня 2018 р. № 67-р. [58], а також Укази Президента України від 14.09.2020 р. № 392/2020 «Про Стратегію національної безпеки України» [56]; від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [57] та інші.

Основними пріоритетами державної політики в інформаційній сфері згідно зазначених документів є законодавче регулювання механізму пошуку, фіксації, блокування і видалення з інформаційного простору держави, зокрема, з українського сегмента мережі Інтернет, інформації, яка загрожує життю або здоров'ю громадян України, розпалює війну, міжнаціональну і релігійну ворожнечу, пропагує зміну конституційного ладу або порушення територіальної цілісності Україна, загрожує державному суверенітету і просуває комуністичні і / або націонал-соціалістичні (нацистські) тоталітарні режими і їх символи, а також створення інтегрованої інформаційної системи оцінки загроз та швидкого реагування на них.

Зазначені обставини вплинули на умови функціонування правоохоронних органів. Слід погодитись із Г.М. Шорохом, що на сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційної підтримки та інформаційного забезпечення, накопичення та систематизації інформації в базах даних [68, с. 246].

При дослідженні різних наукових позицій щодо змісту та ознак інформаційного забезпечення органів публічної адміністрації ми підтримуємо концепцію широкого підходу до розуміння цього поняття, що обумовлено сучасними тенденціями глобалізації та постійного прискорення розвитку електронних ресурсів. Прихильниками цього підходу є такі науковці як Є.Д. Бондаренко, В.О. Єльцов, О.В. Костенко, В.В. Лушер та інші. За їх концепціями інформаційне забезпечення можна визначити як: 1) це процес задоволення потреб в інформації, заснованої на застосуванні спеціальних засобів і методів її одержання, опрацюванні, накопиченні і видачі в зручному для використання виді, а структура

цього забезпечення включає інформаційний фонд та спеціальні прийоми і методи інформаційного забезпечення [4]; 2) представляє собою сукупність організаційної діяльності з одержання, опрацювання, накопичення і видачі інформації, прийомів та методів її здійснення, а також матеріальних об'єктів – інформаційний фонд [4]; 3) сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки [15, с. 101]; 4) комплекс нормативно-правових, організаційно-управлінських, науково-технічних та інших заходів поєднання усієї інформації, що використовується в органах прокуратури, специфічних засобів і методів її оброблення, використання, дослідження, зберігання та захисту [24, с. 340].

О.В. Костенко детальніше визначила ознаки, притаманні інформаційному забезпеченню, врахувавши його зміст, методи реалізації, мету, призначення, та віднесла до них: 1) його зміст складають: певна сукупність усієї інформації; сукупність реалізованих рішень щодо обсягів інформації, її якісного та кількісного складу, розміщення і форм організації; сукупність дій з надання необхідної для управлінської діяльності інформації в зазначене місце на основі певних процедур із заданою періодичністю; діяльність, що пов'язана із засобами збирання, реєстрації, передачі, зберігання, опрацювання та представлення інформації; оперативна система одержання, зберігання та обробки інформації; процес забезпечення інформацією, формування нормативної бази, розміщення інформації, яка використовується в інформаційній системі; діяльність (сукупність певних дій, управлінських рішень); 2) реалізується певними способами та методами; 3) охоплює надходження, рух та перетворення інформації, методи її зберігання та передавання; 4) спрямоване на збирання, реєстрацію, передачу, зберігання, опрацювання, аналіз, поширення та обробку інформації; 5) призначене для використання фахівцями; для відображення інформації, що характеризує стан керованого об'єкта і є основою для ухвалення управлінських рішень; 6) мета – своєчасне надання необхідної і достатньої інформації для розроблення та прийняття рішень [21, с. 116].

У попередніх роботах ми визначили ознаки поняття «інформаційне забезпечення»: 1) мета – задоволення інформаційних потреб та забезпечення реалізації інформаційних прав; 2) ресурс – інформація, вид, якість, обсяг, структура, форма, строк та носії використання якої визна-

чаються інформаційними потребами та правами суб'єкта; 3) зміст – неперервний процес, що складається з різних видів інформаційної діяльності; 4) методи – створення, використання, дослідження, зберігання, захист, передавання, обробка, знищення інформації; 5) засоби – інформаційні системи, мережі, ресурси та інформаційні технології, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки; 6) заходи із реалізації інформаційного забезпечення – комплекс нормативно-правових, організаційно-управлінських, науково-технічних та інших заходів; 7) суб'єкт – фізичні та юридичні особи та їх об'єднання [2, с. 18-19]. З урахуванням зазначено нами було запропоновано визначити інформаційне забезпечення органів публічної адміністрації як забезпечений комплексом нормативно-правових, організаційно-управлінських, науково-технічних заходів неперервний процес створення, використання, дослідження, зберігання, захисту, передавання, обробки, знищення інформації визначеного виду, якості, обсягу, структури, форми, за допомогою інформаційних систем, мереж, ресурсів та технологій, спрямований на задоволення інформаційних потреб і реалізацію інформаційних інтересів органів публічної адміністрації [1, с. 30]. На наш погляд, це поняття може бути покладене в основу формулювання поняття інформаційного забезпечення Національної поліції загалом, та патрульної поліції, зокрема. Особливості змісту інформаційного забезпечення патрульної поліції визначатимуть її інформаційні потреби обумовлені колом повноважень.

Згідно Положення про Департамент патрульної поліції, цей міжрегіональний територіальний орган Національної поліції у інформаційній сфері виконує такі функції: 1) у межах інформаційно-аналітичної діяльності патрульної поліції, формує бази (банки) даних, що входять до єдиної інформаційної системи Національної поліції України та Міністерства внутрішніх справ України, користується базами (банками) даних Національної поліції України, Міністерства внутрішніх справ України та інших державних органів, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, а також обробку персональних даних у межах повноважень визначених законом; 2) здійснює інформаційну взаємодію з іншими державними органами України, органами правопорядку іноземних держав та міжнародними організаціями [47]; 3) для забезпечення публічної безпеки та порядку, попередження, виявлення або фіксування правопорушення, охорони власності, забезпечення безпеки осіб, а також забезпечення дотримання правил дорожнього руху застосовує технічні прилади та технічні засоби, що мають функції фото та кінозйомки, відеозапису, чи засоби фото- і кінозйомки, відеозапису; 4) інформує в порядку та у спосіб, які передбачені законодавством, ор-

гани державної влади, органи місцевого самоврядування, а також громадськість про здійснення державної політики у сферах забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, безпеки дорожнього руху; 5) керівництво департаменту здійснює постійний контроль за збереженням інформації з обмеженим доступом, збереженням державної таємниці та дотриманням режиму секретності в Департаменті патрульної поліції. На наш погляд, визначені у цьому наказі засади інформаційного забезпечення та кібербезпеки патрульної поліції є неповними, їх слід сприймати із врахуванням норм Закону України «Про Національну поліції» [53], що ґрунтовніше визначають елементи механізму інформаційного забезпечення підрозділів Національної поліції та поширюються на патрульну поліцію.

З урахуванням зазначеного підтримуємо позицію Г.М. Шорохової, який інформаційне забезпечення органів поліції визначає як комплекс методів, заходів, засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій, а також їх ефективне використання для вирішення покладених на поліцію завдань [68].

З інформаційним забезпеченням патрульної поліції тісно пов'язані питання кібербезпеки. При чому найчастіше науковці досліджують повноваження Національної поліції як суб'єкта забезпечення кібербезпеки держави, суспільства, різних спільнот та окремих громадян. Так, у галузі забезпечення кібербезпеки, вважає В.В. Бухарев, Нацональна поліція України наділена повноваженнями щодо забезпечення прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі [53]. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», МВС було включено до національної системи суб'єктів забезпечення кібербезпеки. У зв'язку з цим, на МВС було покладено повноваження щодо: створення і забезпечення функціонування підрозділів з протидії кіберзлочинності; розробки та реалізації комплексу організаційних і практичних заходів, спрямованих наборотьбу з кіберзлочинами; створення і забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги у розслідуванні кіберзлочинів, тощо [53]. В положеннях Закону «Про основи забезпечення кібербезпеки України» МВС віднесено до загальних суб'єктів забезпечення інституту [5]. Водночас науковці не достатньо приділяють уваги визначенню змісту поняття кібербепека поліції, якого наразі не сформульовано.

Відсутність достатньої уваги до питань організаційно-правового забезпечення кібербезпеки патрульної поліції призводить до реалізації

загруз у цій сфері. Одна з останніх таких кібератак сталася 23 вересня 2020 року, коли на деяких інтернет-сторінках обласних управлінь Національної поліції була поширена неправдива інформація, повідомлялося про викид радіоактивних речовин на 3-му енергоблоці Рівненської АЕС [27]. На той момент сайт Національної поліції та відповідно інтернет-сайти інших головних управлінь поліції були відключені. Своєю чергою Департамент патрульної поліції був змушений відключити базу ІІПС «Армор», що не давало можливості патрульний поліцейським здійснювати перевірку осіб, транспортних засобів, також виносити електронні постанови правопорушникам. На той момент виклику на спеціальну лінію «102» приймалися і передавалися до чергової частини, в свою чергу чергова частина патрульної поліції також виявилася без зв'язку. Не бачивши на моніторі карти знаходження патрулів, черговий був змушений відправляти будь-якого й орієнтуватися тільки на квадрат прив'язки патруля, в якому екіпажу не завжди виходить знаходиться. Виклику спецлінії «102» оголошувалися по радіозв'язку, яка як ми знаємо не є захищеною, також в телефонному режим. Черговий не бачив рапорту про виконану роботу на виклик і час завершення виклику, щоб направити екіпаж за наступною адресою. Це призвело до черги не обслугованих викликів, громадяни не отримали ту допомогу, котру потребували в ту хвилину.

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення кібербезпеки — це є захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [54]. Кібербезпеку як об’єкт адміністративно-правової охорони В.В. Бухарєв визначає як певний правовий інститут, охорона якого відбувається в межах норм адміністративного права та здійснюється окремими державними органами на засадах імперативності та ієрархічності. Цей науковець визначає наступні особливості кібербезпеки як об’єкта адміністративно-правової охорони: а) відсутність чіткого визначення змісту адміністративно-правової охорони кібербезпеки; б) адміністративно-правова охорона кібербезпеки хоча і являє собою єдиний юридичний інститут, проте закріплюється у нормах різних нормативно-правових актів, якими регулюється діяльність відповідних органів державної влади; в) її забезпечення здійснюється не тільки у правовідносинах, які виникають у сфері вчинення адміністративних правопорушень. Інститут має більш широкий обсяг застосування, який передбачає не тільки припинення ві-

дповідних порушень, а також їх попередження; г) основні засади забезпечення кібербезпеки лише нещодавно знайшли своє закріплення у відповідному нормативно-правовому акті – Законі України «Про основні засади забезпечення кібербезпеки України»; ґ) має місце спеціальний понятійний апарат [5, с. 94]. Науковий стан вивчення змісту поняття кібербезпека патрульної поліції не дозволяє дослідити сформульовані відповідні поняття через їх відсутність. Водночас поняття кібербезпеки тісно пов'язано із поняттям інформаційної безпеки, оскільки є похідним від останнього.

У наших попередніх роботах було сформульовано поняття інформаційної безпеки органів внутрішніх справ України як такий стан захищеності службових інтересів, за якого зводиться до мінімуму заподіяння шкоди та створення перешкод у діяльності органів внутрішніх справ через неповноту, несвоєчасність, недостовірність інформації, що використовується, або протиправний інформаційний вплив, недоліки функціонування інформаційних систем, мереж, технологій, а також через порушення режиму службової таємниці [66, с. 15]. Основними елементами інформаційної безпеки ОВС визначено: 1) інформаційне середовище ОВС України, 2) інтереси МВС України та ОВС України в інформаційній сфері, 3) об'єкти інформаційної безпеки ОВС України, 4) суб'єкти, що забезпечують інформаційну безпеку ОВС України, 5) концепція інформаційної безпеки ОВС України, 6) загрози інформаційній безпеці ОВС України, 7) принципи забезпечення інформаційної безпеки ОВС України, 8) форми і способи забезпечення інформаційної безпеки ОВС України. Важливим для визначення місця інформаційної безпеки патрульної поліції в системі інформаційної безпеки органів внутрішніх справ є визначені нами рівні: 1) інформаційна безпека Міністерства внутрішніх справ як інформаційна безпека центрального органу виконавчої влади; 2) інформаційна безпека підрозділу органів внутрішніх справ України як різновид інформаційної безпеки установи; 3) інформаційна безпека працівника органів внутрішніх справ України як вид інформаційної безпеки людини [67, с. 69]. Таким чином кібербезпеку патрульної поліції можна розглядати як безпеку служби, кібербезпеку Департаменту патрульної поліції як кібербезпеку установи, а кібербезпеку патрульного поліцейського як вид кібербезпеки людини.

Інші науковці, наприклад В. А. Веклич та Д. П. Кисленко визначили Інформаційну безпеку поліції охорони як захист інформаційної сфери поліції охорони від внутрішніх та зовнішніх загроз. На їх думку Інформаційна безпека поліції охорони полягає у спроможності працівників поліції охорони убезпечити інформаційні ресурси від несанкціонованого доступу до них, та унеможливити витоки службової інформа-

ції Забезпечення інформаційної безпеки в діяльності поліції охорони здійснюється через: організаційно-аналітичне управління; управління технічної охорони; відділ правового забезпечення; режимно-секретний сектор Департаменту поліції охорони – структурні служби Департаменту поліції охорони, які забезпечують правове та організаційно-технічне забезпечення інформаційної безпеки в діяльності поліції охорони. Поліція охорони Національної поліції України, зазначають В. А. Веклич та Д.П. Кисленко є складовою частиною системи інформаційної безпеки. Забезпечення інформаційної безпеки поліції охорони здійснюється відповідно до встановлених законом повноважень та спрямоване на своєчасне виявлення, запобігання та припинення загроз в її інформаційному просторі [6, с. 59].

Поліція в рамках інформаційно-аналітичної діяльності формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України [53]. Єдина інформаційна система Міністерства внутрішніх справ - багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супроводження їх діяльності і становить сукупність взаємозв'язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію. Перелік пріоритетних інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ України включає: Єдиний державний реєстр транспортних засобів, Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху та інші. Функціональними підсистемами єдиної інформаційної системи МВС є: національна система біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства; інформаційний портал Національної поліції України; Єдиний державний реєстр транспортних засобів; Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху; система фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі; система екстреної допомоги населенню за єдиним телефонним номером 112; інтегрована міжвідомча інформаційно-телекомунікаційна система щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон; інформаційно-телекомунікаційна система прикордонного контролю «Гарт-1»; інші системи, реєстри та бази (банки) даних, створені суб'єктами єдиної інформаційної системи МВС в межах реалізації владних повноважень. Суб'єктами єдиної інформаційної системи МВС є апарат МВС та його

територіальні органи з надання сервісних послуг МВС, Національна гвардія, заклади, установи і підприємства, що належать до сфери управління МВС, центральні органи виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ, інші державні органи, які обробляють інформацію в єдиній інформаційній системі МВС для реалізації своїх повноважень. МВС здійснює організаційне забезпечення функціонування єдиної інформаційної системи МВС, а також визначає права і обов'язки персоналу служби та адміністратора єдиної інформаційної системи МВС [48].

Єдиний державний реєстр Міністерства внутрішніх справ стосовно зареєстрованих транспортних засобів та їх власників є частиною єдиної інформаційної системи МВС. Постанова Кабінету Міністрів України від 25 березня 2016 р. № 260 визначає умови та підстави безпосереднього доступу посадових осіб органів державної влади, зокрема органів МВС, органів Національної поліції, органів місцевого самоврядування, судів, органів прокуратури, органів СБУ, адвокатів, нотаріусів, інспекторів з паркування (користувачі) до Єдиного державного реєстру транспортних засобів, держателем якого є Міністерство внутрішніх справ, щодо зареєстрованих транспортних засобів, їх власників та належних користувачів у зв'язку із здійсненням ними повноважень, визначених законом, а також механізм користування Реєстром. Доступ до Реєстру надається (припиняється) користувачеві на підставі договору, укладеного між ним та адміністратором Реєстру, і за документами, які надають користувачеві право на отримання такої інформації у зв'язку із здійсненням ним повноважень, визначених законом. У разі коли користувачем є посадова особа органу державної влади або органу місцевого самоврядування, договір укладається між органом, в якому працює такий користувач, та адміністратором Реєстру [11]. Особливий механізм надання Міністерством внутрішніх справ України інформації з Єдиного державного реєстру про зареєстровані транспортні засоби та їх власників Національному агентству з питань запобігання корупції, необхідної для реалізації ним повноважень та прав, передбачених Законом України «Про запобігання корупції» визначений у Порядку надання Міністерством внутрішніх справ України інформації з Єдиного державного реєстру про зареєстровані транспортні засоби та їх власників Національному агентству з питань запобігання корупції [50].

У навчальному підручнику «інформаційні технології», підготовленого авторським колективом у складі В.Б. Вишні, К.Ю. Ісмайлова, І.В. Краснобрижого, С.О. Прокопова, Е.В. Рижкова подана детальна характеристика складових Інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» [18, с. 15; 63, с. 12;

64, с. 8; 65, с. 10]. Розглянемо ключові їх положення.

З метою організації інформаційно-аналітичної підтримки поліції було розроблено Положення про інформаційно-телекомунікаційна систему «Інформаційний портал Національної поліції України». Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (ІПНП) - сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичної підтримки [49].

Основними завданнями системи «Інформаційний портал Національної поліції України» 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.

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 засоба-

ми 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» [49].

В інформаційних ресурсах системи «Інформаційний портал Національної поліції України» обробляється інформація, яка належить до державних інформаційних ресурсів [49]. 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 [49].

Поліція може створювати інші бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, відповідно

до статті 25 Закону України «Про Національну поліцію» [53].

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 [49]. 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 [49].

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 «Інфор-

маційний 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 [49].

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 [49].

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

Система централізованого управління нарядами поліції «ЦУНАМІ»

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.

Вишня В.Б. зазначає, що відома система управління діяльністю, коли на телефон 102 або номер чергової частини райвідділу поліції надходить виклик про допомогу, або повідомлення про вчинене правопорушення чи злочин. Оператор 102 передає отриману інформацію в чергову частину райвідділу поліції по території обслуговування, де вона реєструється у відповідних журналах тижневих пригод. Після чого на виклик направляється екіпаж мобільного патрульного наряду або, за необхідності, слідча оперативна група (СОГ) [41].

Найбільш вдосконаленим технічним рішенням даної проблеми є ство рення системи централізованого управління нарядами патрульної служби (“ЦУНАМІ”), що являє собою комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами мобільних нарядів поліції. Він включає пов’язані між собою блоки оператора 102, диспетчера, чергового районного відділу поліції та обладнання автопатруля у вигляді блока керування та відображення (у подальшому – планшет) із системою супутникового GPS-позиціонування і особистого відеорегістратора патрульного. Диспетчер системи є оперативним черговим і куратором кожного конкретного райвідділу поліції, відповідального за організацію реагування на злочини та пригоди в рамках району. Оператор 102 здійснює прийняття і реєстрацію повідомлень про злочини та події, виконує попередню їх кваліфікацію. Заповнена оператором 102 електронна картка надходить до диспетчера – чергового відповідального за управління мобільними нарядами поліції, де призначається екіпаж мобільного патруля для реагування на сповіщення, що надійшло. Одночасно електрона картка надходить черговому районного відділу поліції, до території якого відноситься звернення, де повідомлення громадян реєструється у журналі “Єдиного обліку злочинів і правопорушень районного управління” [28; 8, с. 114]. 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.

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 8 тис. викликів на добу;

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

– сумарний потік інформації на один пульт – до 320 звернень за добу [7].

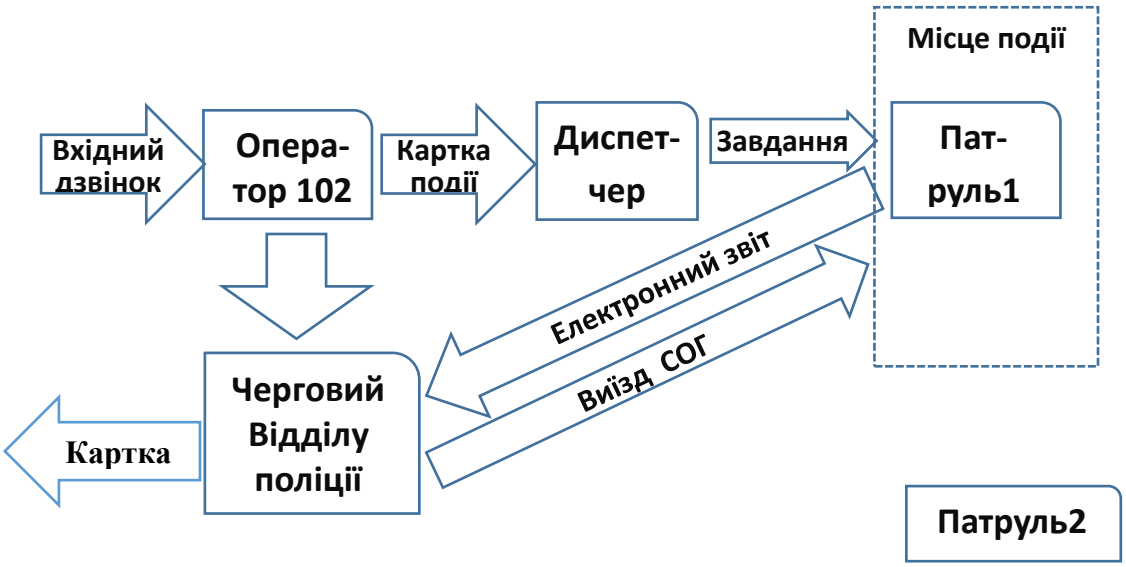


Рис. 1

Як вбачається зі спрощеної схеми, повідомлення отримані оператором служби «102» або черговим районного відділу поліції оперативно надходять в електронному вигляді до чергового-диспетчера, який:

– своєчасно визначає сили реагування (відповідні патрулі) та координує їх роботу;

– оперативно керує роботою патруля (у автоматизованому та голосовому режимі);

– ретельно контролює роботу патруля на маршруті (якість реагування патруля на повідомлення про злочини та правопорушення) [18, с. 16; 63, с. 10; 64, с. 7; 65, с. 11].

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 [18, с. 15; 63, с. 12; 64, с. 8; 65, с. 10].

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) [17].

Створення системи ситуаційних центрів, зазначають автори підручника «Інформаційні технології» 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 2019 році ця цифра перевалила за 9 млн. Свою роль зіграла патрульна поліція. Було створено патрульну поліцію, яка зараз працює в усіх крупних містах України. 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 [18, с. 15; 63, с. 12; 64, с. 8; 65, с. 10].

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" (рис. 2).

Рис. 2

Найважливішим елементом цього середовища є побудова ситуаційних центрів різних рівнів. Залежно від галузі застосування, назва “Ситуаційного центру” може трансформуватися у “центр командування і управління” (command and controlcenter), “кризовий центр” (crisis center), “надзвичайний центр” (emergency center), “залу нарад” (corporate boardroom, conference room). За цього під центром розуміється не лише спеціально обладнане приміщення, але й відповідні інформаційні, телекомунікаційні, програмні та методичні засоби, що забезпечують процес доставки, агрегації інформації з метою вироблення відповідного управлінського рішення [10]. Ситуаційні центри є невід’ємною складовою інформаційної інфраструктури електронного урядування, спрямованої,

насамперед, на підвищення ефективності діяльності органів влади за рахунок оперативного формування більш обґрунтованих управлінських рішень. Ситуаційні центри містять інформаційний простір для ефективного моніторингу, прогнозування, прийняття рішень та контролю їх виконання, що дозволяє реалізувати новий формат управління в умовах жорсткого дефіциту часу та ресурсів, оцінювати можливі стратегічні, політичні, економічні, соціальні, екологічні ризики, які можуть виникати при різних сценаріях управлінських ситуацій. Для мінімізації ризиків використовують довгострокове прогнозування розвитку управлінських (кризових) ситуацій, розробку та моделювання різноманітних сценаріїв їх розвитку. На сьогодні принциповими при прийнятті управлінського рішення є параметри: швидкість реагування на динаміку характеристик та показників стану об'єкта управління; високий ступінь відповідальності за результат управлінського впливу; інформаційна та взаємодія органів влади різного рівня; ефективні комунікації між державними службовцями та посадовими особами органів місцевого самоврядування щодо стану об'єкта управління за допомогою сучасних інформаційно-телекомунікаційних технологій [61]

Основним завданням ситуаційного центру, вважають Ю.Гладун та А. Ліпенцев є забезпечення координації та управління силами і засобами ГУНП, а також в разі ускладнення оперативної обстановки або виникнення надзвичайних ситуацій, організація розгортання оперативного штабу ГУНП з метою взаємодії між іншими органами державної влади та органами місцевого самоврядування [9].

Чергові та аналітики ситуаційних центрів Національної поліції стежать за оперативною обстановкою в країні, щоранку готують доповідь для керівництва: де, скільки і які злочини сталися. Обсяг такої довідки - близько 10 аркушів А4, зведення впродовж доби – це всі вбивства, тяжкі тілесні зі смертельним наслідком, зґвалтування, розбійні напади, масові заходи і події щодо особового складу. Кожну фабулу розбирають окремо й аналізують обставини злочину: що, як сталося, як спрацювала поліція. Це у нас щоранковий аналіз оперативної обстановки. На підставі цієї інформації голова ухвалює рішення – провести додаткові оперативно-розшукові або профілактичні заходи, відправити у відрядження до іншого регіону додаткові сили, посилити охорону публічної безпеки та порядку [18, с. 17; 63, с. 11; 64, с. 9; 65, с. 12].

Крім того, співробітники ситуаційних центрів регіонів стежать за використанням електронних засобів контролю, браслетів, щодо тих громадян, яким було обрано такий запобіжний захід.

Працює ситуаційний центр у двох режимах: стандартному і надзвичайному. Стандартний режим (це коли оперативна обстановка в кра-

їні відносно стабільна, контрольована) - працює чергова частина і кілька аналітиків. Цих сил достатньо, щоб відстежувати обстановку і проводити її якісний аналіз [18, с. 15; 63, с. 12; 64, с. 8; 65, с. 10].

