ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА
ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА ІМЕНІ ЛЕОНІДА ЮЗЬКОВА
ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ
Кафедра публічного управління та адміністрування

МАГІСТЕРСЬКА РОБОТА

на тему: *«***Механізми взаємодії кіберполіції з громадою***»*

Виконала: студентка магістратури за спеціальністю
281 Публічне управління та адміністрування
денна форма навчання
Волошина Тетяна Василівна

Керівник: Требик Людмила Петрівна,
доцентка кафедри публічного
управління та адміністрування,
кандидатка наук з держ.упр.,
доцентка

Рецензент:

Хмельницький – 2022 рік

АНОТАЦІЯ

Волошина Тетяна Василівна. Механізми взаємодії кіберполіції з громадою. – Рукопис.

У магістерській роботі запропоновано напрями покращення механізмів взаємодії кіберполіції та громади.

Було розкрито зміст поняття «інформація», «кібербезпека», «кіберзлочин», «кіберпростір» та «кібергігієна». Автором описано нормативно-правове забезпечення взаємодії кіберполіції та громади.

Встановлено, що на сучасному етапі в Україні взаємодія кіберполіції знаходиться на досить низькому рівні.

Доведена необхідність удосконалення механізмів взаємодії кіберполіції та громади.

Обґрунтовано, що використання концепції «community policing» покращує взаємодію кіберполіції та громади і допомагає розкриттю кіберзлочинів.

Ключові слова: інформація, кіберполіція, кібербезпека, кіберзлочин, кіберпростір, кібергігієна, механізми взаємодії кіберполіції та громади, рівень взаємодії кіберполіції та громади.

Summary

Voloshyna Tetyana Vasylivna. Mechanisms of cyberpolice interaction with the community. - Manuscript.

The master's thesis suggests ways to improve the mechanisms of interaction between cyber police and the community.

The meaning of "information", "cybersecurity", "cybercrime", "cyberspace" and "cyberhygiene" was revealed. The author describes the legal support of cyberpolice and community interaction.

It is established that at the present stage in Ukraine the interaction of cyberpolice is at a rather low level.

The need to improve the mechanisms of interaction between cyber police and the community has been proven.

It is substantiated that the use of the concept of "community policing" improves the interaction of cyberpolice and community and helps to detect cybercrime.

Key words: information, cyberpolice, cybersecurity, cybercrime, cyberspace, cyberhygiene, mechanisms of cyberpolice and community interaction, level of cyberpolice and community interaction.

ЗМІСТ

ВСТУП

Актуальність теми. На сучасному етапі взаємодія кіберполіції та громади є важливим інструментом і засобом запобігання кіберзлочинам, допоміжним засобом розкриття таких злочинів, а також основою раціонального та ефективного використання часу правоохоронними органами. Реформування Національної поліції, яке розпочалось у 2015 році і не закінчилось і досі, залишає за собою ряд важливих питань та невирішених проблем. До числа таких можна віднести і аспект взаємодії кіберполіції та громади. Гостро постає питання про існування як такого механізму взаємодії кіберполіції та громади, що є досить важливим елементом функціонування системи кібербезпеки держави. Роль кібербезпеки передбачена в Стратегії кібербезпеки України на 2021-2025 роки, в якій визначено, що кібербезпека є одним із пріоритетів у системі національної безпеки України. Реалізація відповідного пріоритету здійснюватиметься шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам в сучасному безпековому середовищі. Правову основу кібербезпеки в нашій державі становлять своїми положеннями Конституція України, що визначає забезпечення кібербезпеки однією з найголовніших функцій держави, Закон України «Про основи національної безпеки», Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та Закон України «Про основні засади забезпечення кібербезпеки України».

Тобто для ефективного функціонування національної системи важливими є її елементи, одним з яких ми визначили саме взаємодію кіберполіції та громади, що на нашу думку є одним з найбільш ефективних засобів підвищення результатів функціонування Національної поліції як інституту держави, що покликаний забезпечити охорону прав і свобод, законних інтересів людини і громадянина.

Формування дієвого механізму, який дозволить взаємодіяти кіберполіції з громадянами, державним та приватним сектором – це шлях до підвищення рівня довіри Національної поліції України як до дієвого інституту, здатного стояти на захисті прав і свобод кожного громадянина, будуючи при цьому демократичне громадянське суспільство.

Оцінка сучасного стану наукової розробки. На сучасному етапі тема взаємодії Національної поліції та громади знайшла своє відображення в наукових дослідженнях вітчизняних вчених, її розглядали у різних аспектах, здебільшого праці стосувалися тематики взаємодії поліцейських офіцерів з громадами, питанню кіберполіції присвячено малий обсяг досліджень, що пов'язано на нашу думку, з відносно не довгим функціонуванням нового органу. Тому зазначена тема потребує більш детального аналізу та вивчення.

Тема взаємодії поліції з громадою часто знаходиться в полі зору науковців, що розглядають її в досить різних аспектах. Її розглядали такі науковці як: Назар Ю.С., К.Л. Бугайчук, В.А. Гузь, І.О. Святокум, В.В. Чумак та багато інших.

Але враховуючи, що Департамент кіберполіції Національної поліції створений у жовтні 2015 року і продовжує своє становлення, ще не усі проблематичні питання є вирішені , тому на сьогодні ця тема є не досить досліджуваною та потребує нових наукових розробок.

Метою даного магістерського дослідження є розгляд теоретичних засад здійснення взаємодії кіберполіції та громади, аналіз механізмів взаємодії кіберполіції з громадою, їх характеристика та визначення напрямів покращення взаємодії кіберполіції та громади.

Відповідно до поставленої мети, у магістерській роботі виконуються наступні **завдання:**

- дослідити основні поняття та особливості взаємодії кіберполіції та громади;
- охарактеризувати нормативно-правове забезпечення механізмів взаємодії кіберполіції та громади;
- здійснити аналіз основних показників роботи Департаменту кіберполіції за 2017-2020 рр.;
- охарактеризувати механізми взаємодії кіберполіції та оцінку рівня взаємодії громадянами;
- дослідити шляхи вдосконалення механізмів взаємодії кіберполіції з громадою;

- описати впровадження концепції «community policing» у взаємодії кіберполіції та громади.

Об'єктом дослідження у магістерській роботі є система суспільних відносин між кіберполіцією та громадою.

Предметом магістерської роботи є механізм взаємодії кіберполіції з громадою та його особливості.

Відповідно до мети та завдань дослідження, у роботі використано сукупність загальнонаукових та спеціальних методів і прийомів наукового пізнання. Діалектичний метод дозволив дослідити зміст та особливості взаємодії кіберполіції з громадою, її взаємозв'язку з іншими поняттями (підрозділ 1.1). За допомогою нормативно-правового методу нами було виконано аналіз законодавства, яке регулює відносини у сфері кібербезпеки (підрозділ 1.2). Системний підхід надав можливість здійснити комплексне дослідження механізму взаємодії поліції з громадою, окреслити шляхи удосконалення зазначеного питання (підрозділ 2.2, 3.2). Порівняльний аналіз фактів щодо взаємодії поліції та громади європейських країн, їх синтез надав можливість дослідити ґенезу правового регулювання цієї сфери в зарубіжних країнах (підрозділ 3.1.), виокремити основні сучасні тенденції, можливість їх застосування в органах Національної поліції України.

Практичне значення результатів. Отримані в дисертаційному дослідженні положення, висновки та пропозиції можуть бути використані:

у правотворчості – реалізація пропозицій, сформульованих у магістерській роботі, буде сприяти вдосконаленню правового регулювання відносин у сфері взаємодії кіберполіції та громади ;

у науково-дослідній діяльності – матеріали магістерської можуть слугувати подальшому опрацюванню і вирішенню проблем, пов'язаних з взаємодією кіберполіції та громади.

Апробація результатів магістерської. Основні положення роботи, теоретичні та практичні висновки, результати дослідження були оприлюднені у доповідях на науково-практичній конференції «X Всеукраїнська науково-практична конференція «Становлення та розвиток місцевого самоврядування в Україні»».

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ЗДІЙСНЕННЯ ВЗАЄМОДІЇ МІЖ КІБЕРПОЛІЦІЄЮ ТА ГРОМАДОЮ

1.1. Основні поняття та особливості взаємодії поліції та громади

Розгляд сучасного стану взаємодії кіберполіції та громади є не можливим без визначення основних понять, які входять до цього процесу. Саме тому важливо розглянути основні елементи процесу та охарактеризувати їх взаємозв'язок, щоб в подальшому зрозуміти суть та зміст взаємодії поліції та громади.