Ситуаційні центри координують роботу затримання особливо небезпечних озброєних злочинців по гарячому сліду. Наприклад, якщо просто розшукується викрадений транспортний засіб, то вводять план "Перехоплення". При введенні в дію оперативних планів саме й включається ситуаційний центр: ввели на території міста, ситуаційний центр вже контролює, як місто перекрито, де виставлено наряди, де і які наряди потрібно виставити додатково. Якщо озброєні злочинці тікають з місця розбою або вбивства, вводять план "Сирена", і тоді вся поліція працює на затримання озброєних злочинців, а ситуаційні центри контролюють, як ці сили і засоби застосовуються. Якщо знають, де злочинці перебувають, і їх потрібно вже затримувати, вводять план "Грім". Тоді вже підключається КОРД, інші спецпідрозділи і затримують цих злочинців [22].

У своїй роботі співробітники ситуаційних центрів використовують дрони, спецавтомобілі із щоглою і відеокамерою, з необхідним обладнанням всередині. Є можливість відстеження відео з камер Києва, їх близько 4 тис., Одеси, Дніпра і Харкова.

У ситуаційних центрах працюють офіцери–аналітики, які використовуючи інформацію з баз даних Національної поліції, інтернету, соціальних мереж, зі ЗМІ, відео потоки з он-лайн камер направляють необхідну кількість патрульних нарядів у місце концентрації злочинів, надають необхідну інформацію іншим підрозділам Нацполіції щодо відпрацювання певної місцевості для розкриття певних злочинів та інше (рис. 3) [18, с. 15; 63, с. 12; 64, с. 8; 65, с. 10].

Рис. 3

В ситуаційних центрах працюють оператори лінії «102», які приймають дзвінки з усієї області. Протягом доби по всій країні до поліції звертаються від 20 до 25 тис. осіб. І весь масив цієї інформації опрацьовується. Одночасно з дзвінком оператору «102» автоматично створюється електронна картка, куди оператор і вносить всі дані і суть звернення громадянина. Далі картка передається (протягом не більше двох хвилин) диспетчеру, який скеровує інформацію наряду патрульної поліції для подальшого реагування. Диспетчер бачить всі наряди онлайн. Останній також контролює час прибуття наряду і результат обслуговування виклику. Якщо повідомлення резонансне, воно моментально з'являється в черговій частині ситуаційного центру, його передають аналітикам і включають до зведення для голови Національної поліції. Зараз служби «102» працюють по всій Україні. Загалом на лінії працюють близько 900 операторів [18, с. 15; 63, с. 12; 64, с. 8; 65, с. 10].

Центр прийняття повідомлень – служба «102» вирішує завдання з прийняття та реєстрації повідомлень про злочини та події на єдиній інформаційній базі. Автоматизація служби «102» ситуаційних центрів Національної поліції дозволила вести облік звернень громадян на первинному рівні та здійснювати оцінку криміногенної ситуації в режимі реального часу.

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 [18, с. 18; 63, с. 13; 64, с. 11; 65, с. 11].

Інформаційна електронна картка «102» (рис. 4).

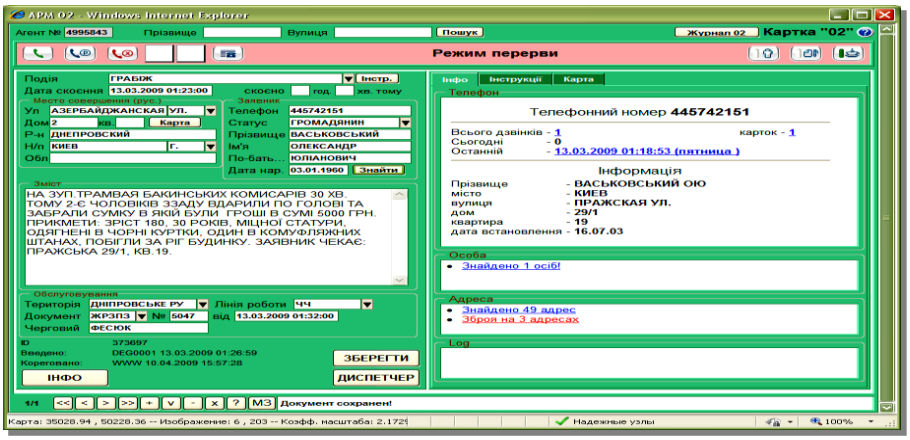
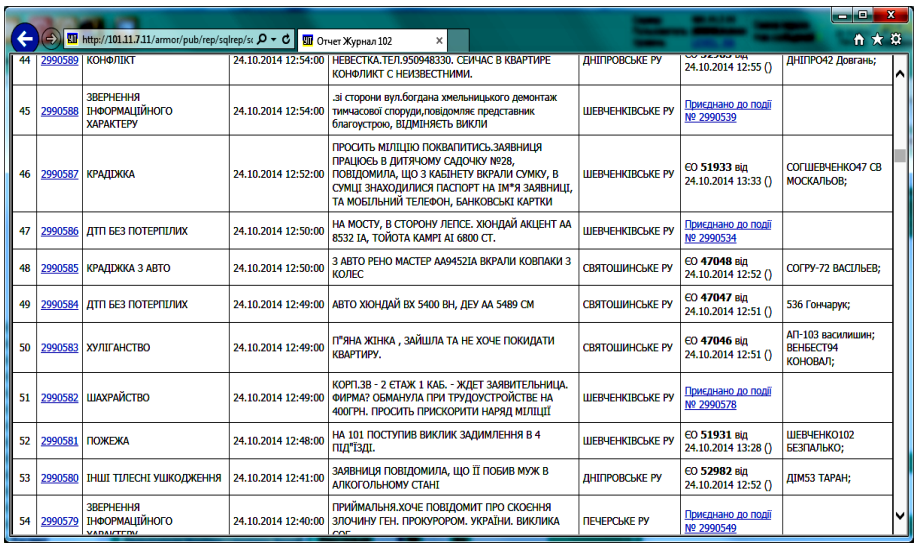


Рис. 4

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 [18, с. 19; 63, с. 13; 64, с. 10; 65, с. 12].

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 (рис. 5) [18, с. 19; 63, с. 13; 64, с. 10; 65, с. 12].



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 ПРАЦЮЄ 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 ХАРАКТЕРУ	24.10.2014 12:40:00	ПРИЙМАЛЬНЯ.ХОЧЕ ПОВІДОМИТ ПРО СКОЄННЯ ЗЛОЧИНУ ГЕН. ПРОКУРОРОМ. УКРАЇНИ. ВИКЛИКА СОГ	ПЕЧЕРСЬКЕ РУ	Приєднано до події № 2990549	

Рис. 5

У столиці України місті Києві до системи «102» підключений сервіс SMS-інформування. Після прийняття оператором служби «102» звернення та його збереження в електронній базі даних до заявника у випадку наявності контактного мобільного номера телефону надходить підтверджувальне SMS-повідомлення про реєстрацію звернення та спеціальний код доступу до спеціалізованого Web-порталу 102kiev.com.ua., де заявник зможе ознайомитись з етапами реагування на своє звернення [18, с. 19; 63, с. 13; 64, с. 10; 65, с. 12].

Онлайн-сервіс 102kiev.com.ua, який є підсистемою системи «ЦУНАМІ», який забезпечується виконання таких функцій:

– прийняття заяв та звернень громадян до поліції міста Києва через спеціалізовану Інтернет-сторінку;

– надання можливості заявникам відслідковувати обробку та ухвалення рішення щодо власного звернення.

В залежності від виду зареєстрованої події система автоматично, в режимі реального часу, інформує керівництво Національної поліції та відповідних працівників про подію за допомогою SMS або Інтернет-повідомлень.

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 наряду та відстеження результатів реагування на заяви та повідомлення громадян про злочини, прийняті рішення тощо [18, с. 19; 63, с. 13; 64, с. 10; 65, с. 12].

Патруль одержує від диспетчера у формі електронного повідомлення основні дані із заяви, у тому числі номер заявника. Після призначення патруля заявник одержує SMS-повідомлення з контактним телефоном чергового-диспетчера, який обслуговує відповідний район. За результатами реагування диспетчер ставить відповідні відмітки. Інформаційна електронна картка (рис. 6) залишається у диспетчера на контролі, поки не буде отриманий повний звіт про результати реагування на звернення.

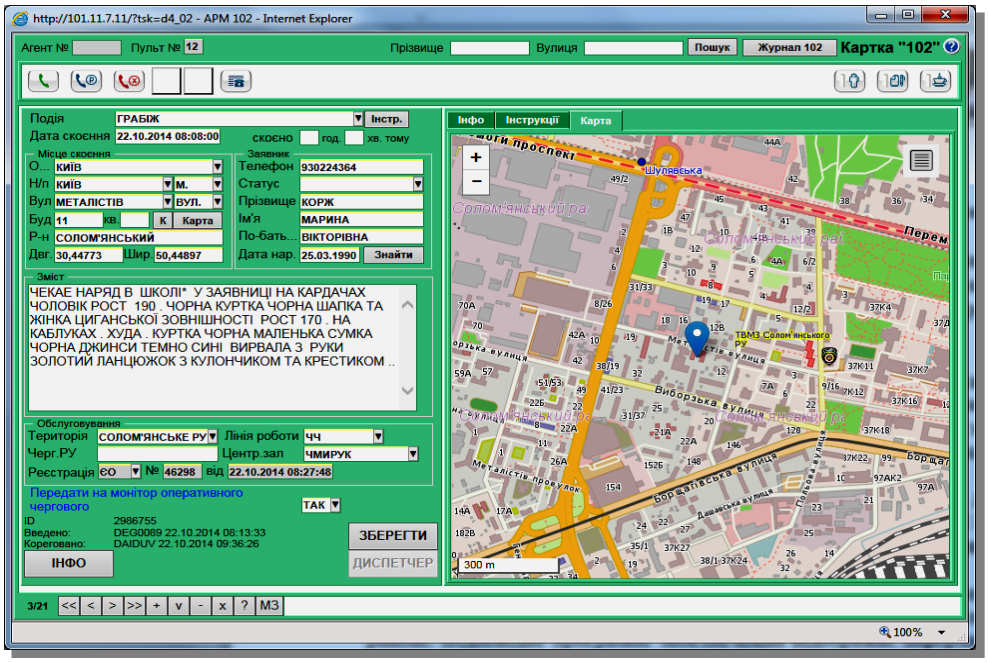


Рис. 6

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 (рис. 7) 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 [18, с. 20; 63, с. 14; 64, с. 11; 65, с. 12].

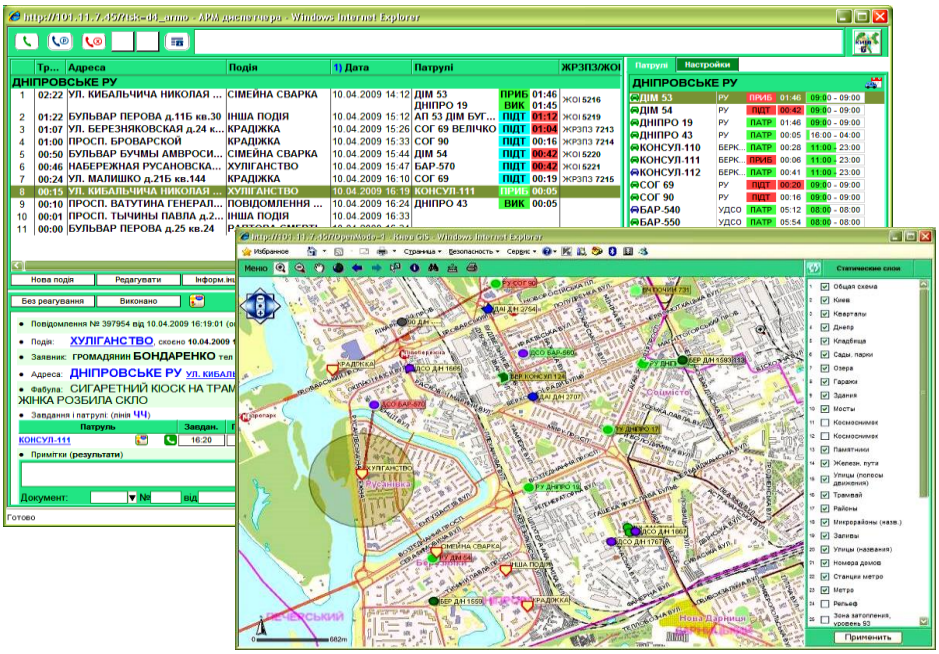


Рис. 7

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 Інформаційного порталу Національної поліції;

– надає повну інформацію на адресу з Інформаційного порталу Національної поліції;

– інформує про повторність надходження інформації про подію;

– контролює реєстрацію події у журналі Єдиного обліку (рис. 8) [22; 25].

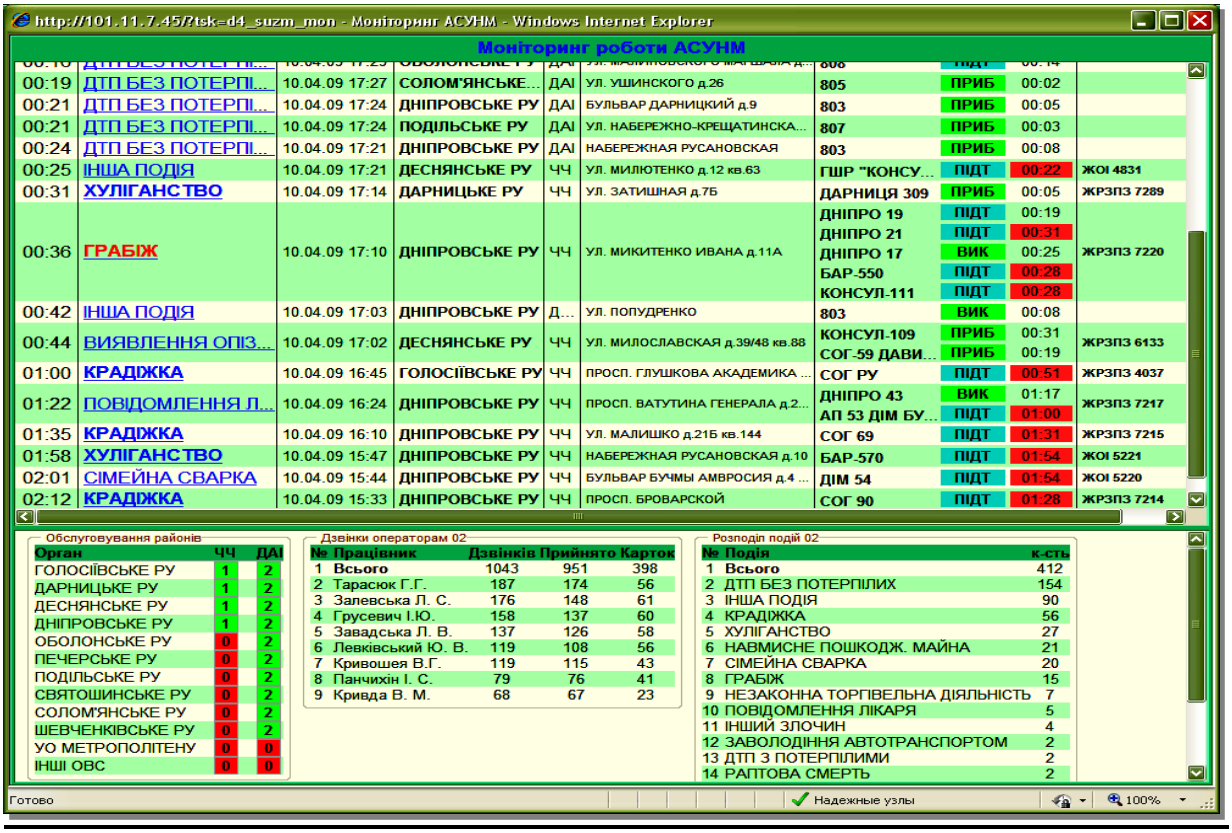


Рис. 8

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 [18, с. 20; 63, с. 14; 64, с. 11; 65, с. 12].

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 [18, с. 20; 63, с. 11; 64, с. 9; 65, с. 10].

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 (рис. 9) [22].

Рис. 9

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 [18, с. 20; 63, с. 11; 64, с. 9; 65, с. 10].

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 (рис. 10) [18, с. 26; 63, с. 14; 64, с. 13].

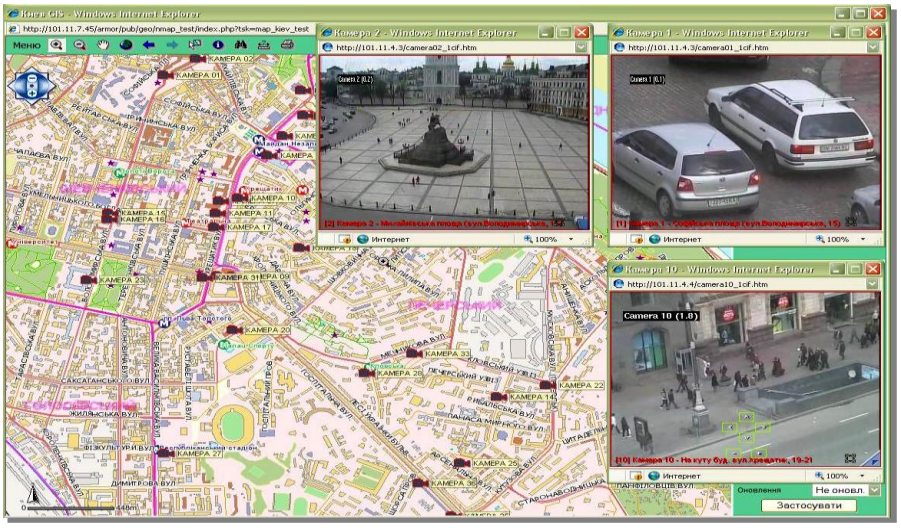


Рис. 10

2. Засоби інформаційного забезпечення та технічні прилади, що мають функції фото- та кінозйомки, відеозапису, які використовуються в діяльності патрульної поліції. Правові, організаційні, тактичні засади їх використання

Використання нагрудних відеокамер (відеореєстраторів) працівниками патрульної поліції під час виконання своїх службових обов'язків здійснюється на підставі статті 40 Закону України «Про Національну поліцію» [53].

Рис. 11

Патрульною Поліцією України використовується персональний відеореєстратор DMT 1.

Рис. 12

Ця модель має такі характеристики:

Датчик	5-Мп CMOS
Чипсет	Ambarella A2
Розширення відео	1920X1080P @ 30fps; 1280x720 @ 30fps; 848x480 @ 30fps @ 60fps
Відео Формат	H.264. MOV
Швидкість перемотки Вперед/Назад	2x, 4x, 8X
Аудіо вхід	Вбудований мікрофон
Аудіо Формат	. WAV
«Водяний знак»	Ідентифікатор користувача, datetime штамп
Камери	16 мега піксельна камера, Підтримка Режиму серійної зйомки
Формат зображення	Макс 4608*3456 JPEG
Snap Shot	Зйомка фото під час запису відео
Час запису	Час безперервного запису: 400 хвилин (батарея повністю заряджена, ІК закриті, 848*480 @ 30fps)
Стан пам'яті	Экран
Одна кнопка записи	+
Функції сигналу	Звуковий, візуальний, тактильні вібрації
ІК-підсвічування	2 ІК

Відео/зображення перегляд, камери,акумулятор

Відео/зображення перегляд	
Екран	2 дюйми tft-lcd-дисплей з високим розширенням
Аудіо	+
Відео вихід	HDMI 1.3
Передача відео	USB 2.0
Камери	
Об'єктив Кут огляду	Широкий 140 градусів
Нічного бачення	До 10 м

Камери	
Об'єктив Кут огляду	Широкий 140 градусів
Нічного бачення	До 10 м

Клас Захисту	IP57
Кріплення	Металевий зажим с 360 градусів обертання

Акумулятор	
Тип	Вбудований 2800 мАч литий-іонний акумулятор
Час заряджання	180 хвилин
Час запису	5 ~ 8 годин
Стан батареї	Екран
Попередження про низький заряд	Звуковий сигнал

Інше	
Ідентифікаційний номер	5-значный ID пристрою та 6-значный ID поліції
Захист паролем	Пароль адміністратора для видалення файлів
Режим серійної зйомки	3/5 зображень
Розміри	94 мм * 61 мм * 31 мм
Вага	175 г
Робоча температура	-40 до + 60 градусів
Температура зберігання	-20 до + 55 градусів

Інструкція щодо порядку зберігання, видачі, приймання, використання нагрудних відеокамер (відеореєстраторів) працівниками патрульної поліції та порядок доступу до відео з них регламентувався Наказом Департаменту патрульної поліції національної поліції України № 100 від 03.02.2016 року [46].

На даний момент наказ №100 відмінено, проводиться робота з розробки нового НПА.

Персональний відеореєстратор є важливим елементом у роботі патрульного поліцейського. Використання нагрудних відеокамер (персональних відеореєстраторів) є превентивним поліцейським заходом, є одним з елементів, що дозволяє наглядно продемонструвати чесність, відкритість та антикорупційну спрямованість діяльності патрульної поліції.

Крім того відеореєстратор виконує профілактичну роль. Наявність відеореєстратора стримує громадян від вчинення певних дій. Ведення відеозапису працює як психологічний стримуючий фактор відносно більшості правопорушників (за винятком особливо зухвалих та цілком неадекватних осіб) [59].

Метою використання персональних відеореєстраторів працівниками патрульної поліції :

- підвищення відповідальності працівників патрульної поліції під час виконання службових обов'язків;
- підвищення рівня довіри суспільства до працівників патрульної поліції;
- підвищення рівня захисту прав та свобод людини і громадянина;
- попередження випадків невиправданого застосування фізичної сили, спеціальних засобів та вогнепальної зброї працівниками патрульної поліції та/або щодо працівників патрульної поліції;
- забезпечення об'єктивного розгляду справ уповноваженими органами шляхом створення додаткових належних доказів;
- підвищення відкритості патрульної поліції;
- забезпечення об'єктивного розгляду скарг на рішення, дії чи бездіяльність працівників патрульної поліції, зменшення кількості безпідставних скарг;
- запобігання конфліктним ситуаціям [59;46].

Починати патрулювання працівник патрульної поліції повинен при наявності відеореєстратора. Нагрудною відеокамерою (відеореєстратором) забезпечується кожен працівник патрульної поліції, який заступає на зміну, в будь-якому випадку хоча б однією нагрудною відеокамерою (відеореєстратором) забезпечується екіпаж.

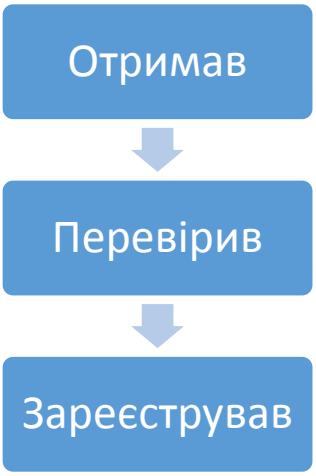


Рис. 13

Перед початком зміни працівник патрульної поліції зобов'язаний самостійно отримати нагрудну відеокамеру (відеореєстратор) у структурному підрозділі інформаційних технологій та зв'язку управління патрульної поліції. Нагрудні відеокамери (відеоресстратори) зберігаються у спеціально відведених приміщеннях управлінь патрульної поліції. Відповідальність за зберігання нагрудних відеокамер (відеореєстраторів),

їх видачу працівникам патрульної поліції та приймання від працівників патрульної поліції несуть уповноважені працівники структурних підрозділів інформаційних технологій та зв'язку управлінь патрульної поліції.

Після отримання відеореєстратора, з метою забезпечення належного функціонування нагрудної відеокамери (відеореєстратора) протягом зміни, працівник патрульної поліції після отримання нагрудної відеокамери (відеореєстратора) зобов'язаний самостійно оглянути та перевірити її [59].

Переконавшись у справності нагрудної відеокамери (відеореєстратора) та відсутності зовнішніх пошкоджень, працівник патрульної поліції здійснює запис у спеціальному журналі, зазначаючи своє прізвище, ім'я, по батькові, роту, номер отриманої нагрудної відеокамери (відеореєстратора) та особистий підпис.

Під час отримання відеореєстратора необхідно звернути увагу на наявність ідентифікаційного номера. Кожній нагрудній відеокамері (відеореєстратору) присвоюється такий ідентифікаційний номер.

Отримання та використання реєстратора під час патрулювання.

Патрульний ЗОБОВ'ЯЗАНИЙ включити відеозапис підчас будь-якого спілкування з громадянами або одразу після прибуття на місце виклику. Нагрудна відеокамера (відеореєстратор) повинна бути включена працівником патрульної поліції та знаходитись в режимі відеозйомки:

- при оформленні дорожньо-транспортної пригоди;
- при перевірці документів;
- при арешті або затриманні особи;
- при поверхневому огляді;
- при загрозі використання фізичної сили, спеціальних засобів або вогнепальної зброї;
- при наданні допомоги особам;
- у випадках, коли усвідомлення особою факту відеофіксації її поведінки може сприяти вирішенню конфліктної ситуації.

У будь-якому іншому випадку контакту з громадянами відеореєстратор повинен бути включений та знаходитись в режимі відеозйомки. У разі активації відеозйомки вона повинна вестися безперервно під час спілкування. Забороняється ставити запис на паузу, або виключати до закінчення спілкування з громадянами. Необхідно контролювати своєчасність включення режиму нічної зйомки у разі необхідності [59].

Отримання та використання реєстратора під час патрулювання.

Нагрудні відеокамери (відеореєстратори) не повинні використовуватись під час:

- розмови з іншими поліцейськими;
- зустрічі з таємними агентами та/або таємними інформаторами з метою забезпечення конфіденційності інформації при виконанні службових обов'язків;
- обідньої перерви;
- перебування у приміщеннях, де працівник патрульної поліції може розраховувати на приватність (вбиральня, кімната відпочинку тощо);
- в інший час, коли немає контакту з особами.

Працівникам патрульної поліції ЗАБОРОНЕНО:

- використовувати нагрудні відеокамери (відеореєстратори) в особистих цілях;
- використовувати нагрудні відеокамери (відеореєстратори) не під час несення служби;
- демонструвати відеозапис з нагрудних відеокамер (відеореєстраторів) третім особам без погодження начальника Департаменту патрульної поліції або начальника управління патрульної поліції у місті;
- змінювати, редагувати, видаляти, копіювати, передавати третім особам
- або іншим чином поширювати відеозаписи, зроблені на нагрудну відеокамеру (відеореєстратор) без дозволу начальника Департаменту патрульної поліції або начальника управління патрульної поліції у місті [59].

Дії з реєстратором після закінчення патрулювання

Процедуру копіювання інформації з камери здійснює уповноважена особа. Самостійно патрульні поліцейські не мають права здійснювати копіювання інформації.

Відеореєстратор дозволяє зняти з нього інформацію тільки за допомогою спеціального програмного забезпечення. Це автоматично захищає патрульного від підозр щодо знищення або зміни відеозапису. Не варто намагатися самостійно підключити реєстратор до комп'ютера та скопіювати записи – не вийде.

Інформація зберігається протягом 30 діб на сервері, цей термін може бути подовжено у випадку отримання скарги від особи на рішення, дії чи бездіяльність працівників патрульної поліції та в інших виключних випадках. Термін зберігання відеозаписів на сервері може бути продовжено за розпорядженням начальника Департаменту патрульної поліції або начальників управлінь патрульної поліції у містах [59].

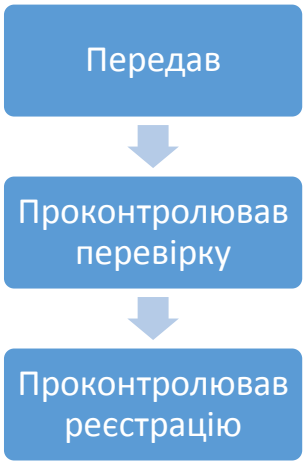


Рис. 14

Характеристики мобільного логістичного пристрою, налаштування його до роботи

У якості робочого термінала патруля використовується мобільна логістична підсистема **LIS-M (Logistic Information System – M)**, що складається з:

– програмного модуля LIS-M для системи Android. Гнучкість програмного забезпечення під операційною системою Android, дозволяє даний продукт інтегрувати в будь-які існуючі пристрої, що мають GSM і GPS модулі;

– сервісу телеметрії й діагностики LIS-M. Програма, використовуючи можливості Google сервісів, визначає місцезнаходження пристрою не тільки по GPS, але й за допомогою стільникового оператора телефонної мережі;

– модуля обміну повідомленнями відображення інформації. LIS-M розроблений для роботи на будь-яких пристроях під операційною системою Android з модулями GPS і GSM (як правило, планшетний комп'ютер з діагоналлю 7» [59].

Рис. 15

LIS-M забезпечує дистанційне отримання завдань та обмін повідомленнями в системі «ЦУНАМІ», інформує диспетчера про етапи виконання, сигналізує про поточний стан виконавця і його переміщення, надає навігаційну допомогу для пошуку оптирисьного шляху до місця призначення, а також забезпечує доступ до баз даних відомчої інформаційної системи. Крім того, надає патрулю можливість введення електронного адміністративного протоколу та друкування квитанції [59].

Параметричні дані пристрою, такі як: заряд батареї, зміна Sim-Карти, наявність зовнішнього живлення, рівень сигналу в мережі, дані про місце розташування (довгота, широта), і т.п. записуються в локальну базу даних обладнання та передаються на сервер у міру можливості із заданим інтервалом.

Тобто, використання LIS-M: 1) сприяє оптимізації ресурсів патрульної служби для реагування в конкретній ситуації; 2) що значно підвищує оперативність реагування на заяви та повідомлення; 3) дозволяє ефективно контролювати роботу патруля.

Робота патруля з системою «ЦУНАМІ» за допомогою мобільного логістичного пристрою складається з таких етапів, як:

– установка зв'язку з центром управління;
– реєстрація патруля в системі;
– прийом та виконання завдання;
– завершення виконання завдання [59].

Підключення мобільного логістичного пристрою до бортової мережі автомобіля, установка зв'язку з центром управління.

В комплект для встановлення планшета в авто входить штатне кріплення, за допомогою якого планшет встановлюється в салоні автомобіля. Рекомендоване місце для кріплення пристрою в авто Toyota Prius зображено на рис. 16.

Також до комплекту входить зарядний пристрій, який потрібно підключити до автомобільної розетки 12 В.

Рис. 16

Якщо пристрій повністю вимкнено, то для того, щоб його включити, необхідно на панелі планшету натиснути кнопку [**Пуск**] протягом 5 секунд. Якщо пристрій тільки заблокований, то для його розблокування потрібно просто натиснути кнопку [**Пуск**] та розблокувати екран.

Після включення з'являється зображення системи Андроїд, яке треба розблокувати.

Для норрисьного функціонування системи по замовчуванню вже налаштовані наступні параметри:

1. GPS повинен бути включений;

2. Передача даних повинна бути включена, правильно налаштована точка доступу APN;

3. Авто-відключення екрану «Сплячий режим» повинно бути більше 2 хвилин;

4. Середовище обміну даних повинне бути включене;

5. Звук повинний бути включений [59].

Після розблокування системи Андроїд (рис. 19):

– запускається програмне забезпечення «LIS-M» (у лівому верхньому куті планшету з'являється значок 

);

– планшет намагається з'єднатися з центром управління, але як правило повідомляє **«No connection»**.

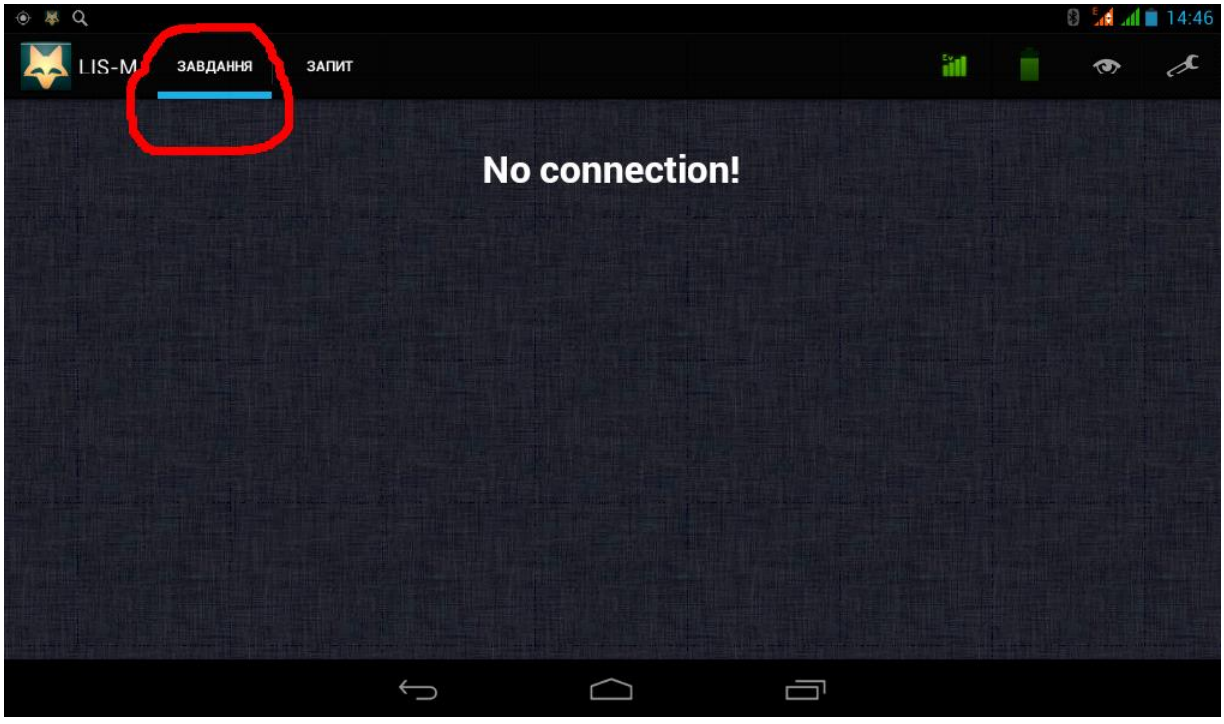


Рис. 17

Слід почекати протягом кількох хвилин, поки планшет автоматично не встановить з центром управління. Якщо на екрані пристрою продовжує відображатися повідомлення **«No connection»,** це свідчить про відсутність сигналу.

Для того, щоб прискорити процесу з'єднання можна натиснути на значок  [**Оновити**] на верхній панелі в правому верхньому кутку екрану.

При першому включенні пристрою заповнюється форма первинної реєстрації (рис. 18).

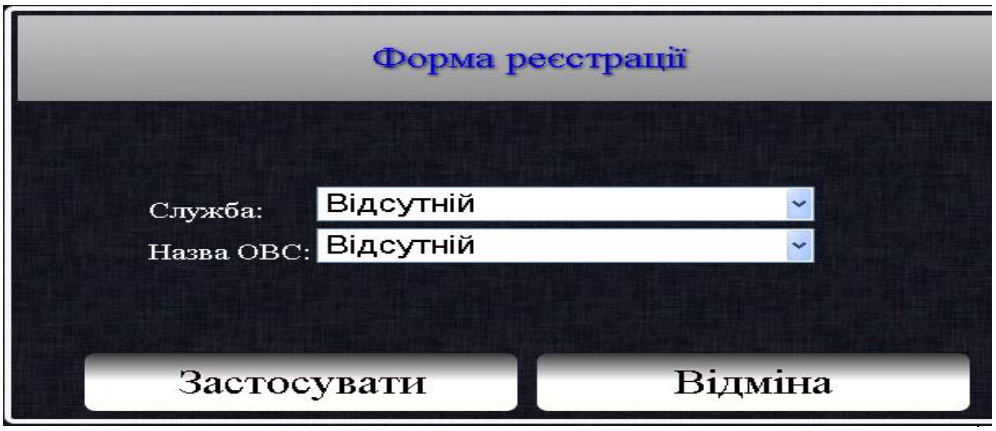


Рис. 18

Для патруля з'єднання пристрою з центром управління можна вважати таким, що відбулося коли на екрані планшету з'явилася форма реєстрації патруля в системі [59].

Визначення місцезнаходження через геоінформаційну систему.

Система GPS мобільних патрулів дає можливість відслідковувати місцезнаходження патруля, його напрямки руху та статус на даний час (зайнятий, вільний).

Для визначення місцезнаходження патруля слід натиснути значок (мапа міста) з правої сторони основної форми документу (рис. 19).

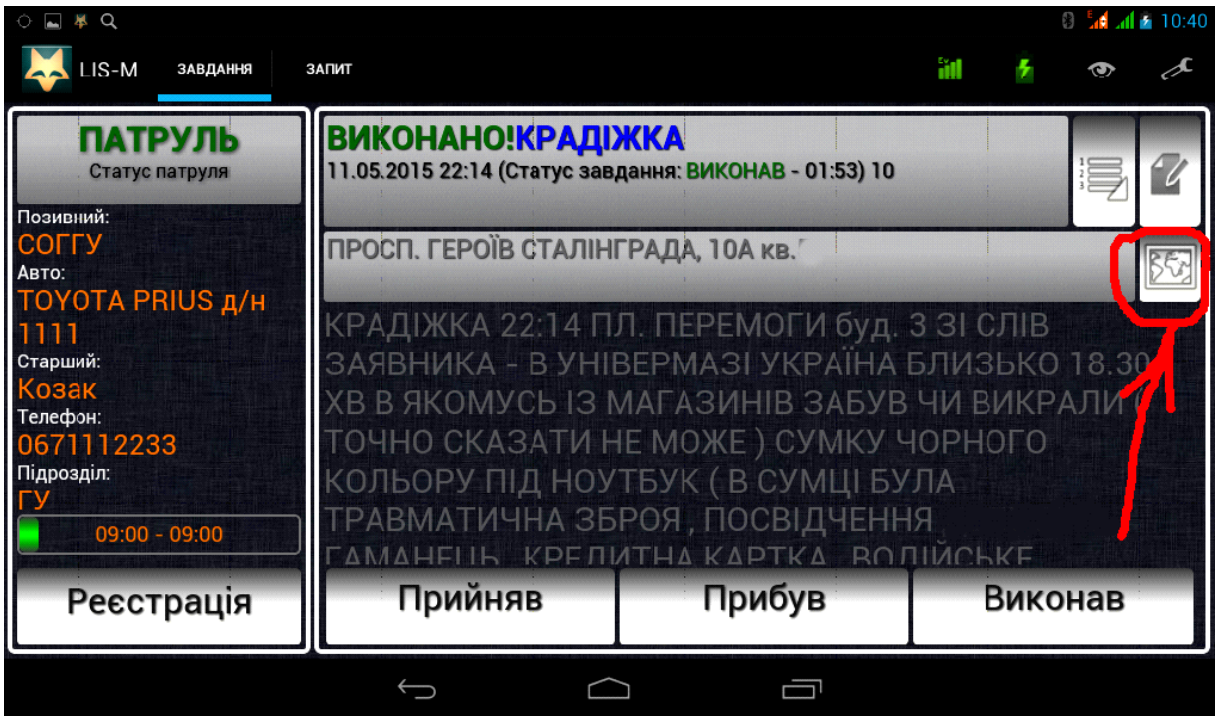


Рис. 19

Водночас буде й показано маршрут руху патруля до адреси, вказаної у завданні (рис. 20).

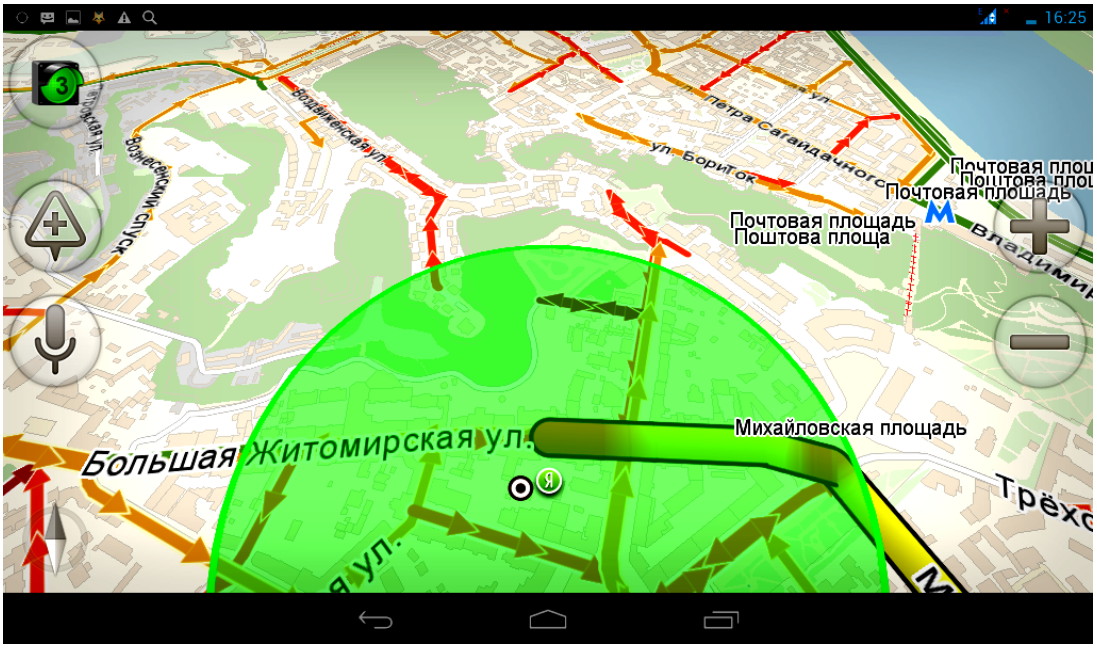


Рис. 29

Отримання патрулем завдання

У 2017 році в Національній поліції впроваджена «Електронна система фіксації поліцейськими результатів реагування на події», відповідно до розпорядження Голови Національної поліції №6327 від 16.06.2017р. та Наказу МВС України 16.02.2018 № 111 «Про затвердження Інструкції з організації реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України» [43], який втратив чинність. Замість нього було прийнято Наказ Міністерства внутрішніх справ України 27 квітня 2020 року № 357 «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» [42]

Зареєструвавшись в інформаційній системі та встановивши статус, патруль приступає до виконання поставлених йому завдань.

Під час підготовки матеріалів поліцейськими, які прибули за викликом або самостійно створили завдання про подію для реагування, після вжиття відповідних заходів щодо припинення правопорушення або здійснення реагування на іншу подію заповнюється інформаційна картка у планшетному логістичному пристрої, у якій детально описується подія (обставини, свідки, необхідні фотозображення тощо) та зазначаються відповідні дії поліцейського. Ці дані інтегруються (автоматично переносяться) в картку підсистеми «Єдиний облік» для подальшого прийняття рішення за спрощеною системою [59].

Порядок користування підсистемою складання рапорту Електронної системи фіксації поліцейськими результатів реагування на події працівниками патрульної поліції ДПП, груп реагування патрульної поліції ГУНП.

Диспетчер, отримавши електронну картку «102» про подію.

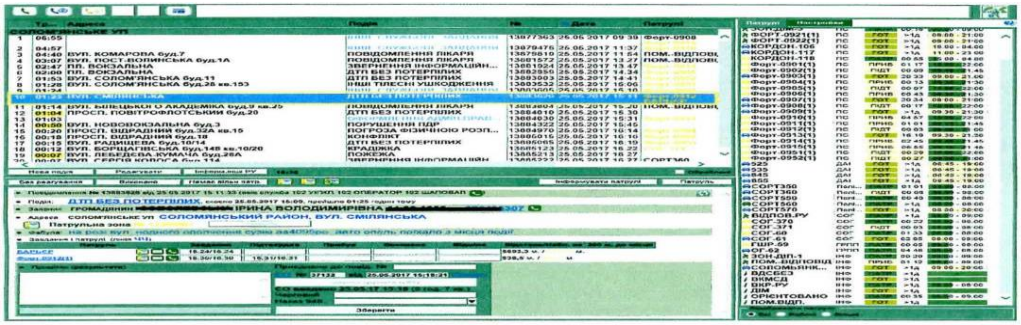


Рис. 21

Ра допомогою АРМ «Диспетчер» ІТП «Цунамі» призначає та направляє на місце події вільний наряд поліції для здійснення реагування Поліцейський, який заступив на чергування, за допомогою планшетного логістичного пристрою реєструється в ІТП «Цунамі», зазначивши при цьому у відповідних полях свій персональний логін та пароль, позивний, марку та номер службового автомобіля, номер мобільного телефону, назву служби та підрозділу. Далі натискає кнопку «Застосувати» (рис. 22) [22].

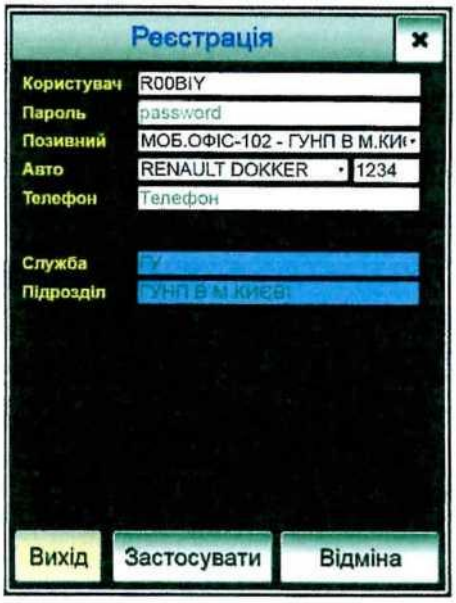


Рис. 22

Отримавши від диспетчера (оперативного чергового) інформацію про правопорушення або подію, поліцейський ставить відповідну відмітку про прийняття виклику (кнопка «Прийняв») у мобільному логістичному пристрої, а прибувши на місце події (виклику), у найкоротший строк ставить відповідну відмітку про прибуття (кнопка «Прибув») (рис. 23).

Рис. 23

У разі безпосереднього виявлення правопорушення або іншої події нарядом поліції поліцейський, натиснувши на кнопку «Введення», заповнює відповідні поля електронної картки програмного забезпечення в розділі «Введення нового завдання», а саме із запропонованого обирає вид події (ПЕРЕСЛІДУВАННЯ, ПЛАН ПЕРЕХВАТ, ДОПОМОГА ПІШОМУ ЕКІПАЖУ тощо), у разі необхідності зазначає номерний знак автомобіля (автомобілів) та описує короткий зміст події, після чого натискає кнопки «зберегти» та «Прибув». (рис. 24)

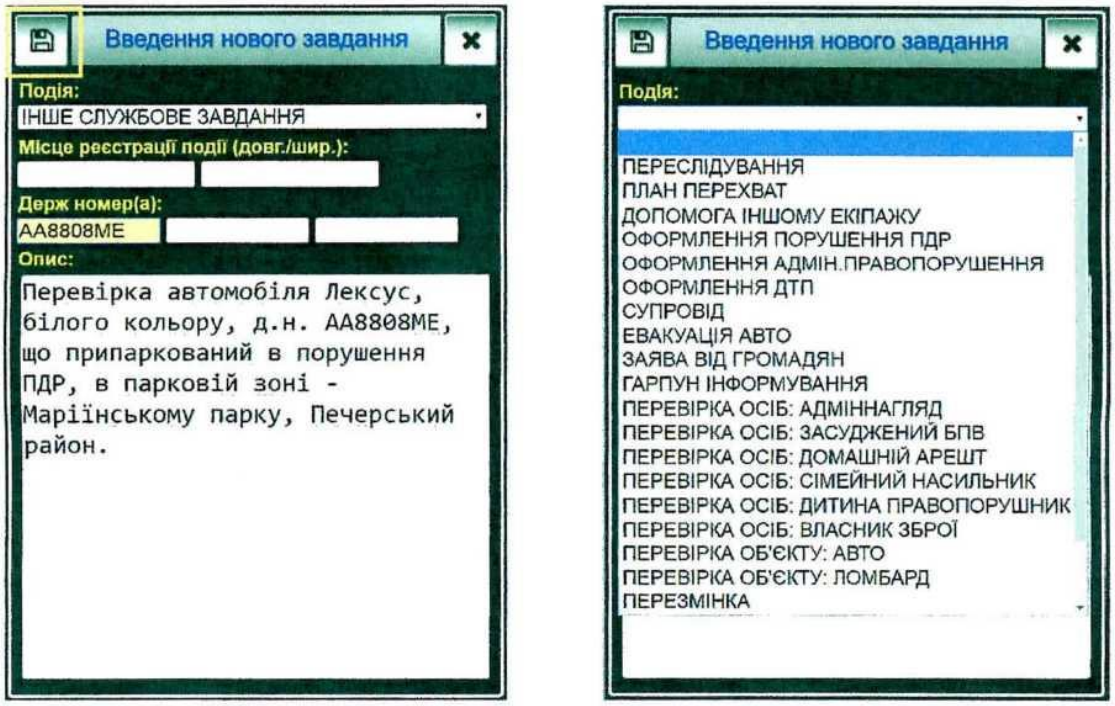


Рис. 24

Звітування про результати виконання завдання

За результатами розгляду звернення (виїзду) поліцейський, натиснувши на виділену на рисюнку кнопку (результат виконання завдання), залежно від виду події та результатів ужитих заходів у розділі «Оберіть категорію» обирає відповідну категорію дій та заповнює відповідні поля електронної картки (рис. 25).

Рис. 25

В обраних категоріях поліцейський заповнює запропоновані програмним забезпеченням поля у вкладках щодо вжитих заходів та отриманої інформації

У категорії «Інші повідомлення» поліцейський заповнює наявну інформацію розділу «Результат виконання завдання» (рис. 25), зокрема:

У полі «Прийняте рішення» обирає із запропонованого класифікатора один з пунктів, якщо відомості не підтвердилися - у категорії «Інформація не підтвердилась» (відсутній заявник, відсутня подія, відсутні наслідки, інше: інформація не підтвердилась), а якщо відомості підтвердилися - у категорії «Прийнято рішення на місці події» (складено адміністративний протокол, евакуація авто з складенням адмінпротоколу, складено постанову про адм. правопорушення та ін.) або «Інше» (інформація потребує додаткового розгляду, відомості кримінального характеру, інший результат) [22].

У полі «Кваліфікація» обирає із запропонованого класифікатора один із пунктів у категоріях:

«Злочин» (вбивство, тяжкі тілесні ушкодження, зґвалтування, розбій та ін.);

- «Подія» (ДТП без потерпілих, ДТП з потерпілими, не працює світлофор, затор на дорозі тощо); «масові заходи» (санкціонований мітинг, не санкціонований мітинг, пікетування та ін.);
- « Адмінправопорушення» (адмінправо- порушення, сімейна сварка, сварка між сусідами та ін);
- «Скарга на працівників поліції» (нереєстрація заяви і повідомлення громадян, неналежне реагування на заяви та повідомлення громадян тощо);
- «Службові завдання» (переслідування, план перехват, допомога іншому екіпажу та ін.);
- «Відсутні кваліфікація» (рис. 26) [22; 18].