Інформація виступає на сучасному етапі основною складовою інформаційного суспільства, та її роль важко переоцінити. Відверто кажучи, інформація інтегрується в усі напрямки діяльності держави, суспільства, громадянина [5, с.1-2]. В даний час інформація є сильним важелем і навіть стає майже фізичною відчутною силою. Визначення поняття «інформація» знайшло своє місце у багатьох наукових працях (Додаток А). Доцільним визначенням на наш погляд, поняття інформації є Законом України «Про інформацію», який говорить, що інформація – це будь які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [28].Специфіку правового регулювання суспільних відносин щодо інформації зумовлюють її низка властивостей:

- здатність до тиражування;
- незалежність прав на матеріальний носій та саму інформацію;
- фізична невідчужуваність інформації;
- необхідність відособлення.

Доцільно зауважити, що саме інформація є базовою складовою кібербезпеки будь якої держави.

На сьогодні існує багато різних наукових підходів і офіційних дефініцій щодо визначення поняття «кібербезпека», що відображають сутність кібербезпеки з різних сторін та під різними кутами зору (Додаток Б), на нашу думку саме в повному обсязі характеризує поняття кібербезпеки таке визначення : «Кібербезпека – певний стан систем, за якого нейтралізуються загрози цілісності, доступності або конфіденційності даних, які поширюються в інформаційних системах». На нашу

думку це визначення є досить незрозумілим, насамперед через відсутність пояснення, про яку систему саме йдеться. Також під кібербезпекою пропонується розуміти окремий випадок інформаційної безпеки, поява якого зумовлена використанням телекомунікаційних мереж та комп'ютерних систем [2].

Науковцями в рамках своїх досліджень для об'єднання явищ пов'язаних з умовами забезпечення захищеності від політичних, фізичних, духовних, емоційних, освітніх, професійних, психологічних та інших видів впливів, а також аварійних наслідків, помилок, нещасних випадків, пошкоджень, шкоди та інших подій, що відбуваються в кіберпросторі, що визнаються небажаними, запропоновано використання терміну «кібербезпека», що й відповідно закріплено в Міжнародній організації стандартизації під кодом «ISO/ IEK 27032 2012».

У цьому стандарті не подається весь обсяг заходів щодо ефективного захисту кібербезпеки. Однак він дає чітке розуміння зв'язку терміна cybersecurity (кібербезпека) з network security (мережевою безпекою), application security (прикладної безпекою), Internet security (Інтернет - безпекою) та critical information infrastructure protection (безпекою критичних інформаційних інфраструктур) з точки зору західних фахівців. У стандарті наводиться ось така схема, яка візуалізує зв'язок різних термінів (рис.1.1).

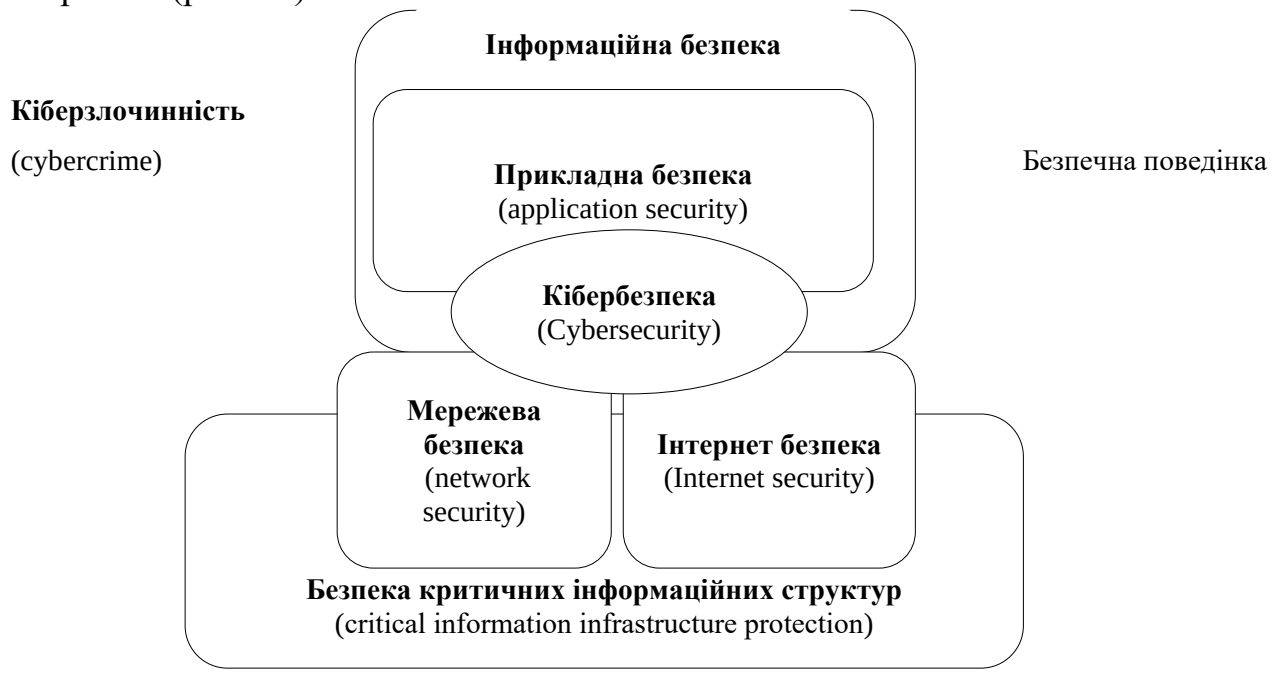

Рисунок 1.1 Взаємозв'язок між кібербезпекою та іншими сферами безпеки [3]

І відразу стає зрозуміло, що кібербезпека, і так нам звична інформаційна безпека – це зовсім не одне і теж. І безпека критичних інформаційних інфраструктур, хоч і пов’язана з кібербезпекою (так як її розуміють в усьому світі), але тільки частково. Кіберзлочинність (cybercrime) ж взагалі стоїть окремо і не має ніякого відношення ні до інформаційної безпеки, ні до кібербезпеки. Також як і поняття cybersafety, яке в Україні не має прямого і ємного перекладу, але сенс його такий – безпечна поведінка в кіберпросторі і, в першу чергу, захист дітей від негативної інформації в мережі Інтернет [7, с.130].

Стаття 1 Закону України «Про основні засади забезпечення кібербезпеки» [34] вказує, що кібербезпека – це 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.

Проблеми кіберзлочинності розглядали у своїх роботах Д.С. Азаров, Ю.М. Батурин, М.В. Карчевський, А.А. Музика, Н.А. Савінова, Є.Д. Скулиш, М.В. Рудик, К.В. Юртаєва та інші (Додаток В). Проте розвиток суспільних відносин та законодавства у цій сфері обумовлює необхідність подальших досліджень, спрямованих, зокрема, на уточнення поняття кіберзлочину.

Довгий час поняття кіберзлочину було суто кримінологічним, адже визначення цього терміну у законодавстві не наводилося. Але ситуація змінилась у зв’язку з прийняттям Закону України «Про основні засади кібербезпеки України» [34] від 05.10.2017 № 2163-VIII, у статті 1 якого наводиться наступне визначення: кіберзлочин (комп’ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. До особливостей усіх кіберзлочинів відносять:

- відсутність взаємодії злочинця із жертвою чи певними матеріальними речами;

- короткий термін часу вчинення злочину та ретельно заметені сліди;
- свій особливий алгоритм вчинення злочину;
- відсутність фактичного місця злочину, адже таким місцем є кіберпростір;
- можливість множинності об’єктів злочину;
- спеціальне знаряддя злочину-комп’ютерна техніка.

Кіберзлочин - це один із найскладніших злочинів для розслідування і для його розкриття необхідна наявність спеціалізованої техніки, та фахівців в сфері IT-технологій.

Система кібербезпеки - комплекс узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом в кібернетичному просторі для забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [6,с.38-39]. Певні особливості та відмінності можуть бути знайдені в кожній системі кібербезпеки, адже кожна з них у певному сенсі є унікальною. Науковці, що досліджували питання системи кібербезпеки, визначають чотири аспекти унікальності системи кібербезпеки, а саме:1) заохочувані дії; 2) драйвери; 3) середовище та 4) аудиторія [3].