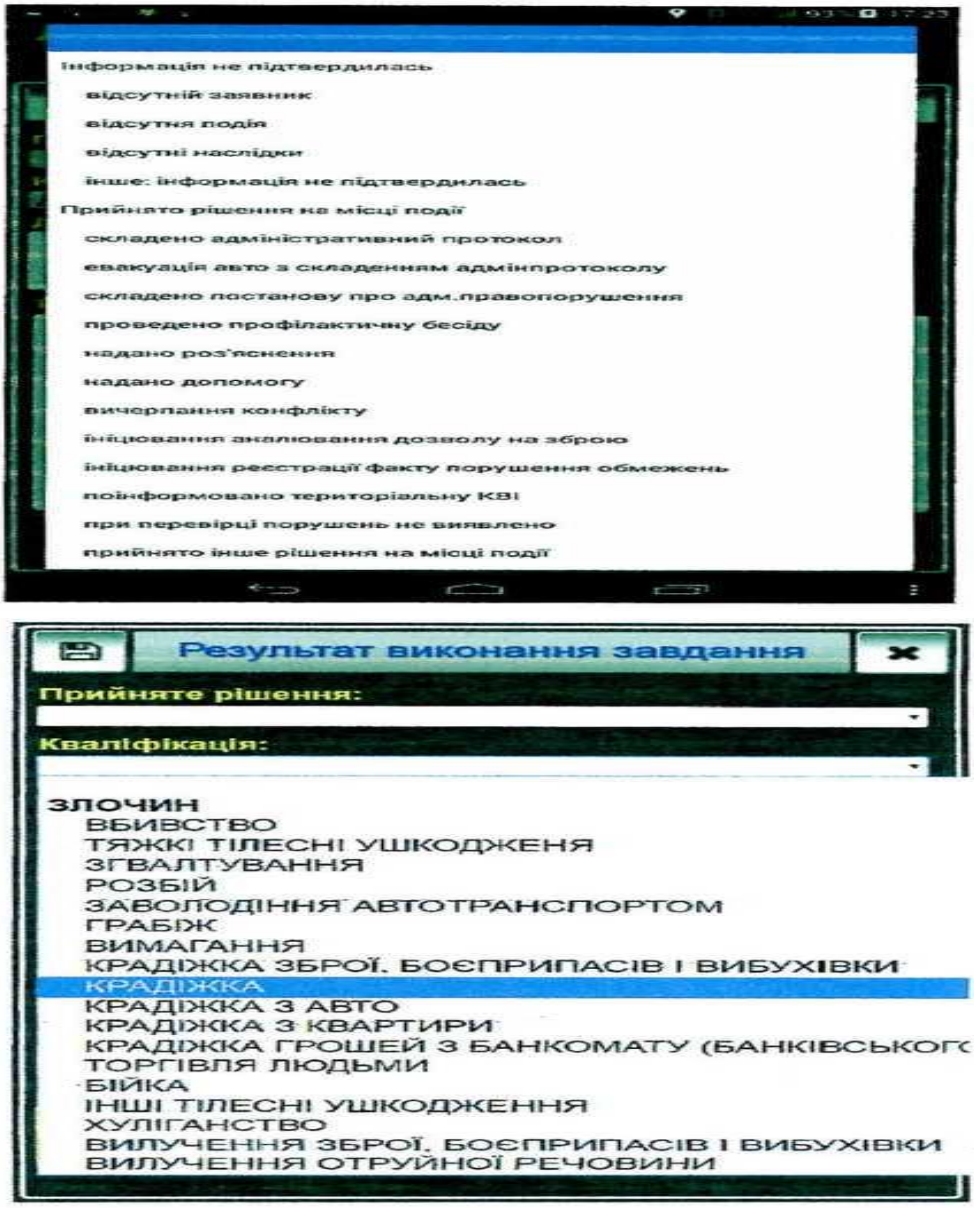


Рис. 26

У полі «Додаткова інформація», натиснувши на кнопку «Ок», вибирає один із запропонованих пунктів у категоріях «Відносно кого» (у відношенні військовослужбовця, у відношенні інкасатора, у відношенні іноземця тощо) та «Мотиви» (мотиви скоєння злочину користь, мотиви скоєння злочину помста, мотиви скоєння злочину хуліганство тощо) (рис. 29) [22].

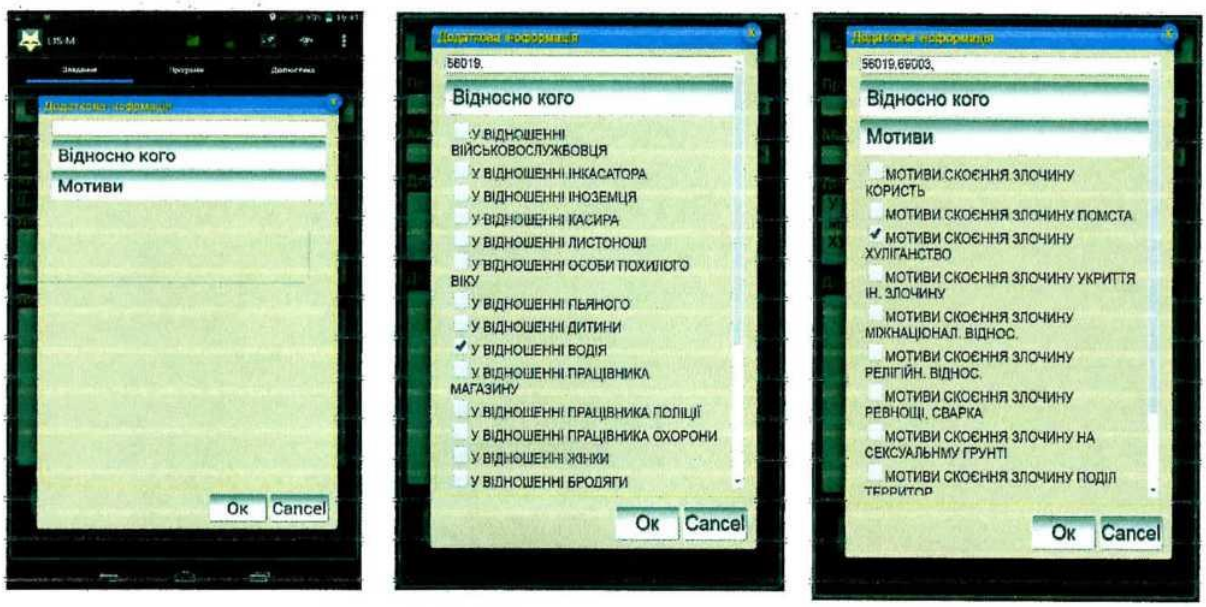


Рис. 27

У полі «Додаткова інформація (Примітки)» зазначає інформацію про подію та вжиті заходи. У полі «Додати» зазначає інформацію про вжиті нарядом поліції заходи, учасників події, виявлені речі, фотозображення (за наявності) шляхом натискання на відповідні кнопки «Дію», «Особу», «Річ» та «Фото». У разі відсутності інформації, яку необхідно додати, зберігає введену інформацію, натиснувши на кнопку «зберегти».

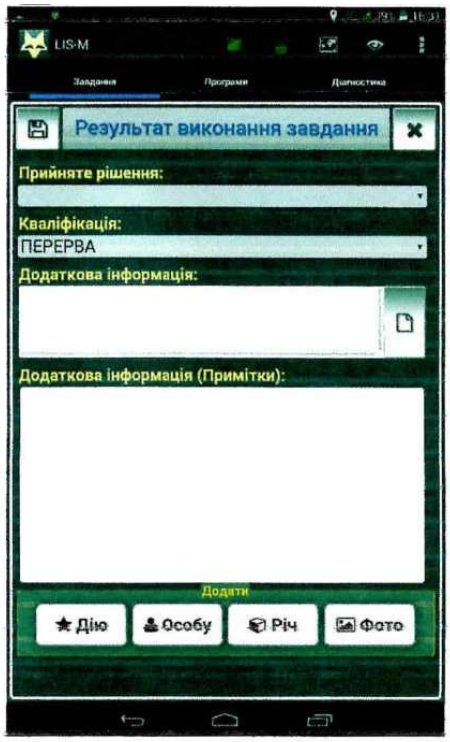


Рис. 28

Залежно від виду події поліцейський, натиснувши кнопку «Дію», із запропонованого словника «Дії патрульного» вибирає назву дії, яку виконано (викликано СОГ, викликано швидку допомогу, встановлено очевидців події, затримано правопорушника, здійснювалася охорона місця події, здійснювалося переслідування злочинця, надано медичну допомогу та ін.) або/та, за необхідності, у вільному полі «Опис» зазначає інші додаткові відомості. Зазначену інформацію зафіксуйте, натиснувши на кнопку «зберегти».

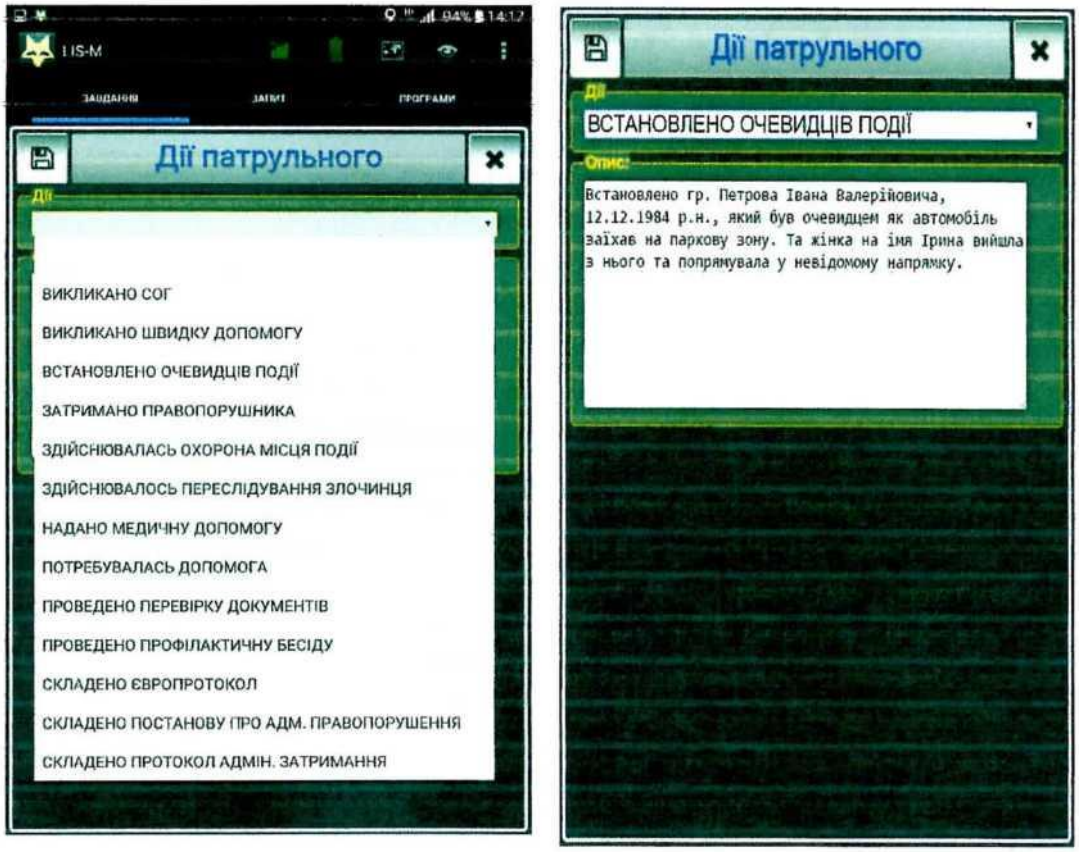


Рис. 29

Залежно від наявної інформації про особу поліцейський, натиснувши на кнопку «Особа», у розділі «Відомості про особу» зазначає наявні (уточнені) відомості про особу (прізвище, ім’я, по батькові, дата народження (у форматі dd.mm.yyyy), вибирає з класифікатора її статус, стать та громадянство), місце проживання (натиснувши на кнопку «» та обравши із запропонованого класифікатора: область, район, вид та назву населеного пункту, вид та назву вулиці, а також зазначає номер будинку та квартири), контактні дані особи (телефон (у форматі 380xxxxxxxxx) та E-mail), спосіб інформування про результати розгляду звернення заявника (проставляючи позначку навпроти обраної категорії: листом, телефоном, E-mail або відмовився) або/та, за необхідності, у вільному полі картки «Примітки/Пояснення» зазначає інші додаткові відомості. Зазначену інформацію зберігає, натиснувши на кнопку «зберегти» [22].

Рис. 30

Залежно від наявної інформації про річ поліцейський, натиснувши на кнопку «Річ», у розділі «Відомості про речі» зазначає наявні відомості про речі, обравши із запропонованого класифікатора групи (гроші, цінні папери; дорог. метали, каміння; метали, речовини; ювелірні вироби; майно житлово- комунального господарства; ордени; зброя; боєприпаси; наркотичні речовини; транспортні засоби; інтернет-ресурси; антикваріат і образотворче мистецтво; предмети колекціонування; апаратура, техніка; вироби; продукти; сільгосппродукція; тварини; документи; обладнання), вид речі та одиницю вимірювання (шт., грам, інше, кг, літр, м, тон), а також зазначає їх номер та кількість) або/та, за необхідності, у вільному полі картки «Особливості» зазначає інші додаткові дані. Зазначену інформацію зберіте, натиснувши на кнопку «зберегти» [59].

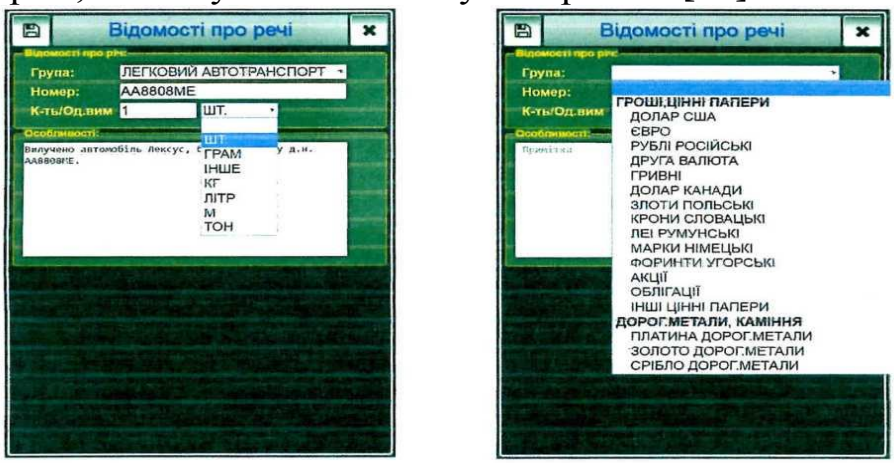


Рис. 31

Поліцейський, натиснувши на кнопку «Фото», має можливість у полі «Виберіть зображення» внести раніше сфотографоване планшетним логістичним пристроєм зображення, при цьому, обравши із запропонованого класифікатора, зазначає в полі «Категорія» інформацію про завантажений матеріал (місце події, особа, предмет) або/та, за необхідності, у вільному полі картки «Опис» зазначає інші додаткові відомості. Зазначену інформацію зберігає, натиснувши на кнопку «зберегти».

Рис. 32

Після заповнення всіх необхідних реквізитів розділу «Результат виконання завдання» категорії «Інші повідомлення», поліцейському надається можливість переглянути внесену інформацію, за заповненими розділами категорій, її відредагувати (натиснувши відповідну кнопку) або видалити (натиснувши кнопку зі стрілкою). Поліцейський, перевіривши правильність внесення інформації, натискає кнопку «Подати рапорт», після чого проект електронної картки надсилається оперативному черговому органу поліції згідно з територіальністю для погодження [18; 22].

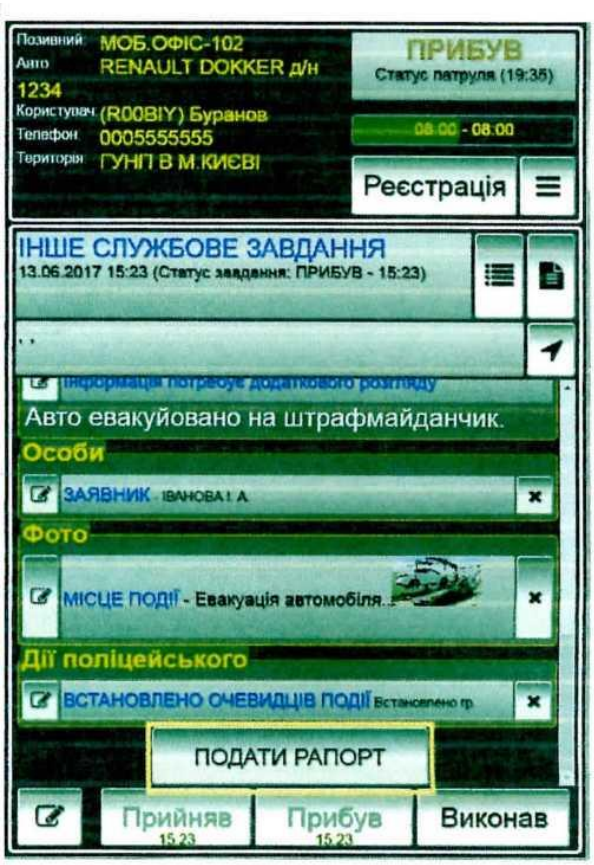


Рис. 33

За разі наявності зауважень (формуються оперативним черговим у вільному полі картки) до змісту проекту картки (недостатня інформація, сумнівні рішення) вносить необхідні зміни або вживає додаткових заходів на місці (уточнює відомості в заявника, установлює можливих очевидців тощо), після чого повторно надсилає картку для погодження (рис. 34).

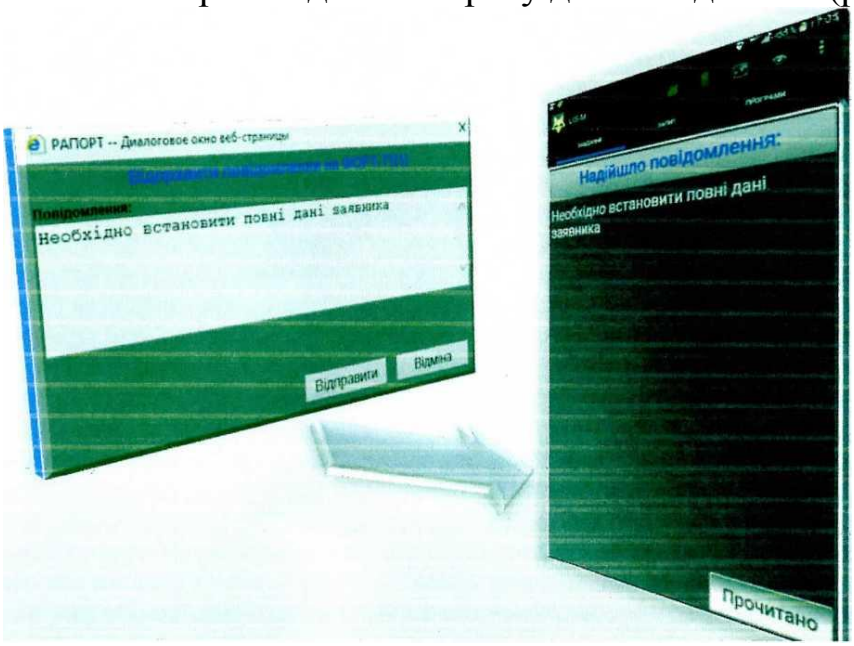


Рис. 34

Після отримання відповідного підтвердження оперативного чергового підрозділу поліції остаточно формує картку (здійснює остаточне збереження)..

У категорії **«Інформація не підтвердилась»** поліцейський заповнює наявну інформацію згідно із запропонованими розділами.

У розділах «Відомості про особу» (програма пропонує заповнити у різних вкладках статуси осіб: заявник та свідок) заповнюється інформація аналогічно розглянутій вище

За наявності двох або більше осіб з однаковими або різними статусами натискає на кнопку «зберегти та додати», що створює додаткове вікно для заповнення наявної інформації про інших осіб. Заповнивши відповідні поля, натискає на кнопку «зберегти та перейти далі». У разі відсутності відомостей про особу поліцейський натискає кнопку «перейти далі» [22; 18].

Рис. 35

У розділі «Дії патрульного» заповнюється інформація аналогічно до розглянутій вище. При заповненні інформації про різні дії (декілька дій) поліцейський натискає, на кнопку «зберегти та додати», що створює додаткове вікно для заповнення інформації про іншу дію. Заповнивши відповідні поля, поліцейський натискає на кнопку «зберегти та перейти далі». У разі невиконання дій поліцейський натискає кнопку «перейти далі» [18, с. 26; с. 56; 63, с. 14; 64, с. 13].

Рис. 36

У розділі «Фото» заповнюється інформація аналогічно розглянутій раніше. За наявності двох або більше фотозображень поліцейський натискає на кнопку «зберегти та додати», що створює додаткове вікно для збереження іншого фотозображення та заповнення інформації про нього. Заповнивши відповідні поля, поліцейський натискає на кнопку «зберегти та перейти далі». У разі відсутності фотозображень поліцейський натискає кнопку «перейти далі» [18, с. 26; с. 56; 63, с. 14; 64, с. 13].

Рис. 37

У розділі «Результат виконання завдання» заповнюється інформація. Після заповнення всіх необхідних полів поліцейський натискає кнопку «зберегти».

Після заповнення всіх необхідних реквізитів розділу «Результат виконання завдання» категорії «Інформація не підтвердилась», поліцейському надається можливість переглянути внесену інформацію, за заповненими розділами категорій, її відредагувати (натиснувши відповідну кнопку) або видалити (натиснувши кнопку зі стрілкою). Поліцейський, перевіривши правильність внесення інформації, натискає кнопку «Подати рапорт», після чого проект електронної картки надсилається оперативному черговому органу поліції згідно з територіальністю для погодження.

За разі наявності зауважень (формуються оперативним черговим у вільному полі картки) до змісту проекту картки (недостатня інформація, сумнівні рішення) вносить необхідні зміни або вживає додаткових заходів на місці (уточнює відомості в заявника, установлює можливих очевидців тощо), після чого повторно надсилає картку для погодження.

Після отримання відповідного підтвердження оперативного чергового підрозділу поліції остаточно формує картку (здійснює остаточне збереження) [18, с. 26; с. 56; 63, с. 14; 64, с. 13].

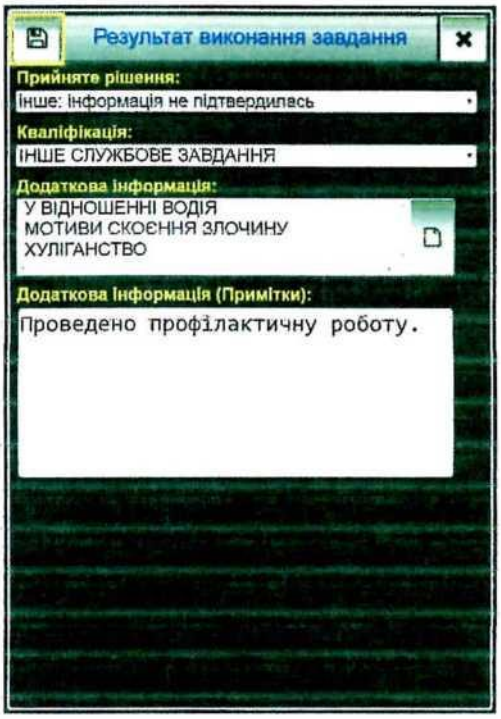


Рис. 38

У категорії «Скласти матеріал про АП» поліцейський заповнює наявну інформацію згідно із запропонованими розділами. У розділах «Відомості про особу» (програма пропонує заповнити у різних вкладках статуси осіб: заявник, свідок, потерпілий, затриманий та порушник) заповнюється інформація аналогічно розглянутій вище. У розділах «Дії патрульного» (програма пропонує заповнити у різних вкладках відомос-

ті про складання постанови та протоколу про адміністративне правопорушення) заповнюється інформація аналогічно розглянутій раніше. Крім того, програма пропонує заповнити поля «Серія» та «Номер» складеного протоколу (постанови), а також із запропонованого словника вибирає статтю КУпАП [18, с. 26; 63, с. 29].

Рис. 39

У розділах «Фото», «Результат виконання завдання» заповнюється інформація аналогічно до категорії «Інші повідомлення».

У категорії «Кримінальні відомості» поліцейський заповнює наявну інформацію, згідно до запропонованих розділів. У розділах «Відомості про особу» (програма пропонує заповнити у різних вкладках статуси осіб: заявник, потерпілий, підозрюваний, свідок, учасник події, затриманий, померлий та порушник) заповнюється інформація аналогічно до розглянутих вище у категорії «Інші повідомлення». У розділах «Дії патрульного» (програма пропонує заповнити у різних вкладках відомості про виклик СОГ, виклик швидкої допомоги, затримання правопорушника, здійснення охорони місця події, здійснення переслідування злочинців, надання медичної допомоги, потребу допомоги, складання постанови та протоколу про адміністративне правопорушення, затримання) заповнюється інформація аналогічно до розглянутих вище у категорії

«Інші повідомлення». У розділі «Відомості про речі» заповнюється інформація аналогічно до розглянутих вище у категорії «Інші повідомлення». За наявності двох або більше речей поліцейський натискає на кнопку «зберегти та додати», що створює додаткове вікно для збереження інших речей та заповнення інформації про них. Заповнивши відповідні поля, поліцейський натискає на кнопку «зберегти та перейти далі». У разі відсутності речей поліцейський натискає кнопку «перейти далі» [18; с. 47; 63, с. 29].

У розділі «Фото», «Результат виконання завдання» заповнюється інформація аналогічно до категорії «Інші повідомлення». Після заповнення всіх необхідних реквізитів у категорії «Кримінальні відомості» поліцейський діє аналогічно до категорії «Інші повідомлення».

У категорії «ДТП без потерпілих» поліцейський заповнює наявну інформацію відповідно до запропонованих розділів, У розділі «Відомості про особу» (програма пропонує заповнити у різних вкладках статуси осіб: заявник, свідок та учасник події) заповнюється інформація аналогічно до категорії «Інші повідомлення». У розділі «Дії патрульного» (програма пропонує заповнити у вкладці відомості про складання постанови про адміністративне правопорушення) заповнюється інформація аналогічно до категорії «Інші повідомлення». У розділі «Відомості про речі» (програма пропонує заповнити у різних вкладках групи транспортних засобів: легковий та вантажний автотранспорт), «Фото», «Результат виконання завдання» заповнюється інформація аналогічно до категорії «Інші повідомлення». Після заповнення всіх необхідних реквізитів у категорії «ДТП без потерпілих» поліцейський діє аналогічно розглянутих вище категорій [22].

У категорії **«Європротокол»** поліцейський заповнює наявну інформацію, відповідно до запропонованих розділів. У розділах «Відомості про особу» (програма пропонує заповнити у різних вкладках статуси осіб: заявник, свідок та учасник події) та «Дії патрульного» (програма пропонує заповнити у вкладці відомості про складання європротоколу) заповнюється інформація аналогічно до категорії «Інші повідомлення». Крім того, програма пропонує заповнити поля номерів транспортних засобів «А» та «В».

Рис. 40

У розділах «Відомості про речі» (програма пропонує заповнити інформацію про страховий поліс), «Фото», «Результат виконання завдання» заповнюється інформація аналогічно до категорії «Інші повідомлення». Після заповнення всіх необхідних реквізитів у категорії «Європротокол» поліцейський діє узгоджує інформацію з черговим територіального підрозділу поліції [18; с. 47; 63, с. 29; 22].

Радіозв'язок

Особливості використання радіозв'язку

- висока мобільність;
- більша швидкість установлення зв'язку;
- можливість підтримання зв'язку з кореспондентами, місце розташування яких невідоме;
- висока швидкість передавання інформації;
- велика відстань передачі сигналів;
- широкий спектр смуги пропускання сигналів;
- можливість одночасного передавання інформації великій кількості кореспондентів;
- велика пропускна здатність каналу зв'язку [59].

Для передачі інформації необхідно:

1. переконатися в тому, що канал вільний (радіообмін не ведеться) В разі, якщо канал зайнятий іншими кореспондентами, необхідно дочекатися завершення їх роботи. Втручатися в радіообмін між двома радіостанціями можна тільки при надзвичайних обставинах. Якщо спробувати вклинитися в розмову, не дочекавшись закінчення чужої передачі, буде тільки створено перешкоду. Запам'ятайте: коли хтось щось передає - чути тільки його;
2. натиснути кнопку передачі та після секундної паузи викликати абонента, назвавши спочатку **ЙОГО, а потім СВІЙ** позивний;
3. через секунду **(НЕ ДО!)** після завершення виклику відпустити кнопку **(НЕ ПОЧИНАТИ ПЕРЕДАЧУ ІНФОРМАЦІЇ)**;
4. отримати підтвердження від абонента і тільки потім передати інформацію. Передача інформації не повинна вестись більш 20-ти секунд. Після цього треба зробити перерву: поки ведеться передача ніхто інший не може скористатися зв'язком;
5. якщо після отримання інформації необхідно передати свою інформацію, зроби невеличку паузу (1-2 секунди). В цій паузі може надійти інший виклик, можливо з терміновим повідомленням.

6. наприкінці сеансу зв'язку кожному учаснику **ОБОВ'ЯЗКОВО** потрібно повідомити про повне прийняття інформації, передавши одне з наступних слів: «кінець зв'язку», «плюс», «зрозумів [59].

Алгоритм проведення радіозв'язку

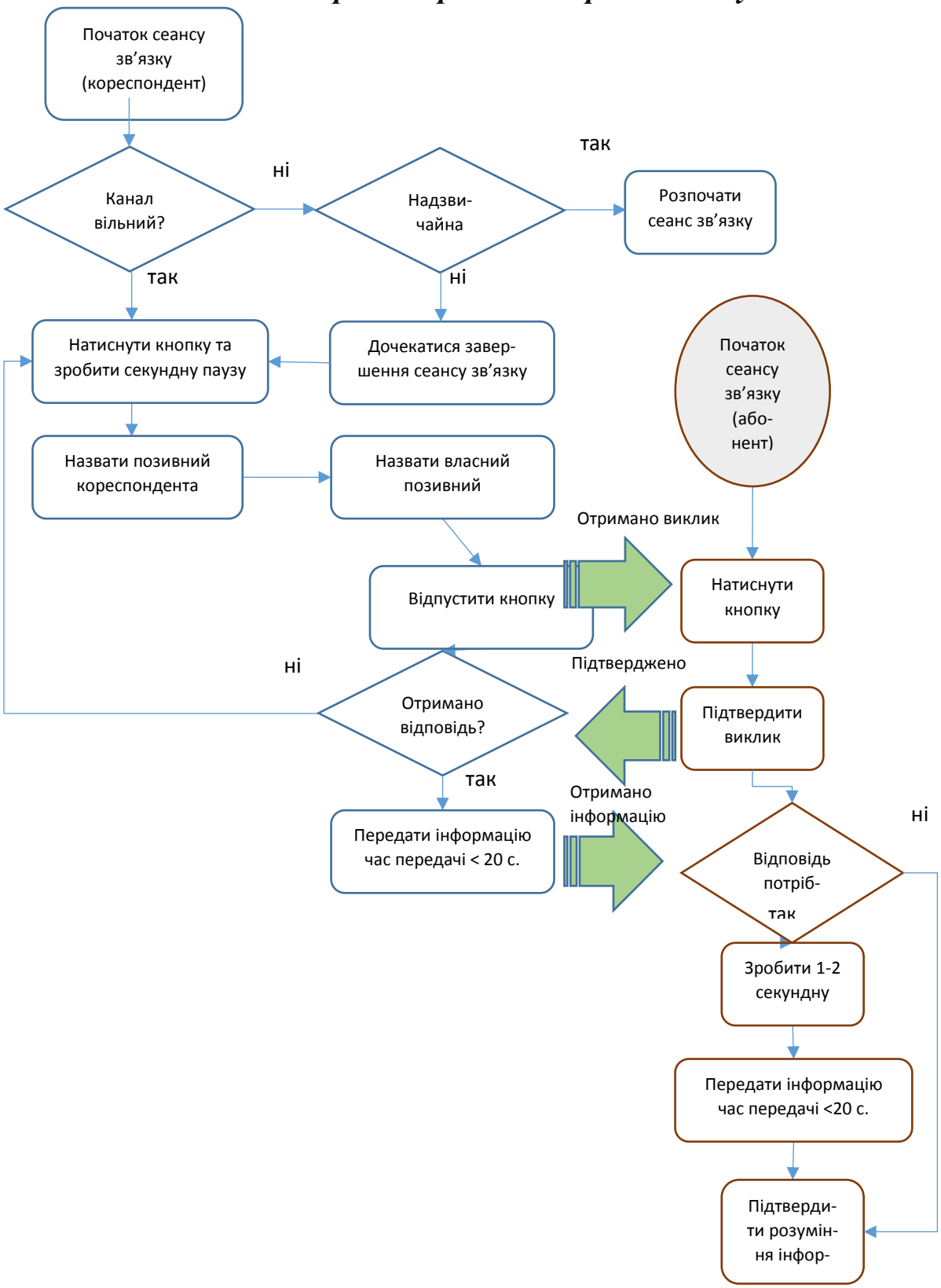


Рис. 41

При проведенні сеансу радіозв'язку КАТЕГОРИЧНО ЗАБОРОНЯЄТЬСЯ:

× Називати посади, прізвища, імена та звання посадових осіб.
× Вести особисті розмови.
× Передавати повідомлення, які розголошують державну або
× службову таємницю.
× Передавати повідомлення, які можуть розкрити сутність оперативних заходів.
× Використовувати при передачі довільні радіопозивні.
× Самовільно без дозволу керівництва вимикати радіостанцію.
× Перевіряти канал зв'язку шляхом проведення переговорів.
× Не виходити на зв'язок, ігноруючи виклик [59].

Перелік повідомлень, дозволених для відкритої передачі:

1) Про розбійний напад, крадіжки, пограбування та інші правопорушення (вид, місце, час).
2) Про виявлення трупа чи людини, яка знаходиться в безпорадному стані.
3) Про стихійні лиха, нещасні випадки (крім особливо важливих об'єктів і кількості жертв).
4) Про окремі пожежі, не розкриваючи найменування і дислокацію особливо важливих об'єктів, відомості, які заборонені для опублікування в пресі.
5) Про стан справ на пожежах і відомості про стан їх гасіння (крім інформації про смерть людей).
6) Про викрадення автомототранспорту.
7) Про належність автомототранспорту і місце його стоянки.
8) ДТП (крім тих, у яких загинуло 5 і більше людей, травмовано 10 і більше людей).
9) Виклик працівників швидкої допомоги до місця пригоди.
10) Про технічний стан наявних засобів зв'язку і службового транспорту.
11) Про стан системи ОПС, електроживлення і телефонного зв'язку на об'єкті, що охороняється, здачі об'єкту під охорону або зняття з-під охорони, отримання сигналу «ТРИВОГА» з об'єкту, що охороняється.
12) Про перебіг спортивно-масових та інших подібних заходів та про стан громадського порядку під час їх проведення.
13) Про метеорологічні та дорожні умови [59].

Приклади радіообміну:

1. Радіообмін між двома абонентами

Радіостанція 1 (позивний Цунамі 7): *Цунамі 12, Цунамі 12, я Цунамі 7, де ви знаходитесь, прийом.*

Радіостанція 2 (позивний Цунамі 12): *Цунамі 7, я Цунамі 12, знаходжусь на об'єкті, прийом.*

Радіостанція 1 (позивний Цунамі 7): *Залишайтесь на місці, зв'язок закінчено.*

Радіостанція 2 (позивний Цунамі 12): *Зрозумів, зв'язок закінчено*.

2. Передача інформації декільком абонентам:

Радіостанція 1 (позивний Цунамі 7): *Цунамі 10, 11, 12, я Цунамі 7, приготуватись до прийому. Цунамі 10, 11, 12, я Цунамі 7, приготуватись до прийому.*

1. ПАУЗА

Радіостанція 1 (позивний Цунамі 7): *Цунамі 10, 11, 12, я Цунамі 7, повернутися на базу.*

Радіостанція 2 (позивний Цунамі 10): *Цунамі 7, я Цунамі 10, Вас зрозумів.*

Радіостанція 3 (позивний Цунамі 11): *Цунамі 7, я Цунамі 11, Вас зрозумів.*

Радіостанція 4 (позивний Цунамі 12): *Цунамі 7, я Цунамі 12, Вас зрозумів.*

Правила проведення сеансів радіозв'язку.

❖ Говори коротко, стисло і з максирисьним змістом. Не «думай» в ефір. Перш ніж почати передачу, подумай і сформулюй що саме ти хочеш сказати, потім скороти це в кілька разів і тільки потім говори коротко, чітко і по суті.

❖ Пам'ятай, що тебе чує не тільки той, до кого ти звертаєшся, а ще багато людей. І зловмисники в тому числі. Думай якою інформацією ти можеш нашкодити собі, колегам, потерпілим і як її передати, щоб зрозумів тільки адресат.

❖ Під час передачі слова треба вимовляти чітко, не поспішаючи. При низькій якості зв'язку не можна кричати в мікрофон, це лише погіршує якість зв'язку. Інформацію в такому випадку необхідно доводити з повтором фраз, або по літерах, а числа – по цифрах.

❖ При вході в «радіопаузу» (тобто при виключенні рації або неможливості її слухати) необхідно повідомити про це на базову станцію сказавши, які позивні і приблизно на який час вийшли з ефіру. Про закінчення радіопаузи обов'язково повідомляти, командиру або в ефір [59].

Комплект приладів для контролю вмісту алкоголю у видихуваному повітрі та протоколювання результатів виміру Drager Alcotest 6820

СКЛАД КОМПЛЕКТУ

- 1 Прилад Drager Alcotest® 6810
- 2 Drager Mobile Printer
- 3 Елементи живлення, 6 штук (вставлені в прилади)
- 4 Кейс для перенесення
- 5 Місце для зберігання документів
- 6 Мундштуки, 3 штуки
- 7 Ремінь
- 8 Паперова стрічка для принтера (вставлена в прилад)

Вимірювальний прилад

1 Дисплей
2 Кнопка меню "Угору"
3 Кнопка "ОК"
4 Кнопка меню "Униз/меню"
5 Ремінь
6 Червоний/зелений/жовтий індикатор
7 Тримач для мундштука

Рис. 42

Портативний принтер

1. Кнопка вимикача
2. Світлодіод
3. Оптичний інтерфейс
4. Верхня кришка
5. ІК інтерфейс
6. Кнопка фіксатора
7. Батарейний відсік

Рис. 43

Лазерний вимірювач швидкості TruCAM для фіксації правопорушень у сфері безпеки дорожнього руху

Рис. 44

МІНІСТЕРСТВО
ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

Серія А № 006694

СЕРТИФІКАТ
затвердження типу засобів вимірювальної техніки

№ UA-MI/1-2903-2012 Виданий 29 серпня 2012 р.

Цей сертифікат, виданий фірмі Laser Technology, Inc., США, засвідчує, що на підставі позитивних результатів державних приймальних випробувань Міністерством економічного розвитку і торгівлі України затверджений тип засобу вимірювальної техніки "Вимірювач швидкості автотранспортних засобів лазерний LTI 20/20 TruCAM", який зареєстровано в Державному реєстрі засобів вимірювальної техніки за номером У3197-12.

Контроль метрологічних характеристик вимірювачів швидкості автотранспортних засобів лазерних LTI 20/20 TruCAM під час випуску з виробництва здійснює метрологічна служба виробника, акредитована національною метрологічною службою США.

Міжповірочний інтервал, установлений під час затвердження типу вимірювача, – не більше одного року.

Заступник Міністра економічного розвитку і торгівлі України – керівник апарату *В. П. Павленко*

МІНЕКОНОМРОЗВИТКУ УКРАЇНИ
Державне підприємство
«Всеукраїнський державний науково-виробничий центр стандартизації, метрології, сертифікації та захисту прав споживачів»
(ДП «УКРМЕТРТЕСТСТАНДАРТ»)
вул. Метрологічна, 4, м. Київ, 03143
Свідоцтво про уповноваження № ПК 001-2014 від 24 лютого 2014 р.

СВІДОЦТВО
про повірку законодавчо регульованого засобу вимірювальної техніки

№ 22-01/11917 Чинне до 25 вересня 2019 р.

Назва та умовне позначення *Лазерний вимірювач швидкості транспортних засобів TruCAM LTI 20/20 №* [redacted]

Виробник *Laser Technology Inc., США*

За результатами повірки встановлено, що засіб вимірювальної техніки (далі – ЗВТ) відповідає вимогам
(назва нормативно-правового акта,

Діапазон вимірювань швидкості - від 2 км/год до 320 км/год
що містить вимоги до метрологічних характеристик і значення метрологічних

Максимально допустима похибка при вимірюванні швидкості в ручному та автоматичному режимах: ± 2 км/год в діапазоні від 2км/год до 200 км/год; ± 1 % в діапазоні від 201 км/год до 320 км/год
характеристик (клас точності, похибки, діапазон вимірювання), особливості застосування ЗВТ)

Додаток: на - стор. у - прим.

Персонал, який виконував роботи з повірки (підпис) Г.В. Моторний (ініціали, прізвище)

Місце відбитка повірочного тавра 25 вересня 2018 р.

Рис. 45

Лазерний вимірювач швидкості TruCAM для фіксації правопорушень у сфері безпеки дорожнього руху

Документування правопорушень, зафіксованих за допомогою приладів, здійснюється поліцейськими згідно зі статтею 251 Кодексу України про адміністративні правопорушення та Інструкції з оформлення поліцейськими матеріалів про адміністративні правопорушення у сфері забезпечення безпеки дорожнього руху, зафіксовані не в автоматичному режимі, затвердженої наказом МВС від 07.11.2015 № 1395 [20; 45].

Місце для роботи з приладом обирається з урахуванням ділянок доріг де зареєстровано найбільшу кількість дорожньо-транспортних пригод у зв'язку із перевищенням водіями транспортних засобів швидкості руху, наведеної в таблиці нижче, а також дорожніх умов, що можуть впливати на якість фіксацій порушень Правил дорожнього руху [55].

Використання приладів у місцях, не передбачених дислокацією маршрутів патрулювання, а також таких, які не відповідають вимогам п. 2, **КАТЕГОРИЧНО ЗАБОРОНЕНО**!

Після отримання приладу поліцейський здійснює виїзд на місце несення служби, визначене дислокацією маршрутів патрулювання та натиснувши кнопку «ввімкнення/вимкнення живлення» заповнює дані на дисплеї приладу:

- ПРІЗВИЩЕ (ПІП поліцейського);
- МІСЦЕПОЛОЖЕНЯ (місце знаходження приладу);

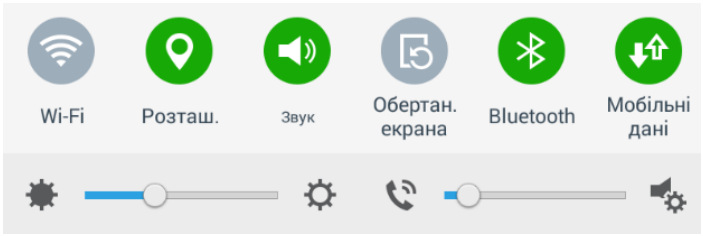
- ОСОБИСТИЙ № (жетон поліцейського);
- ОБМЕЖЕННЯ (максирисьна швидкість для легкових та вантажних автомобілів);
- ФІКСАЦІЯ ПІСЛЯ (швидкість після якої здійснюється фіксація);
- ФОТОГРАФУВАТИ НА (фотографування ТЗ, рекомендовано на відстані 70 м.) [59];
-

Рис. 46

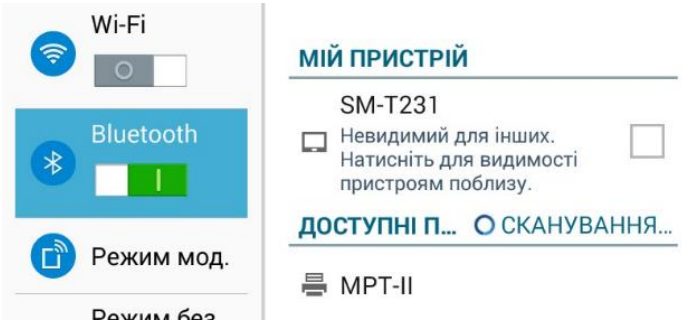
Робота з електронною постановою. Створення. Редагування. Друк.

Рис. 47

Підключення термопринтеру

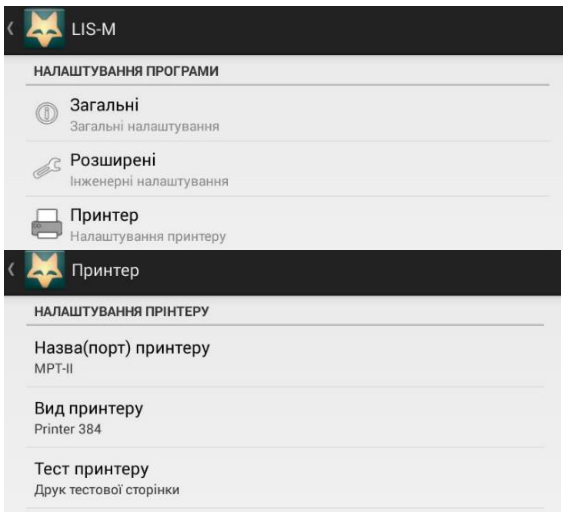


Ввімкнути Bluetooth



Підключити пристрій MPT-I та ввести пін-код «0000»

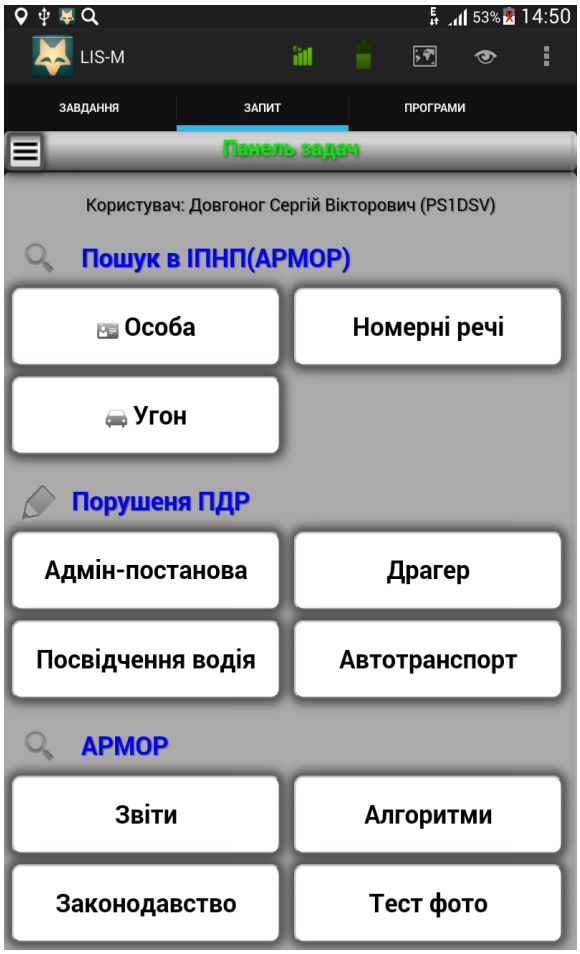
Рис. 48



Відкрити в ПЗ ЛІС-М налаштування та провести тестовий рук з термопринтеру

Рис. 49

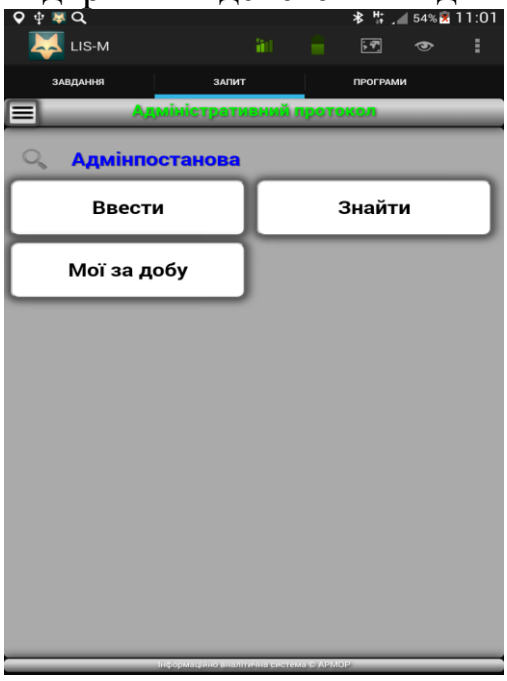
Відкриття підсистеми «Адмін-постанова»



Після успішного тестування термопринтеру та перевірки на працездатність, авторизуватись в «Запит» за допомогою особистого логіну та паролю до системи «АРМОР» та натиснути посилання «Адмін-постанова».

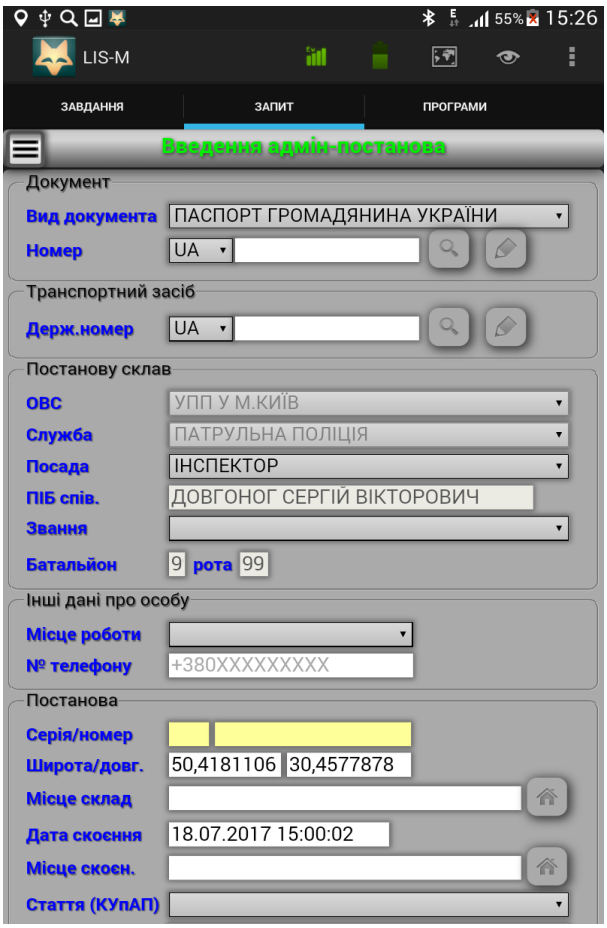
Рис. 50

Відкриття підсистеми «Адмін-постанова»



– **[Ввести]** відкриває форму введення адмінпостанови;
– **[Знайти]** дає змогу знайти раніше введену постанову;
– **[Мої за добу]** відкриває постанови, які були внесені за зміну.

Рис. 51



Введення адмін-постанови

Рис. 52

«Документ»

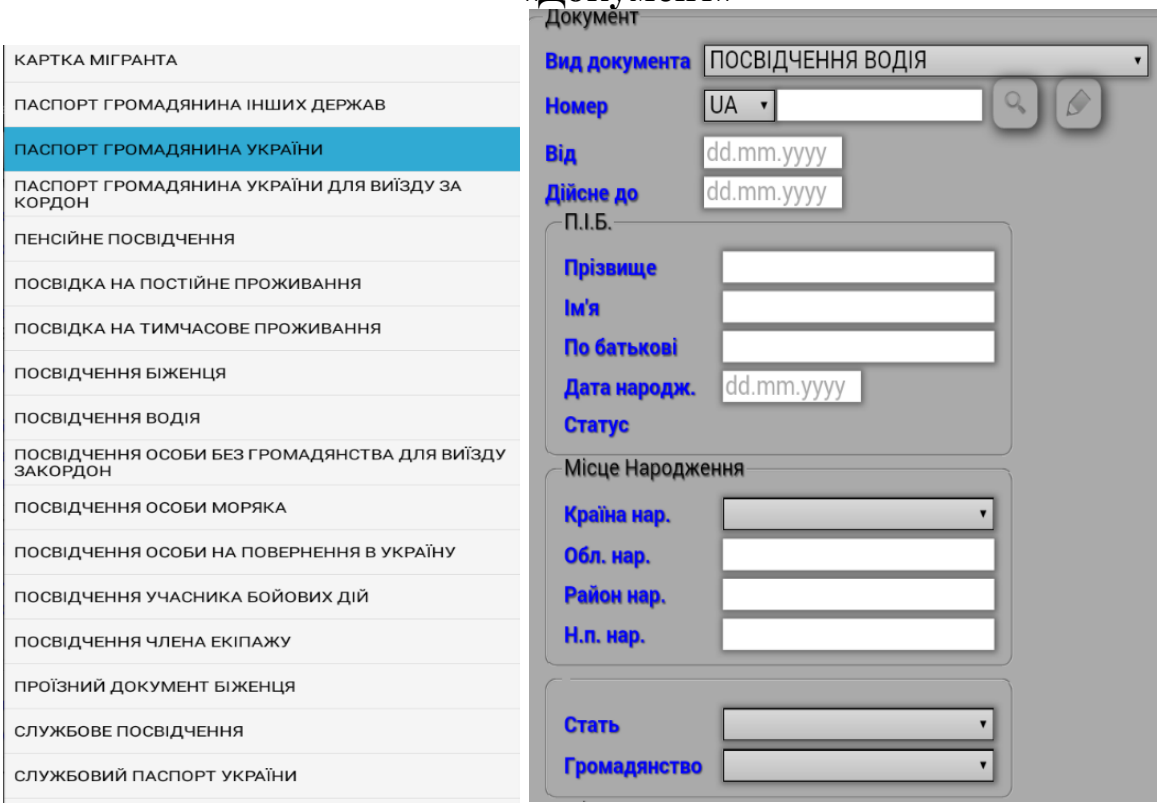


Рис. 53

Вводяться відомості про документ та особу, яку було ідентифіковано за допомогою цього документу.

Доступний вибір з випадаючого меню виду документу.

Пункт «Номер» дозволяє самостійно вказати країну походження документу [59].