Сьогодні безпека роботи з інформацією, як ніколи, є актуальною. Зростаючі кібератаки на державні та приватні підприємства, установи й організації тільки посилюють цей тренд. Окрема категорія загроз стосується громадян, які все частіше стають об’єктом прискіпливої уваги правопорушників. Враховуючи викладене, поступово набуває поширення відносно нова концепція необхідності самостійного дотримання користувачами елементарних правил безпеки. Такий підхід дає змогу значно посилити систему колективної безпеки суспільства та держави в цілому. Агентство Європейського Союзу з мережної та інформаційної безпеки (European Union Agency for Network and Information Security) зазначає, що кібергігієна повинна розглядатися так само, як особиста гігієна, і, після належної інтеграції в організацію, має стати простою повсякденною процедурою, яка забезпечить оптимальний стан кіберздоров’я організації. Навіть великі держави можуть зазнати величезної шкоди від необачного ставлення до вимог безпеки однієї людини. Часто порушники

використовують окрему особу як лаз для проникнення на об’єкти критичної інфраструктури, викрадення чутливих державних даних, створення умов для скоординованих повномасштабних атак.

У світі існує достатньо велика кількість тлумачень слова «кібергігієна». Вони, як правило, відображають найбільш значущі аспекти цього терміна, важливі для конкретної галузі знань. Серед останніх оприлюднених визначень можна навести такі:

- правила кібербезпеки, яких мають дотримуватися онлайн-користувачі з метою забезпечення цілісності та убезпечення своїх персональних даних на мережних пристроях від компрометації у випадку кібератаки;
- сукупність практик, спрямованих на захист від негативного впливу на певні об’єкти ризиків, пов’язаних з кібербезпекою;
- способи заохочення користувачів комп’ютерних технологій до безпечної поведінки в інтернеті.

Більш спрощена інтерпретація цього терміну дозволяє представити кібергігієну як дотримання правил безпечної поведінки у кіберсфері [43,с.6].

В умовах децентралізації влади з’явилася необхідність переходу від традиційно жорсткої поліцейської моделі до моделі реалізації сервісно-орієнтованої концепції забезпечення потреб громади через налагодження комунікацій (взаємодії) поліції, органів місцевого самоврядування та населення, яка отримала назву “community policing” або “community-oriented policing”

Community policing – правоохоронна діяльність, яка спрямована на потреби місцевої громади.

Дана стратегія передбачає збільшення участі громади у прийнятті рішень, а також спрямованість роботи поліції на потреби відповідної громади. Тобто це означає робота «разом з громадою», а не для громади. Відповідно ми бачимо принцип партнерства, який вказаний в ЗУ «Про Національну поліцію України» [31] в практичній дії. Сама стратегія широко застосовується у різних країнах. В Україні ж її почали впроваджувати відносно недавно саме у роботі поліцейських офіцерів громад. В свою чергу ми вважаємо, що ця стратегія буде досить доречною саме у взаємодії

кіберполіції та громади, адже при такій взаємодії не лише покращиться діалог між ними, а й збільшиться рівень довіри та ефективність і якість роботи. На нашу думку, саме це дозволить в подальшому зменшити час затрачений на викриття кіберзлочинів і збільшить можливості підрозділу кіберполіції.

Community policing має базуватися на тих складових, які зможуть допомогти в майбутньому поліції виконувати свою діяльність з більшою ефективністю та меншою затратою на це часу.

1.2. Нормативно-правове забезпечення механізмів взаємодії кіберполіції та громади

Досліджуючи систему нормативно-правового забезпечення механізмів взаємодії кіберполіції та громади, можна сказати, що Конституція України [16] є її фундаментом. Вона визначає забезпечення кібербезпеки однією з найголовніших функцій держави. Також стаття 17 Конституції України говорить, що забезпечення інформаційної безпеки України є «справою всього українського народу». В свою чергу Кримінальний кодекс України [17] подає основні негативні діяння, які стосуються кіберзлочинів, а також санкції та кримінальну відповідальність, яка передбачена для правопорушників. Відповідно можна з впевненістю говорити, що правове регулювання боротьби з кіберзлочинністю можливе лише за умови системного втілення приписів проаналізованого законодавства. Також варто уточнити, що саме Конституція України називає однією з важливих функцій – забезпечення інформаційної безпеки.

В обов'язковому порядку виконуються такі міжнародні правові угоди, а також договори, які ратифікувала Україна (Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. ратифікована 2005 року [13]; Міжнародна конвенція про боротьбу з фінансуванням тероризму від 9 грудня 1999р. ратифікована 2002 року [18]; Конвенція про відмивання, пошук, арешт та конфіскацію доходів отриманих злочинним шляхом від 8 листопада 1990 р. ратифікована 1997 року [15]; Конвенція ООН про боротьбу проти незаконного обігу наркотичних засобів і психотропних речовин від 20 грудня 1998 р. ратифікована 1991 року [14]; Резолюція Генеральної Асамблеї ООН 57/239 «Елементи для створення глобальної культури кібербезпеки» від 20 грудня 2002 р. та ін.

Відповідно до Конвенції про кіберзлочинність, яка була ратифікована Україною від 26 травня 2015 року першочерговим заходом для захисту громадян від кіберзлочинців є побудова чіткого законодавства і налагодження у цій галузі міжнародного співробітництва.

Варто зазначити, що 26 серпня 2021 року Указом Президента України було введено в дію рішення Ради Національної безпеки та оборони «Про Стратегію

кібербезпеки України» [39], в якому головним меседжом є «Безпечний кіберпростір-запорука успішного розвитку країни», тобто цим і наголошено важливість роботи кіберполіції, а також окреслено основні вектори їх стратегічної діяльності.

Основним законодавчим документом у сфері кібербезпеки безумовно виступає Закон України «Про основні засади забезпечення кібербезпеки України»[34]. Він і є одним із найважливіших базисних документів, на які опирається у своїй роботі Департамент кіберполіції. Цей закон визначає основні правові і організаційні засади забезпечення життєво важливих інтересів людини і громадянина, суспільства і держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств та установ, а також основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Досить важливими законодавчими актами для Національної поліції у сфері протидії кіберзлочинам є Закон України «Про національну безпеку України» [30], «Про боротьбу з тероризмом» [21].

Наступним рівнем ієрархії нормативно-правового забезпечення є не менш важливий Закон України «Про Національну поліцію України» [31]. Стаття 5 Закону України «Про Національну поліцію» говорить, що поліція в процесі своєї діяльності взаємодіє з органами правопорядку та іншими органами державної влади, а також органами місцевого самоврядування відповідно до закону та інших нормативно-правових актів. З метою визначення причин та або умов учинення правопорушень планування службової діяльності органів і підрозділів поліції здійснюється з урахуванням специфіки регіону та проблем територіальних громад.

Взагалі Закон України «Про Національну поліцію» [31] досить в загальних рисах окреслює механізм взаємодії поліції з органами місцевого самоврядування.

Задекларовані основи взаємодії поліції і органів місцевого самоврядування базуються на принципах відкритості і прозорості, дотримання прав і свобод людини, взаємодії з населенням на засадах партнерства тощо. Виходячи з положень вказаних в законодавчих актах чітко прослідковуються шляхи взаємодії поліції і органів місцевого самоврядування.

Керівники територіальних органів поліції повинні не менше одного разу на два місяці проводити відкриті зустрічі з представниками органів місцевого самоврядування на рівнях областей, районів, міст та сіл з метою налагодження ефективної співпраці між поліцією та органами місцевого самоврядування і населенням. На таких зустрічах обговорюється діяльність поліції, визначаються поточні проблеми та обираються найефективніші способи їх вирішення.

Відповідно до визначених повноважень органи Національної поліції зобов'язані: забезпечувати виконання загальнообов'язкових рішень місцевих рад, які були ухвалені згідно їх компетенції, з питань охорони публічного порядку та правил торгівлі в невстановлених місцях; виконувати запити органів місцевого самоврядування про наявність документів, що їх цікавлять, і видавати копії документів і архівних довідок. Місцевого самоврядування у цьому контексті повинна спрямовуватися з метою забезпечення правопорядку на певній території, охорони прав і свобод громадян. Так, відповідно до ст. 38 Закону України "Про місцеве самоврядування в Україні" [29], до відання виконавчих органів сільських, селищних, міських рад належать: сприяння діяльності органів суду, прокуратури, юстиції, служби безпеки, внутрішніх справ та адвокатури. Варто зауважити, що роль та інтереси місцевого самоврядування в області охорони публічного порядку повинні бути пов'язані задля реалізації потреб населення, підтримці громадського спокою, створенні хороших умов для функціонування підприємств та установ, а також для захисту інформації та даних місцевих органів влади [3,с.75-76].