При натисканні кнопки

«Посвідчення водія»

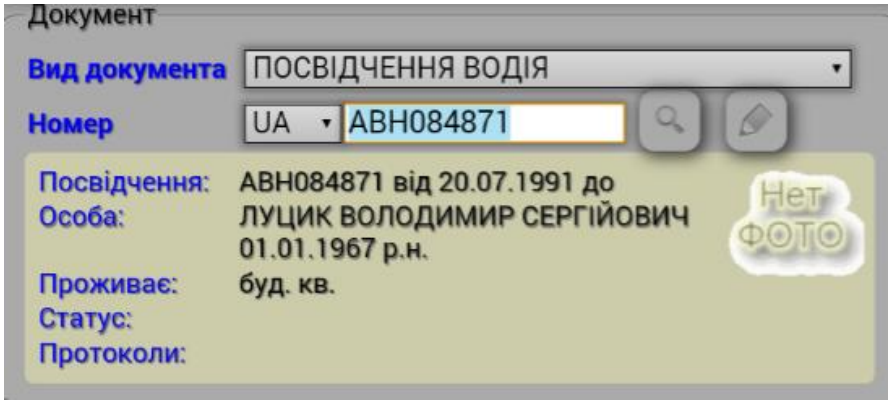
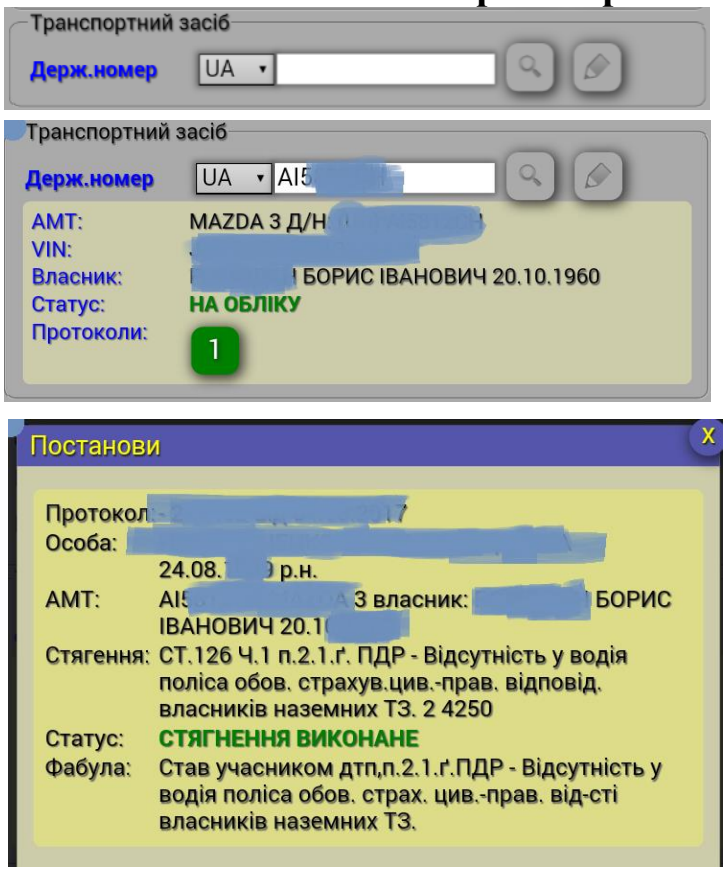


Рис. 54

Відомості про водія система знаходить самостійно при натисканні кнопки внесенні дійсного посвідчення водія.

«Транспортний засіб»

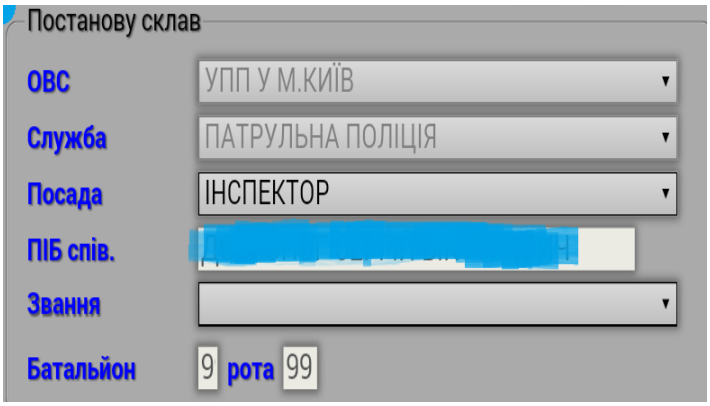


Інформація про ТЗ та про власника ТЗ заповниться автоматично при натисканні кнопки у разі, якщо транспортний засіб було поставлено на облік після 2011 року або на власника ТЗ раніше складався адмінматеріал. В цьому випадку в пункті «Протоколи» буде вказано скільки раніше було складено матеріалів.

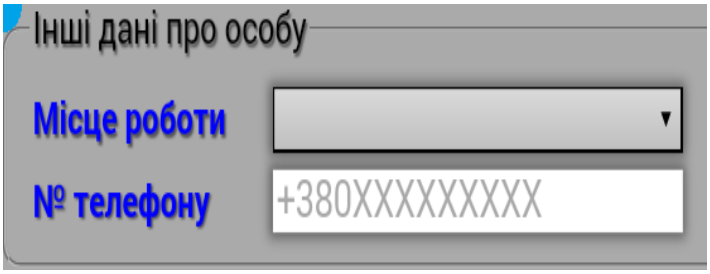
При натисканні на кількість протоколів відкриється детальна інформація.

Рис. 55

«Постанову склав» та «Інші дані про особу»

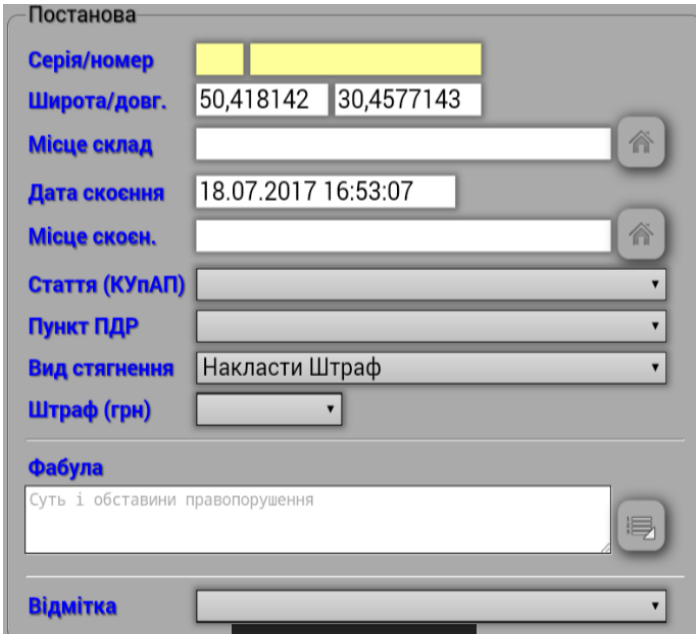


Інформація про посадову особу, яка склала адмінматеріал, вноситься автоматично за наявності достатнього обсягу інформації введеної в системі «АРМОР»



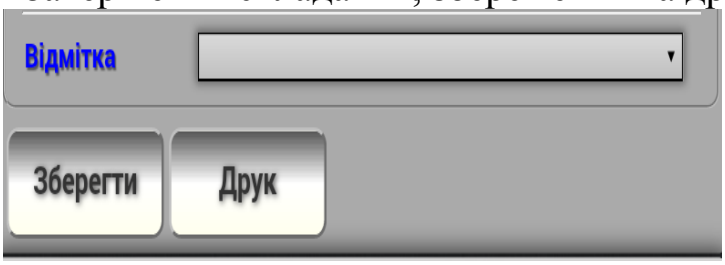
Місце роботи вноситься за наявності підстав вважати, що інформація є достовірною.

«Постанова»



Серія та номер створюються автоматично при збереженні постанови.
Місце складання формується за допомогою координат пристрою, але бажано дублювати адресом.
Місце скоєння може відрізнятися від місця складання.
Стаття КУПАП, Пункт ПДР, вид стягнення та сума штрафу обирається з випадаючого списку.
Вибір фабули стає доступним при обранні статті КУПАП, пун-

«Завершення складання, збереження та друк»



Після заповнення всіх даних та перевірки на достовірність, натиснути кнопку «Зберегти» і тільки після цього натискати «Друк»

Рис. 56

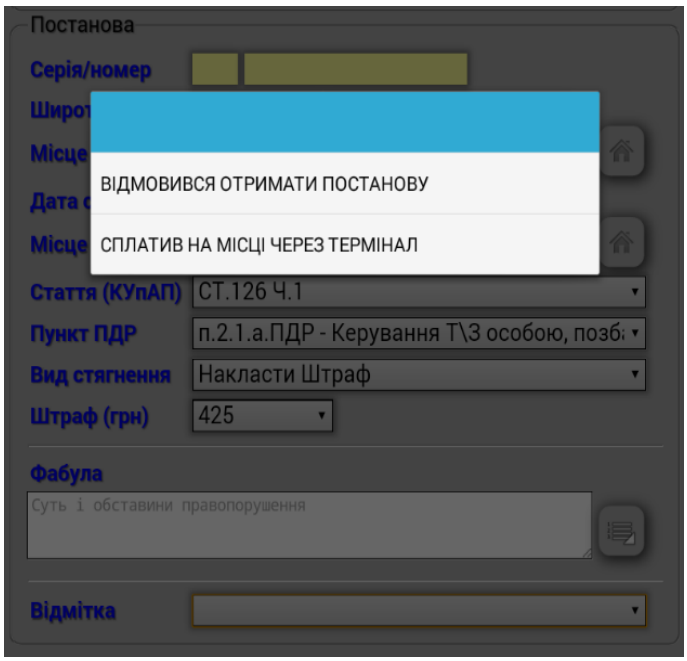


Рис. 57

В разі відмови правопорушника отримувати ЕП обов'язково зазначається в відмітці «Відмовився отримувати постанову» та роздрукована постанова передається до відділу адміністративної практики

Рис. 58

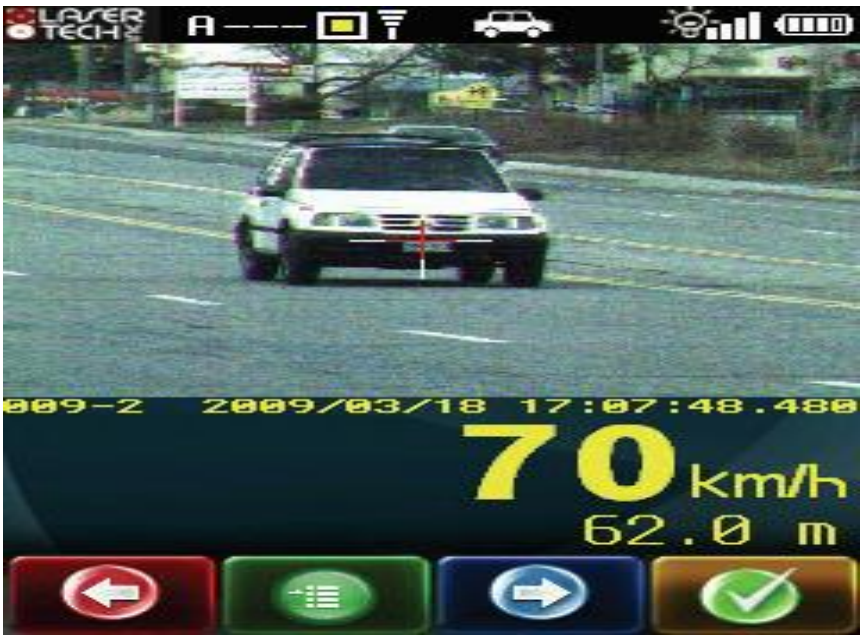


Рис. 59

- З відстані у 350-450 м виконується наведення позначки оптичного прицілу на цільовий автомобіль і натискається спусковий гачок приладу. Прилад починає вимірювання швидкості і включає запис відео, при цьому чути характерний звук низького тону.
- Якщо позначка буде стабільно утримуватись на цільовому транспортному засобі не менше ніж 3-6 секунди , то прилад здійснить вимірювання швидкості. Про фіксацію перевищення швидкості руху свідчитиме характерний звук високого тону і в самому оптичному прицілі та на екрані монітору приладу буде показано числовий показник швидкості [59].

Після закінчення несення служби поліцейський, прибувши до управління, передає прилад уповноваженій особі.

Уповноважена особа, отримавши прилад, перевіряє технічний стан приладу, вносить відмітки до журналу про дату і час здачі приладу, визначає і записує кількість зафіксованих у приладі відеокліпів на момент здачі та ставить особистий підпис.

Уповноважена особа забезпечує копіювання інформації з приладу на жорсткий диск комп'ютера та негайно, але не пізніше наступного робочого дня за допомогою спеціальної програми здійснює друк фото порушень Правил дорожнього руху. Після чого в той же термін друковані фото надсилаються до підрозділів адміністративної практики для приєднання до постанов у справах про адміністративні правопорушення. Уся інформація, яка отримана з приладу, повинна зберігатись на електронному носії впродовж 3 місяців з дня її копіювання [59].

3. Інформаційні системи, бази даних: технічні характеристики, організаційні, правові, тактичні засади їх використання працівниками патрульної поліції

Особливостями використання баз даних **працівниками патрульної поліції** є те, що вони у своїй службовій діяльності використовують наступні інформаційні підсистеми.

Інформаційна підсистема «Повідомлення «102» ІПНП.

Дану підсистему формують оператори служби «102» Управління організаційно-аналітичного забезпечення та оперативного реагування (УОАЗОР) ГУНП, оперативні чергові територіальних підрозділів поліції, працівники Управлінь патрульної поліції та груп реагування патрульної поліції (ГРПП) органів Національної поліції з планшетних пристроїв. Вносяться відомості про отримані телефонні повідомлення на спецлінію «102», які у подальшому автоматично завантажуються до ІП »Єдиний облік». Також вносяться відомості про кримінальні правопорушення та інші події, виявлені безпосередньо поліцейськими (патрульними, інспекторами-черговими тощо).

Фіксація повідомлень регламентується наказом НПУ від 13.06.2017 № 574 «Про затвердженим Інструкції про порядок запису та збереження в цифровому вигляді заяв і повідомлень, які надходять за телефоном «102» [37], або за допомогою інших засобів зв'язку до Національної поліції України». Для запису повідомлень використовується цифровий багатоканальний реєстратор мовленнєвої інформації з вмонтованим автоматичним визначником номерів телефонів та таксофонів. Запис на реєстратор виконується цілодобово з усіх робочих місць уповноважених працівників чергової служби **та** ситуаційних центрів органів поліції.

ІП «Адміністративне правопорушення»

Інформаційна підсистема «Адміністративне правопорушення» ІПНП містить відомості про вчинені адміністративні правопорушення, окрім правопорушень, пов’язаних з корупцією.

В дану підсистему інформацію вводять працівники органів Національної поліції, СУ, УВБ, УБЗПТЛ, УПД. Доступ до перегляду інформації мають всі авторизовані користувачі органів Національної поліції.

Ведення ІП «Адміністративне правопорушення» регламентує наказ МВС від 04.07.2016 № 595 «Про затвердження Інструкції з автоматизованого обліку адміністративних правопорушень» [31].

Обліку в ІП «Адміністративне правопорушення» (ІП «АПРА») підлягають відомості щодо зареєстрованих адміністративних правопору-

шень, осіб, які їх учинили, та результати розгляду цих правопорушень, окрім адміністративних корупційних правопорушень [31]. Відомості щодо зареєстрованих кримінальних та адміністративних корупційних правопорушень, осіб, які їх учинили, та результати розгляду цих правопорушень у судах підлягають обліку у ІП «Корупція».

Відомості щодо адміністративних протоколів, складених за порушення Правил дорожнього руху, уносяться підрозділами Патрульної поліції.

Інформаційна підсистема «Затримані та доставлені» ІПНП

У інформаційній підсистемі «Затримані та доставлені» ведеться облік: осіб, яких було доставлено до відділів, відділень поліції або затримано за підозрою в учиненні правопорушень (кримінальних чи адміністративних), щодо випадків адміністративного затримання осіб працівниками підрозділів Національної поліції або затримання згідно з дорученнями правоохоронних органів, або затримання осіб органами досудового розслідування, а також обліковується інформація про надання затриманим особам безоплатної вторинної правової допомоги [18; с. 47; 63, с. 29; 22].

Відомості до ІП «Затримані та доставлені» уносяться та корегуються тільки авторизованими користувачами – працівниками ЧЧ підрозділу НП, за якими наказом закріплені функціональні обов'язки щодо формування зазначеної ІП, згідно з загальним порядком формування інформаційних ресурсів ІПНП .

ІП «Гарпун»

Метою ІП «Гарпун» є:

об'єднання інформації про розшук ТЗ та номерних знаків в єдиному інформаційному просторі з використанням сучасних інформаційних технологій, комп'ютерного та телекомунікаційного обладнання;

забезпечення оперативного реагування та прийняття управлінських рішень посадовими особами органів (підрозділів) поліції щодо розшуку ТЗ та номерних знаків;

моніторинг тимчасових потоків даних про номерні знаки, що надходять із систем відеофіксації, на предмет їх розшуку, одночасного перебування на різних ТЗ (номерні знаки - двійники), використання номерних знаків, що за даними Єдиного державного реєстру Міністерства внутрішніх справ України (ЄДР МВС) знищено;

забезпечення взаємодії з державними та приватними виконавцями під час розшуку ТЗ боржника у виконавчому провадженні[18; с. 47; 63, с. 29; 22].

Облік об'єктів в ІП «Гарпун» ведеться за такими категоріями:
орієнтування про незаконне заволодіння ТЗ;
орієнтування про залишення ТЗ місця дорожньо-транспортної пригоди;
орієнтування про залишення ТЗ місця вчинення іншого правопорушення;
орієнтування оперативне про ТЗ;
евакуйовані ТЗ;
розшук ТЗ у зв'язку із незаконним заволодінням;
розшук ТЗ, що залишив місце дорожньо-транспортної пригоди;
розшук ТЗ за іншими кримінальними правопорушеннями;
розшук ТЗ боржника державним виконавцем;
розшук ТЗ боржника приватним виконавцем;
розшук викраденого номерного знака;
розшук втраченого номерного знака;
знищені номерні знаки [18; с. 48; 63, с. 28; 22].

ІП «Пізнання»

Ведення обліків ІП «Пізнання» здійснюється відповідно до вимог законодавства, які регламентують в підрозділах Національної поліції організацію розшуку безвісно зниклих осіб, осіб, які не можуть надати про себе відомості в силу хвороби або рисолітнього віку, встановлення особи невпізнаних трупів та інших категорій осіб, що розшукуються;

Обліку в ІП «Пізнання» підлягають відомості щодо безвісно зниклих осіб, невпізнаних трупів, осіб, які не можуть надати про себе відомості в силу хвороби або рисолітнього віку, та інших категорій осіб, що розшукуються.

Інформаційна підсистема введена у Інформаційний портал НП наказом НПУ від 17.05.2019 № 474 «Про заходи щодо підвищення ефективності розшукової роботи» [38].

Інформаційна підсистема «Річ» ІПНП.

Обліку в ІП «Річ» підлягають відомості щодо речей, викрадених, вилучених з ознаками підробки, заборонених або обмежених в обороті у фізичних осіб, безгосподарних, що знайдено або вилучено із камер схову вокзалів, портів, аеропортів, зданих до підрозділу НП, які мають індивідуальні заводські (фабричні) номери.

Інформаційна підсистема введена у Інформаційний портал НП наказом НПУ від 12.06.2018 № 586 «Про заходи щодо ефективного ведення автоматизованого обліку викрадених, вилучених речей, цінностей та іншого майна» [36].

Інформаційна підсистема «Втрачені документи» ІПНП

Обліку в ІП «Втрачені документи» підлягають відомості щодо викрадених, утрачених документів (бланків документів), паспортних документів померлих громадян України, не зданих до органів ДМС, паспортних документів визнаних недійсними, паспортних документів осіб, які знаходяться в розшуку, документи щодо транспортних засобів, документи з ознаками підробки, цінні папери, банківські документи та документи страхування які мають індивідуальні заводські (фабричні) номери.

Інформаційна система «Втрачені документи» регламентує діяльність відповідно до наказу НПУ від 12.06.2018 № 585 «Про заходи щодо ефективного ведення автоматизованого обліку викрадених, утрачених, вилучених документів» [35].

Інформаційна підсистема «Затримання адміністративне» ІПНП

Обліку ІП «Адміністративне затримання» підлягають відомості:

- щодо складених протоколів про адміністративне затримання;
- щодо осіб, які підлягали адміністративному затриманню [18; с. 47; 63, с. 29; 22].

Інформаційна підсистема ІП »Точки інтересів» ІПНП

В інформаційній підсистемі ведеться облік кримінологічно значимих об’єктів (церкви, ломбарди, питні заклади тощо) із застосуванням інтерактивної карти їх розміщення.

Ведення цієї підсистеми ІПНП регламентується дорученням НПУ від 29.01.2019 № 137/02/14-2019 «Про віднесення об’єктів транспортної інфраструктури до підсистеми «Точки інтересів» інформаційно-телекомунікаційної системи ІПНП» [14].

Розлянемо порядок формування інформаційної підсистеми «Точки інтересів» інформаційно - телекомунікаційної системи «Інформаційний портал Національної поліції України».

Методичні рекомендації щодо порядку формування інформаційної підсистеми «Точки інтересів» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» (далі - методичні рекомендації) є посібником користувача. Ці методичні рекомендації роз'ясняють порядок внесення інформації щодо розміщення об'єктів на мапі до інформаційної підсистеми «Точки інтересів» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» (ІП «Точки інтересів» ІТС ІПНП) для подальшого використання у роботі підрозділами Національної поліції України.

ІП «Домашній арешт»

Обліку в ІП «Домашній арешт» підлягають особи, щодо яких підрозділами Національної поліції України здійснюється виконання ухвал слідчого судді, суду про обрання запобіжного заходу у вигляді домашнього арешту та про зміну раніше обраного запобіжного заходу на запобіжний захід у вигляді домашнього арешту та щодо яких працівниками підрозділу НП здійснюється контроль за їх поведінкою [22].

В електронній картці ІП «Домашній арешт» зазначаються такі відомості:

- час поставлення на облік підозрюваного, обвинуваченого;
- особисті дані особи (прізвище, ім'я, по батькові, дата, місце народження, громадянство, серія, номер документа, що посвідчує особу, місце проживання або перебування);
- адреса житла, яке підозрюваному, обвинуваченому забороняється залишати, номер телефону;
- найменування суду, прізвище, ім'я, по батькові судді, слідчого судді, який постановив ухвалу, дата, номер ухвали;
- найменування органу досудового розслідування (суду), прізвище, ім'я, по батькові, номер телефону слідчого, який здійснює досудове розслідування, або судді, яким здійснюється судове провадження;
- номер кримінального провадження за Єдиним реєстром досудових розслідувань, стаття Кримінального кодексу України, яка передбачає покарання за злочин, у вчиненні якого підозрюється або обвинувачується особа, коротка фабула кримінального правопорушення [22].

Інформаційна підсистема «Єдиний облік» ІПНП.

У даній системі містяться відомості про отримані телефонні повідомлення на спецлінію «102», які у подальшому автоматично завантажені до ІП «Єдиний облік». Формується оперативними черговими органів Національної поліції та відповідальними від структурних підрозділів ГУНП за напрямками діяльності. Вона призначена для обробки відомостей під час прийняття та реєстрації заяв і повідомлень про кримінальні правопорушення та інші події.

Ведення інформаційної підсистеми «Єдиний облік» регламентується наказом МВС від 14.06.2019 № 508 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» [32].

Метою інформаційної підсистеми «Єдиний облік» є:

- об'єднання інформації щодо заяв і повідомлень про кримінальні правопорушення та інші події від фізичних або юридичних осіб, що

надійшли до органів поліції, в єдиному інформаційному просторі з використанням сучасних інформаційних технологій, комп'ютерного та телекомунікаційного обладнання;

- забезпечення контролю за додержанням законності під час прийняття та реєстрації заяв і повідомлень про кримінальні правопорушення та інші події;
- моніторинг стану оперативної обстановки в державі, виявлення районів зростання правопорушень для раціональної розстановки і маневрування силами та засобами органів поліції;
- забезпечення інформаційно-аналітичної підтримки діяльності поліції, спрямованої на запобігання та розкриття правопорушень;
- встановлення зв'язків між даними, що мають значення для кримінального провадження та справ про адміністративні правопорушення;
- формування статистичної звітності про результати роботи та дотримання законності органами (підрозділами) поліції під час реєстрації та розгляду заяв і повідомлень про кримінальні правопорушення та інші події [32].

Формування інформаційної підсистеми «Єдиний облік» здійснюється за допомогою програмно-технічних засобів системи «ІПНП».

Облік об'єктів в інформаційної підсистеми «Єдиний облік» ведеться за такими категоріями:

- заяви і повідомлення про кримінальні правопорушення та інші події;
- учасники кримінального правопорушення та іншої події;
- речі, документи та майно, пов'язані з учиненням правопорушення та іншою подією [32].

Інформаційна підсистема ІП «Постанови виконавчого провадження» ІПНП.

Інформаційна підсистема ІП »Органи» Інформаційного порталу Національної поліції узагальнює відомості про постанови державних виконавців щодо обмеження прав боржників у керуванні транспортними засобами та користуванні зареєстрованою зброєю.

Ведення обліку інформаційної підсистеми «Органи» здійснюється автоматично відповідно до вимог наказу МВС, МінЮст України від 31.01.2018 № 64/261/5 «Про затвердження Порядку взаємодії Міністерства внутрішніх справ України, Національної поліції України та органів і осіб, які здійснюють примусове виконання судових рішень і рішень інших органів» [33].

Інформаційна підсистема ІП «Коронавірус» ІПНП.

Інформаційна підсистема ІП «Коронавірус» Інформаційного порталу Національної поліції веде облік відомостей щодо ймовірних місць перебування (проживання) осіб, які повернулись до України через пункти перетину державного кордону та щодо яких є підозра у зараженні або підстави зараження респіраторною хворобою COVID-19.

Ведення цієї інформаційної підсистеми ІПНП регламентується дорученням МВС України від 17.03.2020 № 29/09 «Про невідкладні заходи з організації протидії поширенню гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2» [12].

Інформаційна підсистема «ДТП» ІПНП

ІП »ДТП» – облік відомостей про зареєстровані дорожньо-транспортні пригоди всіх категорій (без постраждалих, з постраждалими та унаслідок яких загинули люди).