Взаємодія кіберполіції із місцевими органами виконавчої влади у профілактиці попередження кіберзлочинів відбувається як на місцевому так і на регіональному рівні. Управлінський вплив із метою координації профілактичної діяльності на регіональному рівні здійснюють обласні державні адміністрації. Відносини обласних державних адміністрацій та кіберполіції будується на підставі субординаційних зв'язків, коли відповідно « вищі органи управління визначають зміст та спрямованість діяльності підпорядкованих суб'єктів для досягнення єдиної мети». А відповідно до п. 2 ст. 119 Конституції України місцеві державні адміністрації забезпечують законність та правопорядок на певній території.

Таким чином, можемо сказати, що місцеві адміністрації є суб'єктами системи профілактики правопорушень [3,с.60-61].

Національна поліція у своїй діяльності керується указами Президента України та розробляє пропозиції щодо вдосконалення актів Президента України.

Кабінет Міністрів України організовує фінансове і матеріально-технічне забезпечення діяльності правоохоронних органів.

Кіберполіція взаємодіє з громадськістю шляхом підготовки і виконання спільних проєктів, програм і заходів для задоволення потреб населення і підвищення ефективності виконання поліцією покладених на неї завдань.

Захист держави гарантується, перш за все, тим, що співробітництво особи з оперативними підрозділами у виконанні спеціальних завдань оперативно-розшукової діяльності вважається державною таємницею, яка відповідно охороняється законами України «Про оперативно-розшукову діяльність» [35], «Про організаційно-правові основи боротьби з організованою злочинністю» [36], «Про державну таємницю» [23] та низкою інших.

Важливі аспекти правового регулювання кібербезпеки відображено в таких правових нормах: Закон України «Про Державну службу спеціального зв'язку та захисту інформації» [22] від 23 лютого 2006 року.

Закон України «Про інформацію» [2] регулює правові питання інформаційної діяльності, крім цього низка законодавчих актів, які теж відповідно окреслюють відносини у інформаційній сфері: Закон України «Про телекомунікації» [40] (втратив чинність 01.01.2022 у зв'язку з набуттям чинності Закону «Про електронні комунікації» ») [24]), «Про Національну програму інформатизації» [32], «Про захист інформації в інформаційно-телекомунікаційних системах» [25].

Нормативно-правові акти Президента України, Верховної Ради України, Кабінету Міністрів України, Ради Національної безпеки та оборони України – підзаконний рівень правового регулювання кібербезпеки.

Також Міністерством внутрішніх справ було прийнято цілу низку нормативно-правових актів, які стосуються саме питання інформаційної безпеки:

- Доручення МВС України від 19.03.2015 № 13155/Ав «Про заходи із протидії витоку службової інформації» [26];

- Доручення МВС України від 24.04.2015 № 19130/Ав «Про недопущення витоку інформації, що утворюється в службовій діяльності» [33];

- Наказ Національної поліції України від 07.12.2015 № 176 «Про запобігання негативним наслідкам використання інтернет-ресурсів російських провайдерів» [27].

Сам Департамент кіберполіції регламентується наказом Кабінету Міністрів України №831 від 13 жовтня 2015 року «Про утворення територіального органу Національної поліції» [41], а також відповідно до наказів МВС від 15.10.2015 №1250 «Про проведення позачергового атестування осіб начальницького складу підрозділів боротьби з кіберзлочинністю [37] та № 1251 від 15.10.2015 «Про проведення конкурсу на заміщення вакантних посад старших інспекторів, інспекторів і спеціальних агентів інформаційних технологій міжрегіонального територіального органу Департаменту кіберполіції Національної поліції» [38]. Також є положення про Департамент кіберполіції НП України, затверджене наказом Національної поліції від 10.11.2015 №85 згідно з яким створено Департамент кіберполіції.

Отже, ми можемо сказати, що реалізація завдань Національної поліції в Україні означає, що поліцейська діяльність здійснюється відповідно до принципів, що закріплені законодавством з урахуванням сучасних тенденцій європейської інтеграції. Принципи як керівні ідеї, які є базою для функціонування кожного органу та підрозділу поліції, покликані сприяти подальшій розбудові поліції як інституту європейського зразка. Своєю чергою завдання поліції визначають методи здійснення поліцейської діяльності, що ґрунтуються на відповідних принципах.

РОЗДІЛ 2
АНАЛІЗ МЕХАНІЗМІВ ВЗАЄМОДІЇ КІБЕРПОЛІЦІЇ З ГРОМАДОЮ

2.1 Аналіз основних показників роботи Департаменту кіберполіції у розрізі 2017-2020 рр.

Відповідно до звітів про роботу Національної поліції України прослідковується тенденція частого використання інтернету для злочинних схем. Департамент кіберполіції наголошує, що особливо чітко то відчувалося в період карантину, коли саме усі операції (робота, покупки, зустрічі і тд.) перейшли в онлайн режим.

Розповсюдження вірусів, викрадення інформації та даних, крадіжки грошей з карток, онлайн-торги зброєю та наркотиками – усі ці злочини розкривала кіберполіція [11, с.12].

Загалом протягом останніх трьох років спостерігається збільшення обсягу розкриття кіберзлочинів (рис.1.2). Усього за 2020 рік було зафіксовано понад 5 тисяч кіберзлочинів, в яких оперативно затримали 106 фігурантів кримінальних проваджень, серед яких 13 педофілів [11, с.12]. В свою чергу у 2019 році було викрито 4263 тисячі злочинів, з яких 1641 стосувалися саме шахрайств у платіжних системах та 1494 кібербезпеки. Також було викрито 332 факти розповсюдження протиправного контенту та 744 факти вчинення злочинів у сфері електронної комерції [9, с.9].

У 2018 році підрозділом було зафіксовано близько 6 тисяч злочинів, які вчинені у сфері використання інформаційних технологій. Тисяча з яких – злочини, що вчинені в галузі кібербезпеки. 11 131 кримінальне провадження супроводжувалось [10,с.14].

На діаграмі ми можемо прослідкувати, що у 2018 році кількість викритих злочинів перевищує їх кількість розкриття у 2019 та 2020 роках.

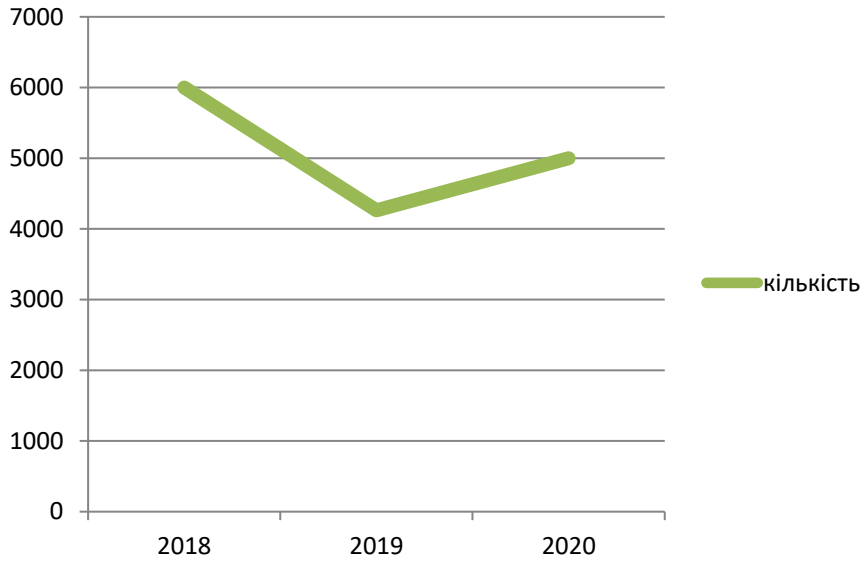

Рис. 2.1. Кількість викритих кіберзлочинів протягом 2018-2020 рр.(побудовано автором на основі даних [9],[10],[11])

Департаментом у 2018 році було проведено чимало успішних операцій: затримання організатора бот-мережі Аваланч, викриття учасника міжнародного хакерського угрупування Кобальт, участь в припиненні діяльності міжнародної хакерської групи FIN7 (ФинСевен).

Також за цей рік було попереджено кіберполіцією поширення 4 масових кібератак на території нашої держави. Затримано декілька організованих злочинних груп, які спеціалізувалися на створенні фіктивних бірж з продажу цінних паперів.

Протягом всього року було закрито роботу близько 40 піратських сайтів.

Гідні здобутки кіберполіція має і на міжнародній арені. У 2018 році було також підписано договори про взаємодію у сфері боротьби з кіберзлочинами з поліцією Сінгапуру, Катару, Австралії та ще декількох країн. В межах міжнародної співпраці було викрито 8 транснаціональних хакерських угруповувань та взято участь у понад 30 міжнародних операціях [10,с.14].

На рис 1.2 та рис. 1.3. відповідно, ми визначили структуру кримінальних правопорушень 2018 та 2020 року за сферами.

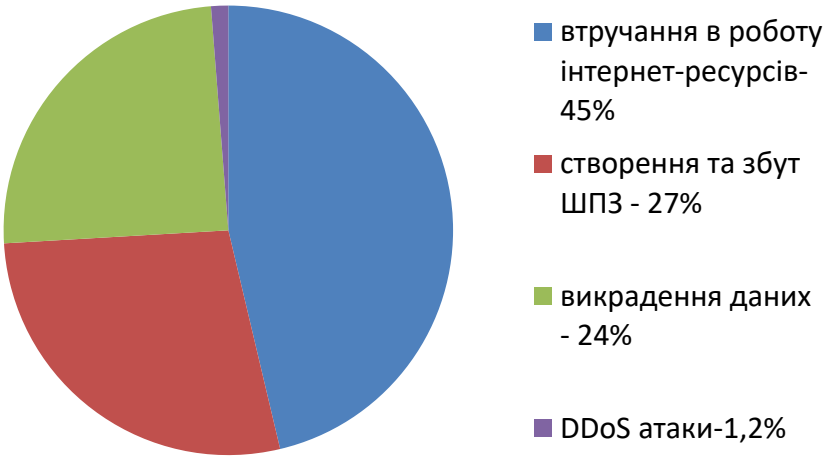

Рисунок 2.2 Структура кримінальних правопорушень 2018 р. [10]

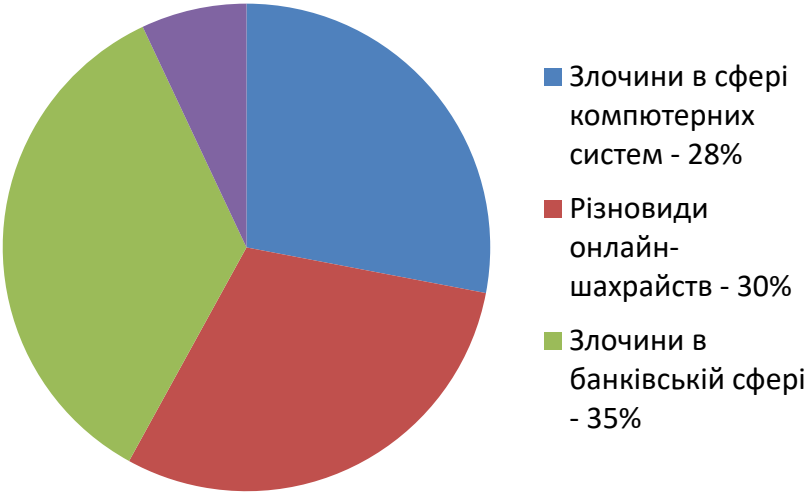

Рисунок 2.3 Структура кримінальних правопорушень 2020 р.[11]

Згідно з даними Департаменту кіберполіції від початку 2020 року підрозділ супроводжував розслідування 10 659 злочинів скоєних у сфері інформаційних технологій [11,с.12].

Якщо порівняти загальну кількість злочинів, яку співробітники Департаменту супроводжували за цей період і кількість завершених розслідувань, то їх співвідношення приблизно дорівнює 80/20. На загальну кількість 10,659 припадає 2,320 розкритих злочинів. Всього з початку 2020 року були встановлені 519 осіб, яким було пред'явлено підозру.

За статистичними даними 2018 році кіберзлочинцями були користувачі ШПЗ (63 %), селери (16%), кодери (10%), продавці баз даних (7%) та члени хакерських APT-груп (4%) (рис.2.4).

Рисунок 2.4 Спеціалізація кіберзлочинців у 2018 році [10]

Варто зазначити що у 2020 році від здійснення кіберзлочинів державі було завдано матеріальних збитків на 241 млн. гривень, в той час як в 2019 році було завдано шкоди на 28 млн. гривень (рис.2.5). Тому можна з впевненістю говорити, що кіберзлочинці завдають щорічно чималої шкоди державі, її фінансовим активам, а також несуть загрозу її національній безпеці.

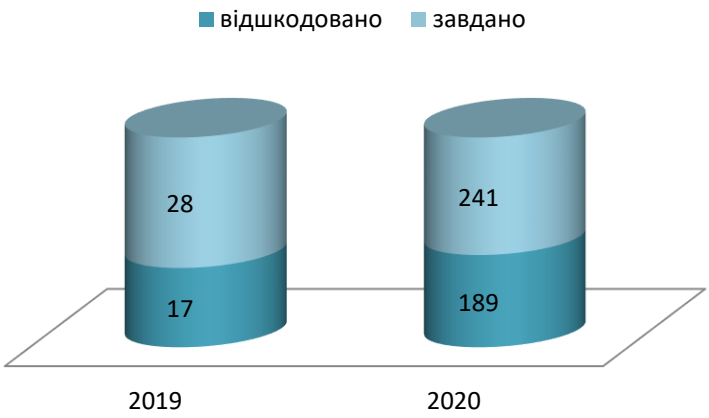

Рисунок 2.5 Сума завданих збитків державі [11]

У кіберполіції також запрацював власний сервісний центр, який був створений саме з метою надання громадянам консультацій з питань кібербезпеки. За 9 місяців роботи надійшло понад 100 тисяч дзвінків та більше 40 тисяч електронних звернень.

Варто наголосити, що однією із сучасних завдань, які поставлені перед кіберполіцією, це викриття наркоторгівлі через інтернет. Згідно з статистикою кожен

7 факт збуту наркотиків здійснювався через інтернет, в основному через різні месенджери [12,с.13].

Однією з важливих проблем залишаються шахрайства в державних установах. За результатами досліджень в Україні лідерами серед економічних злочинів, від яких постраждали українські організації є кіберзлочинність – 31 % та 31% - шахрайство в закупівлях.

Резонансне затримання співробітниками НАБУ за підозрою у розтраті понад 149 млн грн державних коштів заступника Міністра оборони України та директора Департаменту державних закупівель та постачання матеріальних ресурсів Міноборони знову привертає увагу до державних закупівель. Окрім цього були виявлені інші вразливості. Так система Prozorro дозволяла отримати доступ до закритих даних, зокрема, про запропоновані учасниками ціни ще до старту торгів. Згідно з розслідуванням видання, вразливим місцем у деяких типах тендерів став порядок використання його учасниками електронного цифрового підпису (ЕЦП) [19].

У 2020 році за даними Служби безпеки України знешкодили 600 кібератак на держресурси та об’єкти критичної інфраструктури, в той час як у 2019 році цей показник становив 480, а у 2018 – 360(рис.2.6).

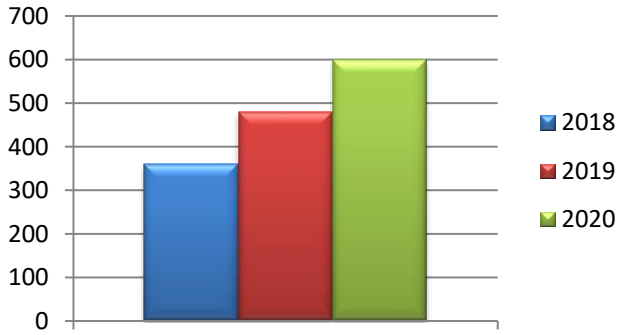

Рисунок 2.6 Кількість кібератак здійснених на державні структури у 2018-2020 роках [20]

Статистика говорить, що більшість кіберзлочинів здійснюється особами чоловічої статі у віці 25-48 років та жінками у віці 25-40 років (рис.2.7). І чітко прослідковується, що відсотки вікової категорії 40 років і більше, перевищують тих кому до 25 [10].