Введення та перегляд інформації – УПП, відповідальні в органах НП, СУ додатково перегляд − СІП та доступ по заявкам ОНП, УОАЗОР, УПД, УКР, СУ ГУНП.

Ведення системи регламентується наказом НПУ від 15.06.2016 № 509 «Про ведення обліку дорожньо-транспортних пригод» та Правилами ведення обліку дорожньо-транспортних пригод [34; 39] .

Інформаційна підсистема «Драгер» ІПНП

ІП »Драгер» – облік спеціальних технічних засобів, якими здійснюється проведення огляду водіїв транспортних засобів на стан алкогольного сп’яніння, осіб, які тестуються на стан алкогольного сп’яніння, та результатів такого тестування.

Введення та перегляд інформації в підсистемі− УПП, УПД, ГРПП через планшетні пристрої.

Введення ІП »Драгер» на підставі листа ДІП КП «102» від 10.02.2017 № 27/01/9-773 [23].

Інформаційна підсистема «Затримані транспортні засоби» ІПНП

ІП »Затримані транспортні засоби» – облік відомостей про транспортні засоби, які доставлені (евакуйовані) до спеціальних майданчиків.

Введення та перегляд інформації – поліцейські УПП, ГРПП [22].

Інформаційна підсистема «Місця зберігання авто» ІПНП

ІП «Місця зберігання авто» – облік відомостей про спеціальні майданчики для зберігання транспортних засобів, які було евакуйовано у зв’язку із порушенням Правил дорожнього руху.

Введення та перегляд інформації – поліцейські УПП, ГРПП [22].

Інформаційна підсистема «Патрулі» ІПНП

ІП «Патрулі» – реєстрація даних про всі патрульні наряди поліції.

Введення – УІАП, відповідальні по ОНП, підрозділам поліції особливого призначення, перегляд УПП, УПД, УОАЗОР, ОНП)

Введена в дію на підставі СТ НПУ від 28.01.2020 № 1167/04/25-2020 «Про внесення змін до логічних умов створення та реєстрації нарядів поліції в ІПНП» [22].

Інформаційна підсистема «Логістичні пристрої» ІПНП

ІП «Логістичні пристрої» – реєстрація даних про планшетні комп'ютери та GPS-пристрої, які використовуються патрульними нарядами.

Введення інформації – УІАП ГУНП [22].

Інформаційна підсистема «Облік GPS-пристроїв» ІПНП

ІП «Облік GPS-пристроїв» – облік GPS-трекерів та транспортних засобів, на яких вони встановлені.

Введення – УІАП ГУНП, перегляд – користувачі, які працюють з електронною мапою та мають відповідний доступ.

Регламентується дорученням НПУ від 18.10.2019 № 11788/01/27-2019 [13].

Інформаційна підсистема АРМ «Диспетчер» ІПНП

АРМ «Диспетчер» –система для призначення завдань нарядам поліції для обслуговування подій, кримінальних правопорушень, а також службових завдань.

Користування – УОАЗОР, УПД, УПО, ОНП [18; 43].

Інформаційна підсистема АРМ «ЦУНАМІ-монітор» ІПНП

АРМ «ЦУНАМІ-монітор» –виведення в режимі реального часу повідомлень про скоєні правопорушення та події на території області, що введені до ІП «Повідомлення 102».

Користування – служби ГУНП, працівники чергових служб відділів поліції [18; 43].

4. Досвід використання засобів інформаційного забезпечення та технічних приладів в роботі патрульних поліцейських, проблеми, що виникають в процесі та шляхи їх вирішення

У квітні 2018 року між правоохоронними органами Харківської області, Харківською обласною державною адміністрацією та Регіональним представництвом Консультативної місії Європейського Союзу розпочалася співпраця в рамках так званої «Стратегії громадської безпеки» [62]. В основі цієї Стратегії лежить Регіональна програма забезпечення публічної безпеки і порядку та протидії злочинності на території Харківської області на 2018–2019 роки [60] . Вище зазначена співпраця охоплює шість основних пріоритетів, які були визначені громадянами Харківської області найважливішими під час соціологічного опитування 2017 року. Одним з шести основних пріоритетів є час реагування поліції. У рамках реалізації Стратегії громадської безпеки навесні 2018 року було створено міжвідомчу робочу групу, яка складається з представників Головного управління Національної поліції (ГУНП) в Харківській області, Управління патрульної поліції (УПП) у Харківській області та Харківського національного університету внутрішніх справ (ХНУВС). Однією з цілей групи є скорочення часу реагування поліції у сільській місцевості та у межах міста. З цією метою було впроваджено пілотний проєкт щодо часу реагування поліції на звернення громадян про кримінальні та адміністративні правопорушення, а також інші заходи у двох пілотних районах Харківської області. Для реалізації пілотного проєкту щодо часу реагування поліції були використані вже існуючі поліцейські структури, технічне обладнання та ІТ-інфраструктура, а також програмне забезпечення. Результати такого дослідження було відображено у відповідному звіті [16].

В рузльтаті дослідження було зроблено ряд наступних висновків. Використання планшетних пристроїв з необхідним програмним забезпеченням є зв’язувальним елементом між різними частинами ланцюга комунікації, коли йдеться про обробку екстрених викликів. Вони дозволяють диспетчерам і черговим отримувати необхідну інформацію про місцезнаходження та переміщення патрульних нарядів; вони забезпечують джерело даних для співробітників поліції шляхом надання доступу до даних, що зберігаються у базі даних. Більше того, ГРПП та також СОГ можуть негайно ділитися зібраною інформацією і доказами з іншими службовцями та підрозділами шляхом внесення таких відомостей у базу даних, використовуючи планшетні пристрої. Це не лише позитивно впливає на час реагування поліції, але й підтримує внутрішню комунікацію всередині організації

Кількість виїздів з використанням планшетів за функціональним підрозділом (ГРПП або СОГ)

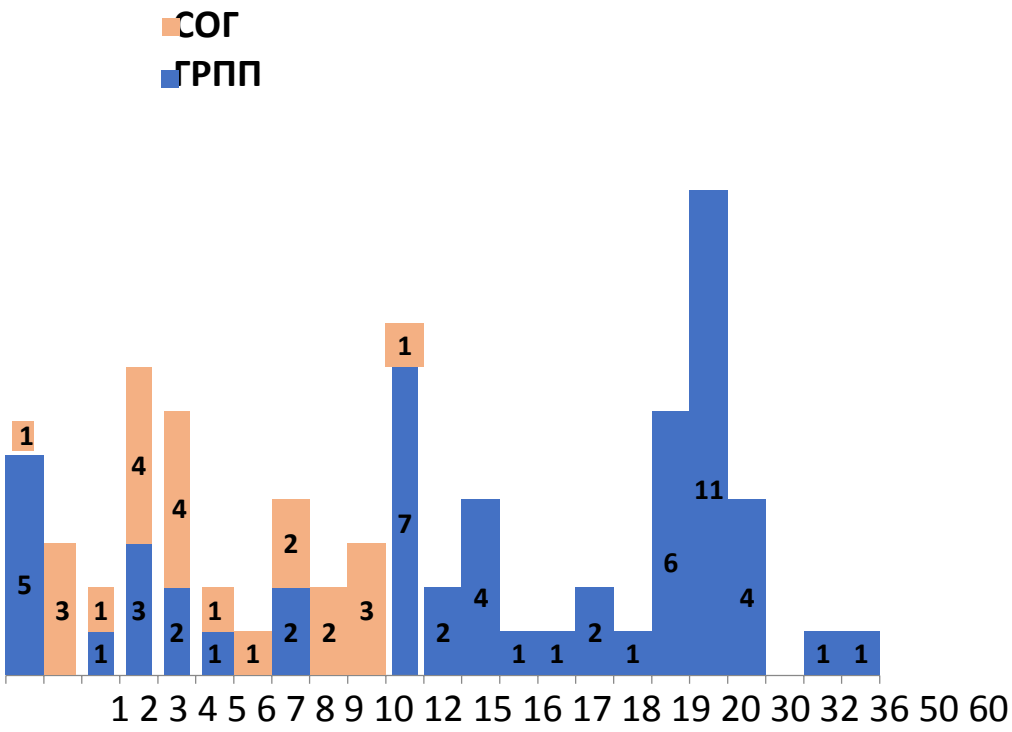
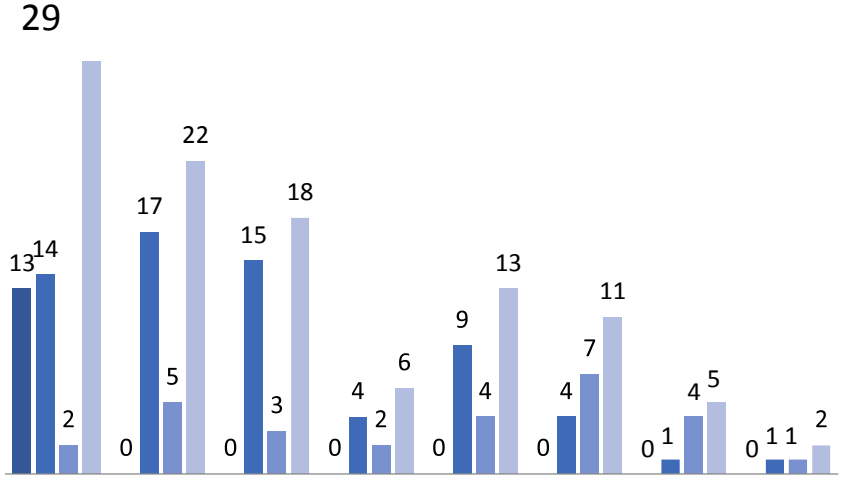
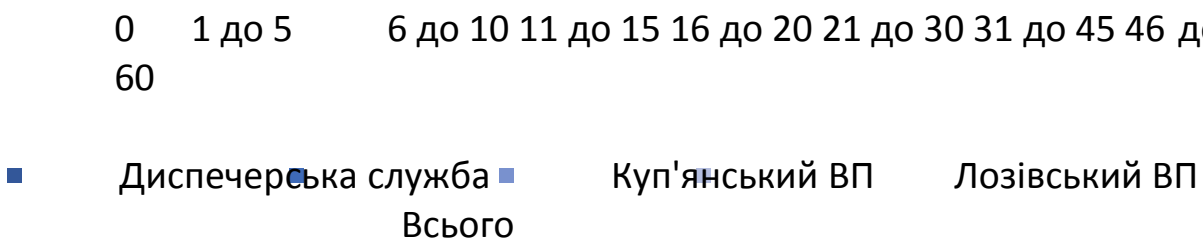


Рис. 60

З рисунку, на якому представлено кількість виїздів з використанням планшетів за функціональним підрозділом, видно, що працівники слідчих підрозділів (СОГ), використовували планшети у своїй діяльності рідше, ніж працівники ГРПП

Скільки (приблизно) разів Ви використовували планшетний пристрій під час реагування **на звернення громадян?**





З огляду на завдання та зобов’язання диспетчерської служби, її співробітники не використовують планшетні пристрої під час роботи з системою «Цунамі». 14 учасників з Куп’янська і 2 учасники з Лозової також не використовували планшетні пристрої у своїй щоденній роботі. Більшість членів ГРПП та СОГ (22 співробітника) використовували планшетні пристрої від 1 до 5 разів під час реалізації пілотного проєкту, зокрема, 18 співробітників використовували планшетні пристрої від 6 до 10 разів під час своєї зміни протягом березня та квітня 2019 року [16].

Планшетні пристрої використовувалися 16–20 разів під час змін 13 співробітниками (9 співробітників з Куп’янська та 4 співробітника з Лозової). Загалом п’ять співробітників використовували планшетні пристрої 31–45 разів протягом періоду реалізації пілотного проєкту або кожного другого дня в середньому.

Більшість опитаних працівників поліції Куп’янська та Лозової оцінюють використання планшетних пристроїв під час їх щоденної роботи позитивно (25 – дуже позитивно; 23 – досить позитивно).

Відгуки співробітників диспетчерської служби щодо впливу використання планшетних пристроїв на їх щоденну роботу також є позитивними (9 – дуже позитивні; 2 – досить позитивні). 15 учасників опитування (10 поліцейських співробітників з Куп’янська; 4 поліцейських співробітника з Лозової; 1 співробітник диспетчерської служби) не помітили жодного впливу на свою щоденну роботу під час пілотного проєкту. Лише 11 поліцейських співробітників з Куп’янська та Лозової повідомили, що використання планшетних пристроїв може мати негативний вплив на їх щоденну роботу (9 – досить негативний;

2 – негативний), і один співробітник диспетчерської служби повідомив про негативний вплив. 20 учасникам опитування було складно визначитись, який саме вплив мало використання планшетних пристроїв під час щоденної роботи.

Загалом використання планшетних пристроїв у щоденній роботі поліції Куп’янська та Лозової було оцінено опитаними учасниками проєкту позитивно. Цей також було підтверджено під час підсумкової зустрічі з керівництвом Куп’янського та Лозівського відділення поліції.

Розподіл відповідей на запитання «Як вплинуло на процес реагу-

вання використання планшетів у роботі ГРПП / СОГ?» за територіальним та функціональним підрозділом поліції представлено у таблиці та на рисунках нижче [16].

Як вплинуло на процес реагування використання планшетів у роботі ГРПП / СОГ? (кількість осіб, які вибрали певний варіант відповіді)

	Суттєво покращило роботу	**Скоріше покращило, ніж погіршило**	**Нічого не змінилось**	**Скоріше погіршило, ніж покращило**	**Суттєво погіршило роботу**	**Важко відповісти однозначно**	**Всього**
Територіальний підрозділ							
Диспетчерська служба	9	2	1	0	1	0	13
Куп'янський ВП	15	17	10	6	1	16	65
Лозівський ВП	10	6	4	3	1	4	28
Всього осіб	**34**	**25**	**15**	**9**	**3**	**20**	**106**
Всього %	**32,1**	**23,6**	**14,2**	**8,5**	**2,8**	**18,9**	**100,0**
Функціональний підрозділ							
Диспетчерська служба	10	2	1	0	1	0	14
Чергова частина	5	7	0	0	0	2	14
ГРПП	19	15	6	3	0	12	55
СОГ	0	1	8	6	2	6	23
Всього осіб	**34**	**25**	**15**	**9**	**3**	**20**	**106**
Всього %	**32,1**	**23,6**	**14,2**	**8,5**	**2,8**	**18,9**	**100**

З наведеного нижче рисунку видно, що працівники слідчих підрозділів (СОГ), надають більш негативні оцінки використанню планшетів в своїй роботі, ніж працівники патрульних підрозділів (ГРПП) та диспетчерської служби.

Розподіл відповідей на запитання «Як вплинуло на процес реагування використання планшетів у роботі ГРПП / СОГ?» за функціональним підрозділом

Рис 62

Працівники слідчих підрозділів у своїй більшості вважають що використання планшетів Скоріше погіршило або Суттєво погіршило їх роботу. В той час як працівники ГРПП та диспетчерської служби у більшості вказують на те, що їх робота Скоріше або Суттєво покращилась.

В цілому ж дані показують, що думка учасників експерименту про вплив використання планшетів на процес реагування переважно позитивна.

Розподіл відповідей на запитання «Як вплинуло на процес реагування використання планшетів у роботі ГРПП / СОГ?» в цілому

Рис. 63

Учасників проєкту попросили поділитися своїми думками та ідеями щодо поліпшення використання планшетних пристроїв та системи «Цунамі» в їх щоденній роботі. Їм було поставлено запитання «Будь ласка, поясніть, що саме покращилось». Відповіді надавались у вигляді текстових коментарів, на основі яких було визначено п’ять основних категорій позитивного впливу проєкту на діяльність ГРПП та СОГ.

Покращилося

Для інформаційного забезпечення патрульної поліції використовується програмний комплекс «Цунамі», який можна розділити на дві основні.

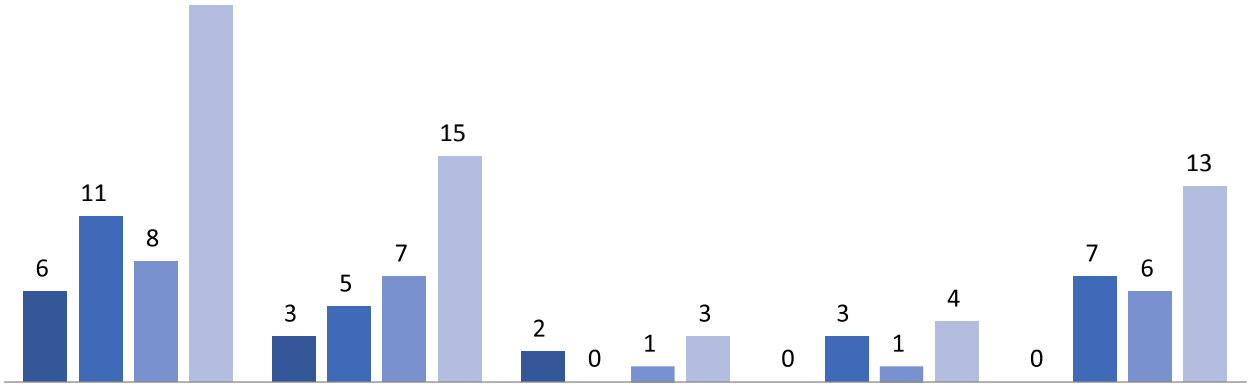
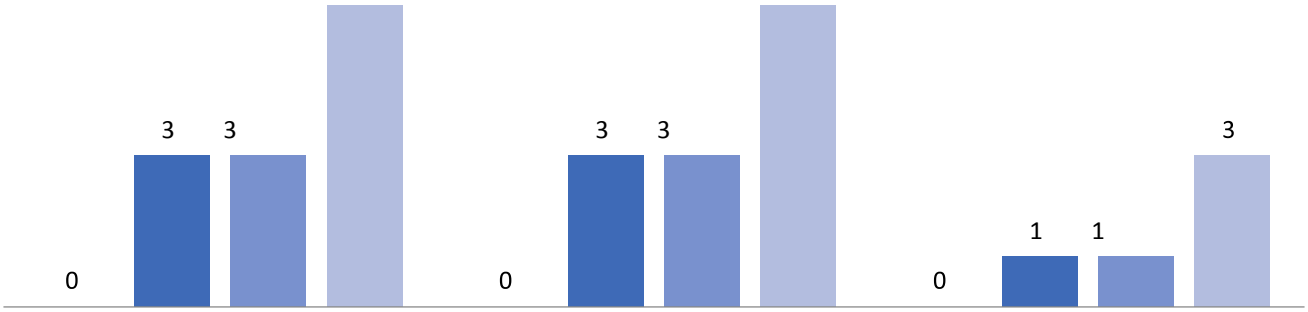


Рис. 64

Погіршилось



Зазначена інформація свідчить про необхідність проведення відповідного моніторингу в усіх областях України, а також виявляє напрями подальших наукових досліджень у сфері інформапціного забезпечення патрульної поліції.

Проблеми, які виникають при використанні оболонки «ЦУНАМІ» та шляхи її вдосконалення.

Спочатку проаналізуємо організаційно-контролюючу частину програмного комплексу «Цунамі». Патрульна поліція виконує функції підрозділу швидкого реагування у боротьбі з кримінальними та адміністративними правопорушеннями, вона повинна якнайшвидше прибувати на місце події. Час реагування на подію , як правило, складається з трьох етапів:

1) приймання повідомлення у Call центрі (служба « 102»);

2) обробка диспетчером інформації за карткою «102» та складання завдання для найближчого вільного патруля;

3) прийом завдання, прибуття на місце та реагування поліцейськими на подію [18, с. 50].

Автори навчального посібника «Інформаційні технології» зазначають, що як показують дослідження у м. Дніпро найбільш проблемною ділянкою у цьому ланцюжку є служба «102». Оператори часто не якісно та повільно збирають первинні відомості щодо події. Це пояснюється відсутність мотивації працівників Call центру , посади яких комплектуються за остаточним принципом, та як правило, з поліцейських, посади яких скорочені.

Окрім того програмне забезпечення Call центру « Цунамі» розроблено для цифрових телефонних станцій, відсутність якої в Управлінні поліції м. Дніпра ГУНП в Дніпропетровській області обмежує можливості оболонки «102» щодо он-лайн інформації про заявника та швидкості оформлення картки «102». Заповнена картка надсилається диспетчеру та черговому відділу поліції за місцем відбування події для занесення у спеціальні обліки .

Диспетчер виконує функції організаційно-інформаційного супроводження діяльності патрульної поліції і є дуже важливим елементом ефективності роботи. Як на нашу думку, необхідно розширювати інформаційну підтримку патрулів з боку диспетчерів, яким тільки два місяці тому надали доступ до Інтегрованої інформаційно-пошукової системи Національної поліції України [22].

Науковці вважають, що необхідні помічники диспетчерів для більш швидкого збирання інформації стосовно встановлених учасників та місця (адреси) відбування зареєстрованої події для подальшого надання патрульному екіпажу цієї інформації ще до його прибуття за цією адресою. Це може значно впливати на тактику поводження патрульних під час реагування на подію, підвищують ефективність їхніх дій та можливо збереже їх життя та здоров’я. Такі експерименти проводяться у Патру-

льній поліції м. Києва, де на допомогу диспетчеру надаються найбільш підготовлені патрульні поліцейські, що дуже позитивно впливає на швидкість та правильність надання завдань патрулям не за принципом найкоротшої відстані на карті, а за принципом найшвидшого прибуття на місце події. Виникає можливість закріплення за одним патрулем декілька незначних подій у одному районі почергово, що значно оптимізує використання наявних патрулів та пришвидшує час реагування на резонансні події [22].

Найбільше нарікань, з боку патрульних поліцейських, на мобільну частину комплексу «Цунамі», яка встановлена на планшетах патрульних. В усіх містах України де працюють патрульні поліції, система «Цунамі» доволі часто дає збій під час реєстрації нової зміни патрульних, яка проходить одночасно у всіх містах і сервера, які фізично розташовані у місті Київ та обслуговують всю Україну, не витримують цього великого потоку одночасної інформації. Але основні скарги на роботу «Цунамі» у патрульних поліції Дніпра викликає постійно виникаюча відсутність зв'язку з мобільним оператором «Київстар» , за допомогою стільникових мереж якого здійснюється обмін між мобільними та стаціонарними частинами комплексу. Це викликано перевантаженістю стільникових мереж оператора «Київстар» у м. Дніпро. Окрім того як вхідна так і вихідна інформація шифрується для захисту засобами мобільного оператора, що призводить до збільшення об'єму інформаційних потоків. Як вихід, пропонується надання переваги (пріоритету) сім-карткам «Київстару», які встановлені в планшети з «Цунамі». Часто виникали збої на планшетах патрульних під час оформлення звіту про виконані завдання, після яких зникала введена інформація. На теперішній момент проблема зі зникненням введеної інформації вирішена. Але виникає питання вдосконалення системи (ЦУНАМІ) при складанні звіту шляхом реалізації функції «Голосового набору», яка вже давно реалізована в ОС Андроїд. Патрульні поліцейські піднімали питання нормативно-правової підтримки їхньої діяльності в системі «ЦУНАМІ», яка була частково реалізована розробником і зараз є можливість доступу до необхідних для роботи законодавчих та нормативних актів [22].

У патрульних поліцейських міста Дніпро виникли проблеми з роботою вбудованого у «ЦУНАМІ» GPS-навігатора, який доволі часто працює дуже некоректно. Для встановлення місцезнаходження адреси події, у наданому диспетчером завданні, вони дуже часто використовують особисті гаджети.

Зазначені проблеми організаційно-контролюючого характеру в роботі мобільної частини комплексу «ЦУНАМІ» у свої більшості пов'язані з технічною підтримкою мобільного оператора «Київстар».

Але це доволі часто зводить нанівець можливості вкрай необхідної інформаційно-технічної підтримки патрульних поліцейських, що реалізована в комплексі «ЦУНАМІ». Дане питання можна вирішити тільки на рівні міністерства.

Деякі проблеми виникають і у інформаційно-пошуковій частини комплексу «ЦУНАМІ». В першу чергу патрульні поліцейські скаржаться, як вони кажуть, на «напівпусті» бази даних Інтегрованої інформаційно-пошукової системи Національної поліції України стосовно осіб, речей та транспортних засобів, що знаходяться у розшуку. Достатньо часто, коли запит по «ЦУНАМІ» не дає результату, але «шосте відчуття» поліцейського підказує, що це не так, вони звертаються до диспетчера або працівників Національної поліції, які мають доступ до ІІПС зі стаціонарних робочих місць і отримують позитивні запроси на осіб, які риси багато «стосунків» з правоохоронними підрозділами. Небагато допомагають патрульним і інформаційні обліки власників авто-, мототранспорту, які викладені у неповному обсязі [22].

Достатньо часто у патрульних поліцейських виникає необхідність наявності фото осіб, які неодноразово попадали в поле зору правоохоронців, але інформація по яким не міститься в Інтегрованій інформаційно-пошуковій системі Національної поліції. Фототеки даного континенту осіб розміщені у районних відділеннях поліції.

Відсутність можливості розміщення фото потенційних правопорушників, а точніше тих, які не були спіймані «на гарячому», у системі «ЦУНАМІ», замінюється обліком фото, та іншої необхідної службової інформації за допомогою оболонки «Viber» на особистих смартфонах поліцейських. Використання незахищених оболонок може призвести та вже призводило до витоку службової інформації. Тому виникає необхідність розміщення такої фототеки на захищеній мобільній частині комплексу «ЦУНАМІ».

Аналіз зазначених проблем з інформаційним забезпеченням патрульної поліції України та окреслені авторами можливі шляхи вирішення деяких з них, окреслюють напрями вдосконалення існуючого інформаційного комплексу «ЦУНАМІ». Посилення інформаційної підтримки патрульних поліцейських неодмінно буде впливати на якість виконаної ними роботи та поширення позитивного іміджу працівників правоохоронних структур [18, с. 50].

В.Б. Вишня вважає, що при ефективній взагалі роботі системи проявляється суттєвий недолік – відсутня можливість у диспетчера оперативно відслідковувати ход подій та дії патрульного безпосередньо при виконанні отриманого ним завдання. Тим самим виключається можливість у чергового диспетчера, в разі необхідності, втручатися в хід виконання

завдання нарядом, оперативно коригувати дії наряду, виключити випадки некваліфікованих дій патрульних. Цей науковець пропонує в основу вдосконалення системи управління нарядами мобільної патрульної служби пропонується, шляхом уведення нових зв'язків елементів, забезпечити можливість відображення у диспетчера інформації, яка попадає у поле зору об'єктива відеорегістратора патрульного. Це дозволяє диспетчеру в режимі реального часу оперативно контролювати дії патрульного поліцейського у процесі відпрацювання поставленого завдання і, за необхідності, своєчасно втручатися в його роботу, і за рахунок цього підвищити ефективність та безпеку діяльності патрульного наряду [8].

Можливі проблеми та їх усунення під час роботи з радіостанцією:

• Відбувається «спонтанний» вихід в ефір. Необхідно перевірити розташування рації на спорядженні. Обов'язково розташуйте станцію на спорядженні так, щоб ніщо випадково не могло зачепити кнопку передачі.

• Рацію включено, але не можливо провести сеанс зв'язку. Необхідно перевірити антену. Радіостанція з пошкодженою антеною працювати не буде. Для уникнення пошкодження антени не беріть портативну радіостанцію за антену – (антенна) від цього виходить з ладу

• Є проблеми з отриманням викликів під час руху. Треба перевірити розміщення рації. При перенесенні антена рації не повинна впритул прилягати до тіла, і бути по можливості вертикально спрямованою.

• Під час патрулювання в зимовий час рація швидко розряджається. В умовах низьких температур бажано тримати портативну радіостанцію в кишені або під одягом. Охолоджений до мінусових температур акумулятор розряджається значно швидше.

• Зв'язок під час сеансу поганий, абонент не чує інформацію. Необхідно перевірити правильність тримання рації. При передачі антена рації має бути спрямована вертикально. Мікрофон радіостанції, або саму станцію з вбудованим мікрофоном слід тримати на відстані близько 5 см від рота, говорити голосно і виразно, але не кричати, розбірливість це не підвищить, а знизить

• При знаходженні на далеких відстанях пропускаються виклики. Необхідно, якщо станція обладнана шумоподавлювачем який відключається, відключіть його, на граничних відстанях зв'язку це допоможе не пропустити виклик [59].

Під час роботи з радіостанцією необхідно дотримуватися певних заходів безпеки:

- Радіостанції можна встановлювати в автомобілях із заземленою мінусовою клемою акумулятора.
- Забороняється включати радіостанцію в безпосередній бли-

зькості від займистих рідин чи вибухонебезпечних приладів!

- Під час установки чи зняття з транспортного засобу мобільна радіостанція повинна бути вимкнена.
- Не можна використовувати передавач поблизу незахищених електродетонаторів чи у вибухонебезпечній атмосфері.
- Не можна дозволяти дітям гратися радіостанцією.
- Не рекомендовано використовувати радіостанцію з головним телефоном чи звуковим приладдям з високим рівнем гучності
- Не можна робити підзарядку акумулятора при температурі нижче 10°С чи вище 40°С, адже це може зменшити термін служби акумулятора.
- Заборонено використовувати зарядний пристрій, якщо він вологий чи ушкоджений.
- Заборонено розбирати акумулятор.
- Заборонено кидати акумулятори у вогонь – вони можуть вибухнути [59].

Проблеми використання нагрудних камер та напрями їх вирішення

Працівників патрульної поліції оснащено нагрудними камерами (відеореєстраторами), наявність яких розглядається ними як засіб захистити себе від упереджених заяв щодо їхньої неправомірної поведінки.

Проте, на думку деяких юристів, такий захист вступає у конфлікт із правом на приватність. Сьогодні, коли записи з цих реєстраторів публікуються самою поліцією у YouTube чи передаються у ЗМІ. Інколи вони є фрагментарними, тобто нарізкою із різних кадрів, що відображають упереджену позицію щодо людини, порушуючи презумпцію невинуватості. Крім того, правове регулювання автоматичної зйомки (тобто без згоди на це особи) є непродуманим і таким, що суперечить чинному законодавству. А саме правове регулювання є непрозорим, адже розібратись в цьому питанні шляхом вивчення опублікованої нормативно-правової бази неможливо.

Відомчі акти Національної поліції, що регулюють порядок застосування приладів, зберігання та режим доступу до відеозаписів, неопубліковані, на думку деяких юристів становить загрозу для дотримання прав людини на приватність поліцією [29].

Коли мова йде про право на приватність, наш законодавець керується поняттями »персональні дані» та «конфіденційна інформація». Відповідно *до* ст. 2 ЗУ «Про захист персональних даних», персональними даними *є «*відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована*»*. Однак чин-

ним законодавством не встановленого чіткого переліку таких відомостей, що могли б бути захищені цим Законом. Щодо конфіденційної інформації, то її визначення знаходимо *у* ч. 1 ст. 7 ЗУ «Про доступ до публічної інформації», відповідно до якої це «інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов» [51; 40].

Діяльність поліції, пов'язана із захистом і обробкою персональних даних, здійснюється на підставах, визначених Конституцією України, ЗУ «Про захист персональних даних», іншими законами України (ч. 4 ст. 25 *ЗУ* «Про Національну поліцію»). Відтак, передача відео у ЗМІ або розміщення його на відеохостингах (наприклад YouTube) є обробкою персональних даних. Така обробка, відповідно до ст. 6 ЗУ «Про захист персональних даних», не допускається без згоди особи**,** крім випадків, визначених законом**,** і лише в інтересах національної безпеки, економічного добробуту та прав людини. Саме тому, у вищезгаданій Інструкції (затв. Наказом № 100) було вжито формулювання «виключно для здійснення превенції та профілактики правопорушень з метою забезпечення національної безпеки та захисту життєво важливих інтересів людини і громадянина, суспільства і *держави*». Але це норма підзаконного акту, а Закон чітко передбачає, що такі випадки мають бути встановлені саме законом.

Відтак, сьогодні відеозаписи, отримані з відеореєстраторів і опубліковані без згоди на це особи, котра була об'єктом відеозапису, є порушенням норм Закону України «Про захист персональних даних**».** Така ситуація буде продовжуватись до узаконення (тобто вказання норми у законі) вищенаведених формулювань. Очевидно, що такі зміни мають бути внесені до Закону України «Про Національну поліцію». Основним шляхом вирішення проблеми є врегулювання суперечностей законодавчої бази з цього питання. Однак це не має бути просте узгодження правових норм без зміни концепції автоматичної відеофіксації. Враховуючи принципи прав людини, зокрема права на приватність та практику Європейського суду з прав людини (Peck v. the United Kingdom*;* Sciacca v. Italy), на наш погляд, доцільним було б застосовувати деперсоніфікацію**.** Тобто закриття обличчя особи, інформацію про П.І.Б. (зокрема озвученої патрульними), номерних знаків транспортних засобів, серії та номери документів, що посвідчують особу тощо. Крім того, мова може йти про інші особливості особи (татуювання, зачіска тощо) [30]. При цьому, така деперсоніфікація має бути здійснена ще до передачі такого відео третім особам, тобто вона має бути зроблена самою Національною поліцією України**.**

Післямова

Сьогоднішні системи управління документами, в тому числі використовувані патрульною поліцією, являють собою майже всі комп'ютерні цифрові файли. Сервіс 102 заснований на інтернет-протоколі і дозволяють обмінюватися текстовими повідомленнями, а також фотографіями і відео. Автоматизовані диспетчерські системи також є різновидом цифрових технологій. У цьому постійно мінливому світі захист інформації правоохоронних органів вимагає набагато більшого, ніж просто фізична безпека. Керівники поліції повинні дуже серйозно ставитися до кібербезпеки і усвідомлювати потенційну загрозу надання послуг громадської безпеки.

Таким чином, ми приходимо до висновків, що патрульна поліція повинна йти в ногу з технологічним розвитком і володіти необхідними знаннями та навичками для боротьби зі зростаючою цифровий злочинністю на національному, регіональному та міжнародному рівнях. Вирішення проблеми інформаційного супроводження, а саме налагодження комунікації між поліцейськими, поліпшення радіозв'язку, мобільного устаткування, забезпечення кібербезпеки патрульної поліції повинно стати пріоритетами державної політики в сфері інформаційного забезпечення правоохоронних органів України. Удосконалення законодавчого регулювання механізму пошуку, фіксації, блокування і видалення з інформаційного простору держави, зокрема, з українського сегмента мережі Інтернет, інформації, яка загрожує життю або здоров'ю громадян України, розпалює війну, міжнаціональну і релігійну ворожнечу, загрожує державному суверенітету і просуває комуністичні і / або націонал-соціалістичні (нацистські) тоталітарні режими і їх символи сприятиме також створенню в патрульній поліції України інтегрованої інформаційної системи оцінки загроз та швидкого реагування на них.

Враховуючи зазначені вище визначення та ознаки інформаційного забезпечення, вважаємо за можливе визначити наступні ознаки інформаційного забезпечення патрульної поліції: 1) цілі – задоволення інформаційних потреб патрульної поліції, забезпечення реалізації інформаційних прав поліцейських, ефективне інформаційне забезпечення функціонування патрульної поліції; 2) ресурс – інформація, вид, якість, обсяг, структура, форма, строк та носії використання якої визначаються інформаційними потребами та правами патрульної поліції; 3) зміст – неперервний процес, що складається з різних видів інформаційної діяльності працівників патрульної поліції; 4) методи – створення, використання, дослідження, зберігання, захист, передавання, обробка, знищення інформації; 5) засоби – інформаційні системи, мережі, ресурси та інформаційні технології, які використовуються в системі МВС України;

6) заходи із реалізації інформаційного забезпечення – комплекс нормативно-правових, організаційно-управлінських, науково-технічних та інших заходів; 7) суб'єкт – патрульна поліція України.

Таким чином інформаційне забезпечення патрульної поліції можна визначити як забезпечений комплексом нормативно-правових, організаційно-управлінських, науково-технічних заходів неперервний процес створення, використання, дослідження, зберігання, захисту, передавання, обробки, знищення інформації визначеного виду, якості, обсягу, структури, форми, за допомогою інформаційних систем, засобів, мереж, ресурсів та технологій, що використовуються в системі МВС України, спрямований на задоволення інформаційних потреб та реалізацію інформаційних інтересів патрульної поліції.

Ознаками кібербезпеки патрульної поліції є : 1) це стан захищеності службових інтересів патрульної поліції; 2) досягається шляхом дотримання правових, організаційних технічних вимог з використання інформаційних ресурсів, мереж, носіїв інформації, програмного забезпечення, засобів фото та відео зйомки в роботі патрульних поліцейських; 3) забезпечується спеціальними підрозділами патрульної поліції та кожним патрульним поліцейським в межах своїх функціональних обов'язків та обсягу спеціальних знань; 4) проявляється у сфері кіберпростору; 5) мета - своєчасне виявлення, запобігання і нейтралізація реальних і потенційних кіберзагроз.

Таким чином кібербезпеку патрульної поліції можна визначити як стан захищеності службових інтересів патрульної поліції у кіберпросторі, що досягається шляхом дотримання правових, організаційних, технічних вимог з використання інформаційних ресурсів, мереж, програмного забезпечення, носіїв інформації, засобів фото- та відео- зйомки в роботі патрульних поліцейських для ефективного інформаційного забезпечення функціонування патрульної поліції, своєчасного виявлення, запобігання і нейтралізація реальних і потенційних кіберзагроз.

У зв'язку із пришвидшенням процесів інформаційно-технічного удосконалення роботи патрульної поліції та збільшенням ризиків негативного впливу на функціонування її системи інформаційного забезпечення вважаємо за необхідне розробити концепцію інформаційного забезпечення патрульної поліції, що буде містити запропоновані визначення та включатиме окремий розділ про кібербезпеку патрульної поліції. Також для підвищення рівня кібербезпеки патрульної поліції пропонуємо посилити співпрацю з кіберполіцією, розробити відповідні методичні рекомендації, запровадити тренінги з питань правового забезпечення та ефективного використання баз даних, інформаційних систем, мереж, програмного забезпечення, засобів відео- та фотозйомки в роботі патрульних поліцейських.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Блінова Г.О. Інформаційне забезпечення органів публічної адміністрації в Україні: адміністративно-правові засади : монографія. Запоріжжя: Видавничий дім «Гельветика», 2019. 495 с.
2. Блінова Г.О. Понятие и содержание информационного обеспечения органов публічной администрации. Legea si Viata . 2018. № 12. С. 17–21.
3. Блінова Г.О. Правове регулювання взаємодії державних електронних інформаційних ресурсів у концепції електронного урядування в Україні. *Jurnalul juridic national: teorie şi practică*. 2019. № 5. С. 39–44.
4. Бондаренко Є.Д. Особливості інформаційного забезпечення торгівельного підприємства. Актуальні проблеми сучасної науки: п’ята Всеукраїнська науково-практична інтернет-конференція.. URL: http://intkonf.org/ bondarenko-ed.
5. Бухарев В.В. Адміністративно-правові засади забезпечення кібербезпеки України .дис на здобут наук ступ канд. юрид наук. Суми. 2018. 221 с. URL: https://core.ac.uk/download/pdf/324216462.pdf
6. Веклич В. А., Кисленко Д. П. Інформаційна безпека майбутніх фахівців поліції охорони. Наукові записки [Центральноукраїнського державного педагогічного університету імені Володимира Винниченка]. Сер. : Педагогічні науки. 2017. Вип. 159. С. 57-61. URL: http://nbuv.gov.ua/UJRN/Nz_p_2017_159_10
7. Вишня В. Б. Система централізованого управління нарядами поліції «ЦУНАМІ». Лекція. ДДУВС. 2017. 30 с. URL: http://arm.ho.ua/f1/l2.pdf
8. Вишня В. Б. Удосконалення системи управління нарядами мобільної патрульної служби Національної поліції України. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2017. № 2. С. 113-116. URL: http://nbuv.gov.ua/UJRN/Nvdduvs_2017_2_17
9. Гладун Ю., Ліпенцев А. Побудова типового центру забезпечення публічної безпеки на прикладі ситуаційного центру Головного управління Національної поліції у Львівській області. Ефективність державного управління. 2016. Аип. 4 (49). Ч. 1. URL: http://www.lvivacademy.com/vidavnitstvo_1/edu_49/fail/15.pdf
10. Данчуло А. Н. Информационно-аналитические технологи и ситуационные центры . Государственная служба . 2004. № 4. С. 65—69.
11. Деякі питання надання інформації про зареєстровані транспортні засоби, їх власників та належних користувачів: Постанова Кабінету Міністрів України від 25 березня 2016 р. № 260. Урядовий кур'єр від 07.04.2016. № 66
12. Доручення МВС України від 17.03.2020 № 29/09 «Про невідкладні заходи з організації протидії поширенню гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2»
13. Доручення НПУ від 18.10.2019 № 11788/01/27-2019
14. Доручення НПУ від 29.01.2019 № 137/02/14-2019 «Про віднесення об’єктів транспортної інфраструктури до підсистеми «Точки інтересів» інформаційно-телекомунікаційної системи ІПНП»
15. Єльцов В.О. Щодо удосконалення інформаційного забезпечення судової діяльності. Право і безпека. 2010. № 5. С. 99–103.
16. Звіт про результати реалізації пілотного проєкту щодо використання планшетних пристроїв групами реагування патрульної поліції та слідчо-

оперативними групами у Куп'янському та Лозівському районах Харківської області / Харків. нац. ун-т внутр. справ, наук.-дослід. лаб. з проблем протидії злочинності ; Голов. управління Нац. поліції в Харків. обл. ; Регіон. представництво КМЄС у м. Харкові ; [О. Сердюк, К. Бугайчук, Д. Гальченко та ін.]. Харків : ХНУВС, 2019. 60 с.

17. Інформаційне забезпечення органів Національної поліції. Лекція. Харьківський національний університет внутрішніх справ. Харків. 2019. 10 с. URL: *lib.univd.edu.ua*

18. Інформаційні технології: навч. підручник. / В.Б. Вишня, К.Ю. Ісмайлов, І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро : ДДУВС, 2020. 418 с.

19. Кібератака вірусу Petya: що відомо. URL: https://www.dw.com/uk /a-39452258

20.Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 8073-X. Відомості Верховної Ради УРСР. 1984. № 51. Стаття 1122.

21. Костенко М.Ю. Правовые проблемы налоговой тайны: дисс. ... канд. юрид. наук. М. 2002

22. Краснобрижий І.В., Прокопов С.О., Рижков Е.В. Інформаційне забезпечення професійної діяльності: навч. посіб. Дніпро : ДДУВС, 2018. 218 с.

23. Лист ДІП КП «102» від 10.02.2017 № 27/01/9-773

24. Лушер В.В. Поняття інформаційного забезпечення органів прокуратури України. Форум права. 2014. № 1. С. 338–341. URL: http://nbuv.gov.ua/UJRN/FP_index.

25. Методичні рекомендації проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції/ О.О. Акімова, О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков, Ю.І. Тюря. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2017. 37 с.

26. Міжнародний досвід протидії гібридним загрозам : законодавче регулювання та організації з питань стратегічних комунікацій: Інформаційна довідка підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України. URL: http://euinfocenter.rada.gov.ua/uploads/documents/29377.pdf

27. На сайтах поліції хакери опублікували фейки про загибель американських військових та викид радіації (оновлено). URL: https://lb.ua/society/2020/09/23/466595_saytah_politsii_hakeri.html

28. Навчальна інформаційно-технічна платформа Національної поліції в системі практичного навчання (досвід ДДУВС) / Гавриш О.С., Махницький О.В., Рижков Е.В., Прокопов С.О. Використання сучасних інформаційних технологій в діяльності Національної поліції України : матер. наук.-практ. семінару (25 листопада 2016 р.). –Дніпро : ДДУВС, 2016. – С. 34–40.

29. Нагрудна камера (відеореєстратор) патрульного: правове регулювання і порушення права на приватність. URL: http://umdpl.info/police-experts.info/2016/04/14/article-videofixation/

30. Нагрудна камера поліцейського — порушення права на приватність. URL: https://protocol.ua/ua/nagrudna_kamera_politseyskogo_porushennya_prava_na_priv

atnist/

31. Наказ МВС від 04.07.2016 № 595 «Про затвердження Інструкції з автоматизованого обліку адміністративних правопорушень»

32. Наказ МВС від 14.06.2019 № 508 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України»

33. Наказ МВС, МінЮст України від 31.01.2018 № 64/261/5 «Про затвердження Порядку взаємодії Міністерства внутрішніх справ України, Національної поліції України та органів і осіб, які здійснюють примусове виконання судових рішень і рішень інших органів

34. Наказ Національної поліції України № 509 від 15.06.2016 «Про ведення обліку дорожньо-транспортних пригод»

35. Наказ НПУ від 12.06.2018 № 585 «Про заходи щодо ефективного ведення автоматизованого обліку викрадених, утрачених, вилучених документів»

36. Наказ НПУ від 12.06.2018 № 586 «Про заходи щодо ефективного ведення автоматизованого обліку викрадених, вилучених речей, цінностей та іншого майна»

37. Наказ НПУ від 13.06.2017 № 574 «Про затвердженим Інструкції про порядок запису та збереження в цифровому вигляді заяв і повідомлень, які надходять за телефоном «102»

38. Наказ НПУ від 17.05.2019 № 474 «Про заходи щодо підвищення ефективності розшукової роботи»

39. Правила ведення обліку дорожньо-транспортних пригод: Постанова Кабінету Міністрів України від 22 травня 2019 р. № 424. Урядовий кур'єр від 28.05.2019. № 98

40. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Відомості Верховної Ради України (ВВР). 2011. № 32. Стаття 314.

41. Про затвердження Інструкції з організації діяльності чергової служби органів (підрозділів) Національної поліції України: Наказ Міністерства внутрішніх справ України 23.05.2017 № 440. URL: https://zakon.rada.gov.ua/laws/show/z0750-17#Text

42. 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: Наказ Міністерства внутрішніх справ України 27 квітня 2020 року № 357. URL: https://zakon.rada.gov.ua/laws/show/z0443-20#n7

43. Про затвердження Інструкції з організації реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України: Наказ МВС України 16.02.2018 № 111. URL: https://zakon.rada.gov.ua/laws/show/z0371-18#Text

44. Про затвердження Інструкції з організації реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України: Наказ МВС від 16.02.2018 № 111

45. Про затвердження Інструкції з оформлення поліцейськими матеріалів про адміністративні правопорушення у сфері забезпечення безпеки дорожнього

руху, зафіксовані не в автоматичному режимі. Наказ Міністерства внутрішніх справ України 07.11.2015 № 1395. URL: https://zakon.rada.gov.ua/laws/show/z1408-15#Text

46. Про затвердження Інструкції про порядок зберігання, видачі, приймання, використання нагрудних відеокамер (відео реєстраторів) працівниками патрульної поліції та доступ до відеозаписів з них. Наказ Департаменту патрульної поліції національної поліції України № 100 від 03.02.2016 року

47. Про затвердження Положення про Департамент патрульної поліції : Наказ МВС №73 від 06.11.2015

48. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів: Постанова Кабінету Міністрів України від 14 листопада 2018 р. № 1024. Урядовий кур'єр від 12.12.2018. № 235.

49. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: Наказ Міністерства внутрішніх справ України 03.08.2017 № 676. https://zakon.rada.gov.ua/laws/show/z1059-17#Text

50. Про затвердження Порядку надання Міністерством внутрішніх справ України інформації з Єдиного державного реєстру про зареєстровані транспортні засоби та їх власників Національному агентству з питань запобігання корупції: Наказ Міністерства внутрішніх справ України 21 серпня 2018 року № 689, Рішення Національного агентства з питань запобігання корупції 21 серпня 2018 року № 1843. Офіційний вісник України від 02.10.2018. 2018 р. № 75. стор. 67. стаття 2518. код акта 91570/2018

51. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI (у редакції від 19.10.2017). Відомості Верховної Ради України. 2010. № 34. Стор. 1188. Стаття 481.

52. Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Директива Європейського Парламенту і Ради від 6 липня 2016 року № 2016/1148. Офіційний вісник Європейського Союзу від 19.07.2016 — 2016 р., / L 194 /, стор. 1

53. Про Національну поліцію: Закон України від 2 липня 2015 року № 580-VIII Відомості Верховної Ради. 2015. № 40-41. ст.379

54. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Голос України від 09.11.2017. № 208

55. Про Правила дорожнього руху. Постанова Кабінету Міністрів України від 10 жовтня 2001 р. № 1306. Офіційний вісник України від 26.10.2001. 2001 р. № 41. стор. 35. стаття 1852. код акта 20133/2001

56. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020. Урядовий кур'єр від 16.09.2020. № 179

57. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 року № 96/2016. Урядовий кур'єр від 18.03.2016. № 52.

58. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. Урядовий

кур'єр. 2018. № 88.

59. Прокопов С.А. Правила радіообміну. Порядок встановлення та ведення радіозв'язку між двома абонентами. Циркулярний радіозв'язок. Персональний відеореєстратор, його функції та можливості. Відеофіксація під час службових обов'язків. Лекція до теми №11. 2020.

60. Регіональна програма забезпечення публічної безпеки і порядку та протидії злочинності на території Харківської області на 2018–2019 роки : затв. рішенням Харків. обл. ради від 01.03.2018 № 656-VII : зі змін., внес. рішенням обл. ради від 07.06.2018 № 734-VII, 30.08.2018 № 783-VII, 28.02.2019 № 925-VII. URL: http://www.oblrada.kharkov.ua/uploads/docs/
Regional_programs/38_publicna_bezpeka/_656-VII_program.doc. *5*

61. Ситуативні центри органів державної влади : наук. розроб. / авт. кол. : А. І. Семенченко, І. В. Клименко, А. В. Журавльов [та ін.] ; за заг. ред. д-ра н. держ. упр., проф. А. І. Семенченка. К. : НАДУ, 2013. С. 3.

62. Стратегічні напрями забезпечення публічної безпеки і порядку на території Харківської області на 2018–2019 роки : затв. рішенням Харків. обл. ради від 07.12.2017 № 557-VII. URL: http://www.ts.lica.com.ua/ b_text.php?type=3&id=18422&base=77.

63. Текст лекції з навчальної дисципліни «Інформаційні технології». Система централізованого управління нарядами поліції «Цунамі» / уклад. Т.П. Колісник, Д.І. Євстрат. Харків: ХНУВС, 2019. 31 с. URL: http://lib.univd.edu.ua/?controller=service&action=downloadRep&id=118127

64. Текст лекції з навчальної дисципліни «Інформаційне забезпечення професійної діяльності». Система централізованого управління нарядами поліції «Цунамі» / уклад. Т.П. Колісник. Харків: ХНУВС, 2019. URL: 30 с. http://lib.univd.edu.ua/?controller=service&action=downloadRep&id=120215

65. Текст лекції з навчальної дисципліни «Інформаційні технології». Робота з базами даних, використання радіозв'язку та відео фіксації у роботі патрульного поліцейського / уклад. Т.П. Колісник, Д.І. Євстрат. Харків: ХНУВС, 2019. 34 с. URL: http://lib.univd.edu.ua/?controller=service&action=downloadRep&id=119580

66. Шлома Г.О. Адміністративно-правове забезпечення службової таємниці в органах внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.07. Дніпропетр. держ. ун-т внутр. справ. Д., 2008. 20 с. С. 15.

67. Шлома Г.О. Адміністративно-правове забезпечення службової таємниці в органах внутрішніх справ України: дис. ... канд. юрид. наук: 12.00.07. Дніпропетр. держ. ун-т внутр. справ. Д., 2008. 286 с. С. 69

68. Шорохова Г.М. Використання інформаційних технологій в діяльності Національної поліції України. VIII Міжнародна науково-практична конференція НАНР Економіко-правові виклики 2017 року (14 січня 2017 року). Львів: НАНР-Національна академія наукового розвитку, 2017. Том 2 296с. С.274-278

69. Action Plan on Strategic Communication. URL: http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf

70. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http:.eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ENм

Навчальне видання

Бочковий Олексій Васильович
Блінова Ганна Олександрівна
Прокопов Сергій Олександрович
Мамедова Єльміра Алагамівна

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПАТРУЛЬНОЇ ПОЛІЦІЇ

Методичні рекомендації

Підп. до друку 22.04.2021 р. Формат 60х84/16. Гарнітура – Times.
Друк трафаретний (RISO), цифровий. Папір офісний. Ум.-друк. арк. 6,50. Тираж 50 прим.

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49000, м. Дніпро, просп. Гагаріна, 26, rvv_vonr@dduvs.in.ua
Свідоцтво суб'єкта видавничої справи ДК № 6054 від 28.02.2018