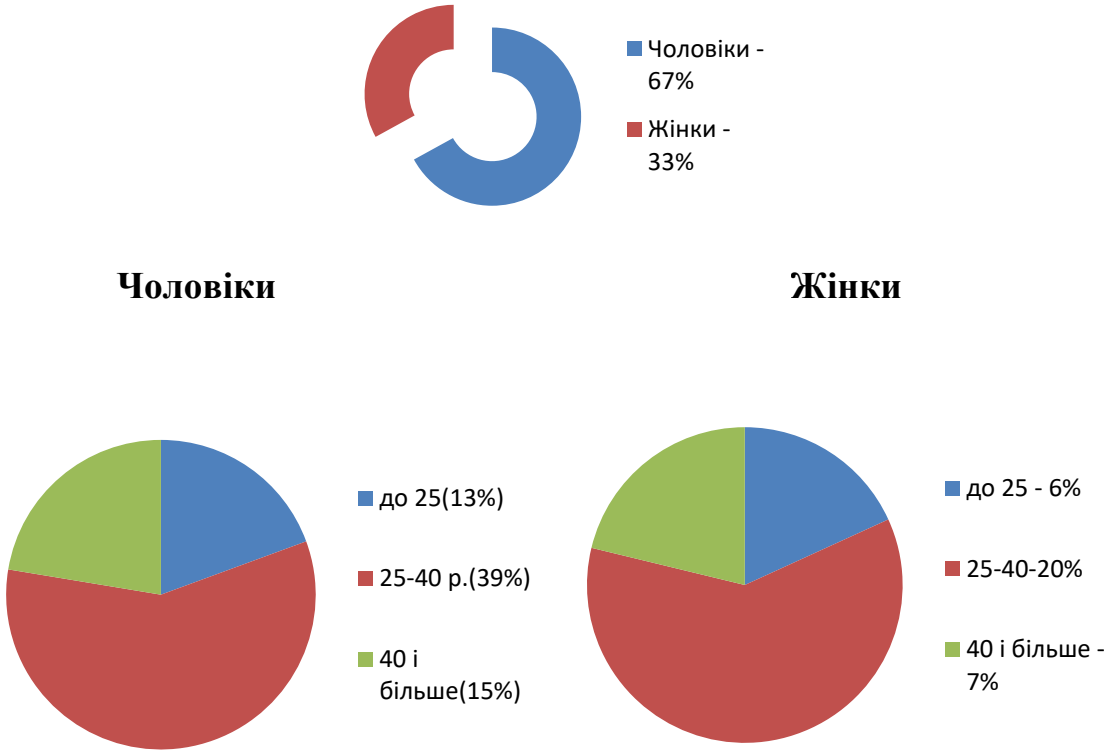

Рисунок 2.7 Класифікація злочинців за віком[10]

Досить важливою складовою, яка беззаперечно впливає на діяльність кіберполіції та ефективність її роботи – це матеріально-технічне забезпечення. Адже неможливо виконувати свою роботу добре, якщо немає матеріальних заохочень та стимулів. Це стосується не лише низького рівня заробітної плати, а й технічного забезпечення. Якщо до прикладу патрульну поліцію для виконання завдань забезпечують службовими автомобілями, то оперативні працівники кіберполіції мусять користуватися власними авто для виконання покладених на них завдань. Нових авто немає, а старі в досить поганому стані. Проблематичним питанням є і рівень заробітної плати, адже в таких підрозділах ненормований робочий графік, тобто працівники можуть виходити на роботу на вихідні і в позаробочий час, але це не впливає на оплату праці.

Статистика свідчить, що рівень кіберзлочинності щороку в нашій державі зростає і з великою швидкістю. Розвиток інформаційних технологій не лише

полегшує наше життя, але й без надійного захисту створює проблеми як для держави так і для кожного громадянина. Саме для того аби поліпшити кібербезпеку нашої держави, досить важливо забезпечити взаємодію кіберполіції з громадою. Пошук кращих варіантів взаємодії дасть змогу зміцнити національну безпеку України та зменшить витрати часу та ресурсів для розкриття зловмисників.

2.2. Характеристика механізмів взаємодії кіберполіції та оцінка рівня взаємодії громадянами

Community Policing – це підхід у щоденній роботі поліції, побудований на принципах постійної комунікації, де:

- поліція та місцева громада відчувають спільну відповідальність за безпеку;

- поліція реагує на місцеві потреби й вимоги, які визначає громада;

- взаємодія і комунікація між населенням і поліцією є ефективною і приносить результати;

- застосовується індивідуальний підхід до вирішення місцевих проблем у взаємодії з населенням та відповідальними органами влади;

- співпраця спрямована на попередження правопорушень і наявний спільний план превентивної діяльності.

Потреба у безпеці є однією з базових потреб людини, а співпраця поліції та громади – найкращий спосіб її забезпечити. Адже цей підхід ґрунтується на взаємодії між усіма, від кого залежить безпека: між громадою, поліцією та місцевою владою.

Відповідальний орган місцевого самоврядування завжди зацікавлений у забезпеченні правопорядку на своїй території. Адже від рівня безпеки в громаді залежить і добробут людей, від швидкого й ефективного реагування на злочини – їхня захищеність, а від превентивної роботи – менша кількість правопорушень і злочинів в майбутньому [4,с.3].

В Українських реаліях ми можемо сказати, що community policing – це стратегія співробітництва поліції та громад, зокрема сформованих ними місцевих органів влади (органів місцевого самоврядування, як-то виконкомів місцевих рад, ОСББ тощо), основною метою якої є запобігання і розв’язання проблем злочинності та гарантування захищеності життєдіяльності населення.

Ефективна взаємодія громадянського суспільства та держави під час реалізації правоохоронної функції може зблизити населення та владу, вирішити багато протиріч у соціальній та державно-правовій сферах. Тільки тісна взаємодія держави і громадянського суспільства в особі його інститутів допоможуть ефективному здійсненню правоохоронної функції держави в сучасних умовах.

Система партнерської взаємодії інститутів громадянського суспільства і держави у сфері забезпечення кібербезпеки передбачає наявність (рис.2.8):

- нормативно-правового механізму;
- соціального механізму;
- економічного механізму;
- інформаційно-комунікаційного механізму;
- організаційного механізму.

Рисунок 2.8 Система партнерської взаємодії інститутів громадянського суспільства і держави

Нормативно-правовий механізм є основою для побудови партнерських відносин між кіберполіцією та громадою. Саме завдяки законодавчо-закріпленим принципам та моделям поведінки, дана взаємодія стає не просто філософією, а справжнім зобов'язанням до виконання.

В свою чергу даний механізм може включати в себе такі норми права:

- зобов'язуючі – закріплюють певні обов'язки (до прикладу обов'язок громадянина повідомляти про злочин, якщо він став свідком такого злочину);
- забороняючі – забороняють вчиняти певні дії, (прикладом може бути будь яка норма правового акту, яка встановлює певні межі для дій);
- уповноважуючі – наділяють суб'єктів певними правами (встановлюють межі дозволеної поведінки).

Тобто ми можемо впевнено говорити, що даний механізм не лише законодавчо закріплює взаємодію поліції з громадою, але й регулює їхні відносини та встановлює певні обов'язки.

На сучасному етапі розвитку нашої держави дані відносини загально окреслені в Законі України «Про Національну поліцію України» [31].

Проблемним є законодавче закріплення визначення «взаємодія поліції з громадою», а також відсутність будь яких конкретизуючих документів, які б описували закріплену Україною модель взаємовідносин та встановлювала певні обов'язки щодо двох сторін даних відносин. Варто зазначити, що багато країн розробляють «Стратегію взаємодії поліції та громади», що є також відсутньою практикою у нашій державі. Фактично зазначені взаємовідносини не є прописаними і виконуються в більшості на рівні так званих «моральних норм» і не є закріпленим обов'язком, що потребує подальших напрацювань та бенчмаркінгу.

Соціальний механізм передбачає встановлення відносин між кіберполіцією та громадою за допомогою різних соціальних заходів, проєктів та безпосередньо комунікаційного контакту з іншою стороною.

До складових соціального механізму ми віднесли:

- проведення спільних заходів з кібербезпеки з активістами та волонтерами;
- розробка різних проєктів з поліцією та громадянами;
- активна участь у спільних форумах поліції, органів місцевого самоврядування, it-спеціалістів;
- закладення в освітню програму дисципліни з кібербезпеки тощо.

Кіберполіція взаємодіє з громадськістю шляхом підготовки і виконання спільних проєктів, програм і заходів для задоволення потреб населення і підвищення ефективності виконання поліцією покладених на неї завдань. Співробітництво між кіберполіцією і суспільством направлене на виявлення і усунення проблем, пов'язаних з здійсненням поліцейської діяльності, і запровадженню сучасних методів для підвищення результативності та ефективності своєї роботи. Також відкриття нового сервісного центру на базі Департаменту кіберполіції, який надає консультації громадянам є важливим чинником співпраці. Керівники територіальних органів поліції з метою підвищення авторитету та довіри населення до поліції систематично інформують громадськість про стан правопорядку, заходи, які вживаються щодо попередження правопорушень.

Поліція надає підтримку програмам правового виховання, пропагандує правові знання з кібербезпеки в освітніх закладах, засобах масової інформації і в видавничій діяльності. До ініціативи взаємодії з поліцією долучаються і громадські організації. Так до прикладу у Вінниці ГО «Паросток» започаткувало для поліцейських курси мови жестів з метою забезпечення їх спроможності спілкуватися з людьми з вадами слуху. У Полтаві в рамках проєкту «Кава з поліцейськими» громадяни можуть у неформальній атмосфері поспілкуватися з поліцейськими, а також дізнаються про особливості їх діяльності та безпеку в місті [44, с.82-83].

Досить вдалим прикладом взаємодії кіберполіції та громадянина є проєкт боротьби з наркокрамницями. Telegram чат-бот «Стоп-Наркотик» був розроблений курсантами та науково-педагогічними керівниками факультету кіберполіції Харківського національного університету внутрішніх справ, який став досить дієвим засобом боротьби з незаконним поширенням наркотиків через мережу інтернет. Кожного дня чат-бот розсилає своїм користувачам кілька «наркоадрес», на які їм пропонується залишити скаргу. Він дає можливість користувачам надсилати фото «графіті» (написи) з наркоадресами із обов'язковими зазначенням GPS-координат або фізичних адрес, де вони виявлені.

Співпраця поліції та громадян завжди є ефективною і дає найкращий результат, що доведено цифрами. На сьогоднішній день користувачі боту допомогли

заблокувати 1000 електронних адрес у месенджері Telegram. Також чудовою є ініціатива зафарбовування «нарконаписів» на вулицях спільно з поліцією та молоддю [42.с.161-162].

Економічний механізм включає в себе комплекс економічних методів та важелів, за допомогою яких, можна активізувати процес взаємодії кібероподіції з органами місцевого самоврядування, громадянами та it-спеціалістами. В нашій державі даний механізм не набрав широкої популярності, тому на сучасному етапі він майже не використовується на практиці. Через великий рівень корупції, корупційних зв'язків та хабарництва в Україні, економічний механізм є досить болючим питанням. Проте в умовах сучасних реформ варто говорити про нововведення в рамках фінансової децентралізації щодо можливого часткового фінансування правоохоронних органів з місцевих бюджетів, що є актуальним у зарубіжних країнах, де сприяє зближенню відносин місцевих органів влади та правоохоронних структур, адже хто як не місцева влада, розуміє потреби та необхідні ресурси для забезпечення правопорядку власного регіону. Також в рамках даного механізму здійснюється надання фінансової та іншої необхідної підтримки особам, залученим до вирішення завдань, пов'язаних зі скороченням злочинності та підвищенням безпеки.

Інформаційно-комунікаційний механізм розглядається як сукупність сучасних інформаційних технологій за допомогою яких здійснюється взаємодія кіберполіції з громадою.

До інформаційно-комунікаційного механізму входить:

- організація роботи кіберполіції в соціальних мережах Facebook, Instagram, Twitter тощо.
- інформування громадян на власних веб- сайтах;
- співпраця з сайтами місцевих органів влади;
- створення чат ботів, додатків за допомогою, яких відбувається тісна взаємодія з громадянами тощо.

Організаційний механізм включає в себе організацію структури всередині органу, а також налагодження клімату та робочої атмосфери між співробітниками

кіберполіції. Сюди ми можемо ще віднести мотивацію співробітників для позитивного сприйняття та бажання працювати над взаємодією з громадою.

Ми провели дослідження, де громадяни змогли оцінити рівень взаємодії кіберполіції та громади на сучасному етапі (Додаток Е).

В анкетуванні взяло участь 100 осіб. Опитування було проведено за допомогою гугл форми в соціальних мережах, в якому брали участь співробітники відділу протидії кіберзлочинам в Хмельницькій області, працівники Хмельницької міської ради, лікарі, студенти та активні громадяни міста Хмельницького. Згідно з результатом більшість опитаних знають, що являє собою кіберзлочин та яка відповідальність настає за скоєння такого злочину(рис 2.9).

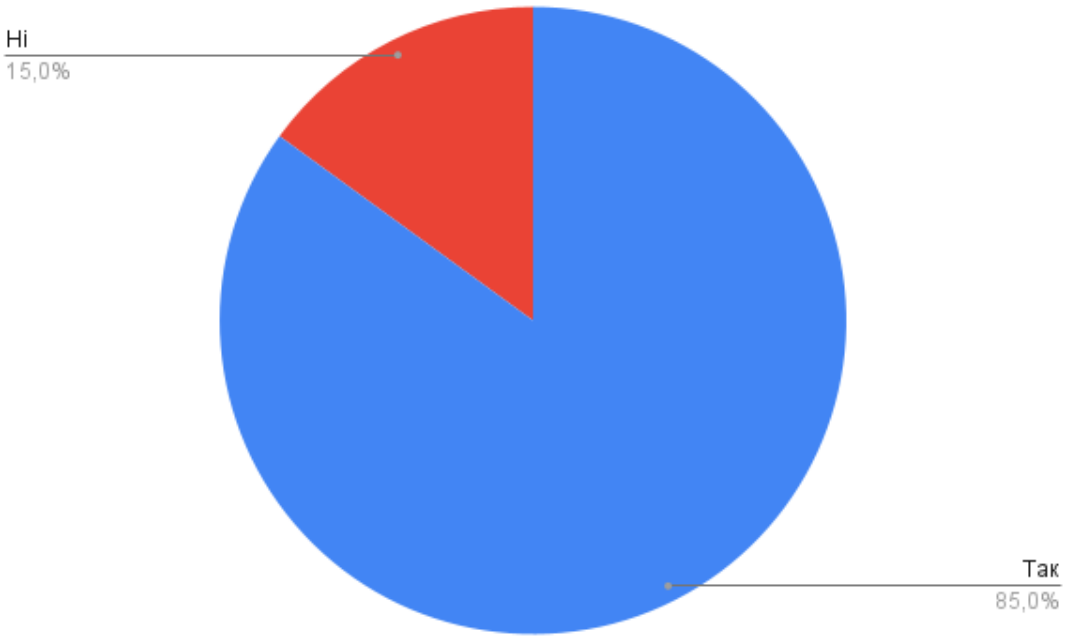

Рисунок 2.9 Чи відомо вам, що таке кіберзлочин та яка настає відповідальність за скоєння такого злочину?

80 % людей знають чим займається кіберполіція та які завдання покладені на неї, в свою чергу 15 % сказало, що не знає завдань і функцій кіберполіції. Таким чином ми можемо сказати, що більшість опитаних мають поняття, що таке кіберполіція і чи вона займається, проте варто аби частка 15% мала тенденцію зменшуватися.

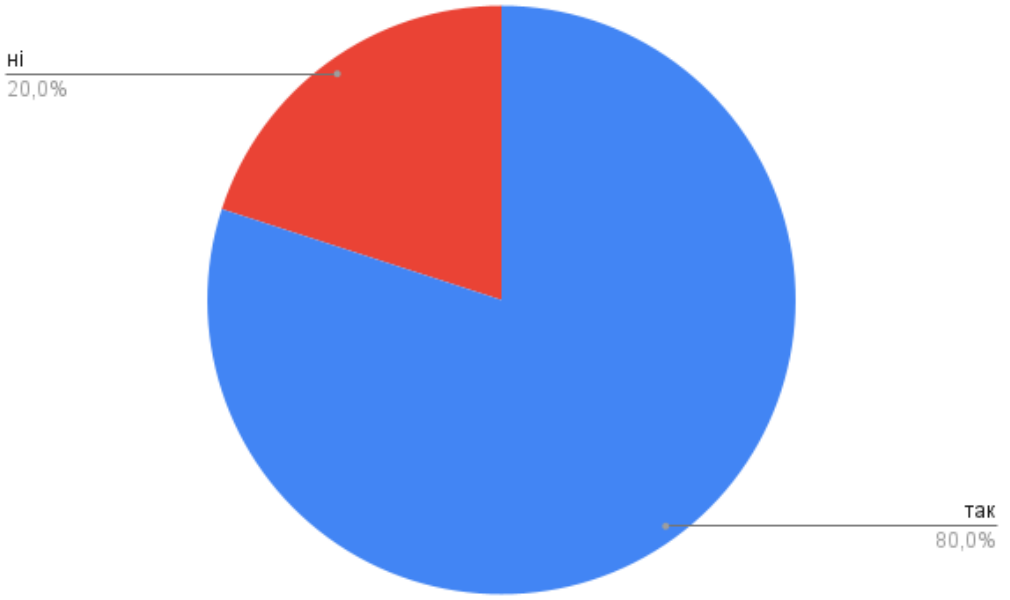

Рисунок 2.10 Чи знаєте ви, які завдання покладені на кіберполіцію України?

На питання «Чи були ви коли не будь залучені до співпраці з кіберполіцією?» 91 % респондентів відповіли – ні, і лише 9% опитаних все таки якимось чином співпрацювали з кіберполіцією України (рис 2.11).

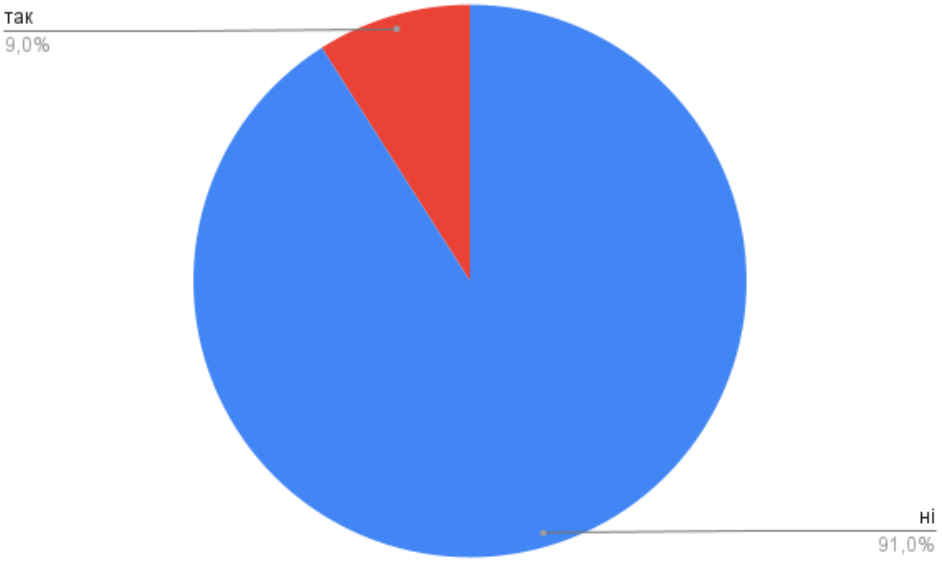

Рисунок 2.11 Чи були ви коли не будь залучені до співпраці з кіберполіцією?

Більшість громадян оцінюють роботу кіберполіції на середньому рівні – 40 %, на низькому 13% , а на високому лише 10%.Також варто сказати, що 37% опитаних осіб не змогли дати відповідь на поставлене питання(рис.2.12).

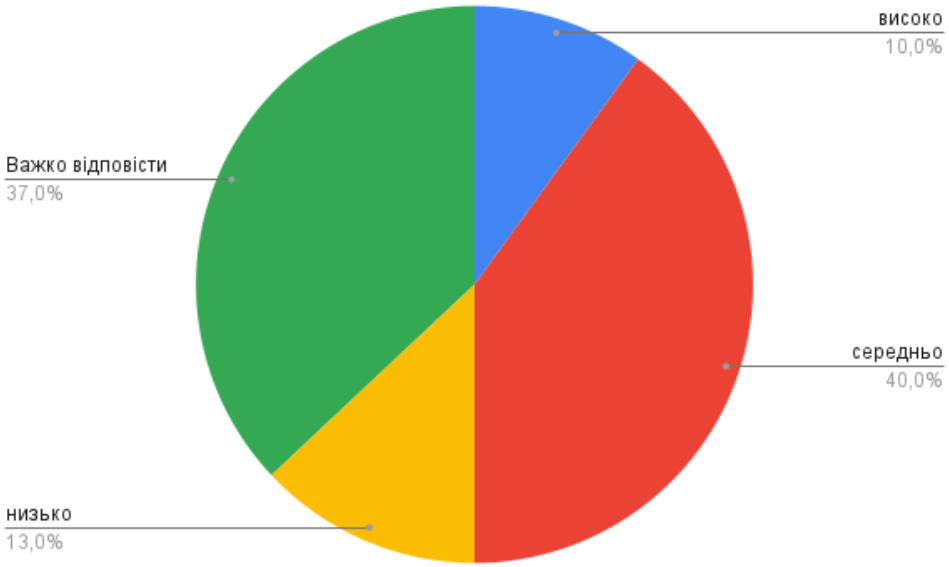

Рисунок 2.12 Як ви оцінюєте роботу кіберполіції України?

Потрібно зазначити, що 66% опитаних осіб бажало б долучитися до співпраці з кіберполіцією, якби була така можливість, 12% громадян не хотіли б взагалі долучатися до співпраці і 22% людей ще не визначилися з своєю відповіддю (рис.2.13).

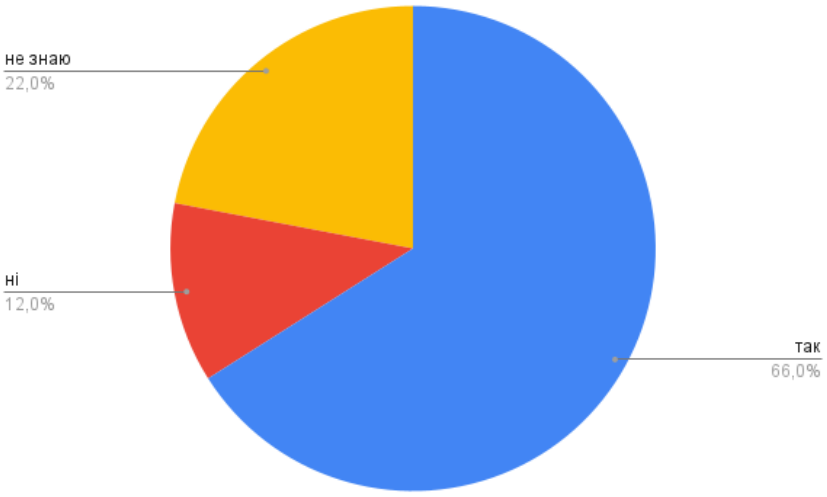

Рисунок 2.13 Чи долучились би ви до співпраці з кіберполіцією, якби вам запропонували?

Довіряють кіберполіції та її діям 40% опитаних і лише 16 % осіб висловили недовіру до даної структури. В свою чергу 44 % опитаних не змогли дати відповідь чи довіряють вони кібеполіції чи ні (рис.2.14).

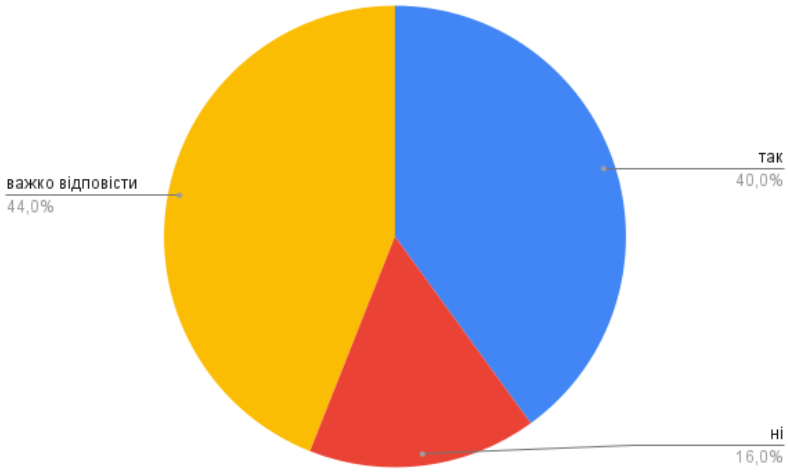

Рисунок 2.14 Чи довіряєте ви кіберполіції України?

87% опитаних вважають, що є велика потреба у законодавчому закріпленні взаємодії поліції та громади і лише 7% не вважають, що у цьому є нагальна потреба. В свою чергу 6% респондентів не змогли дати відповідь на дане питання (рис.2.15).

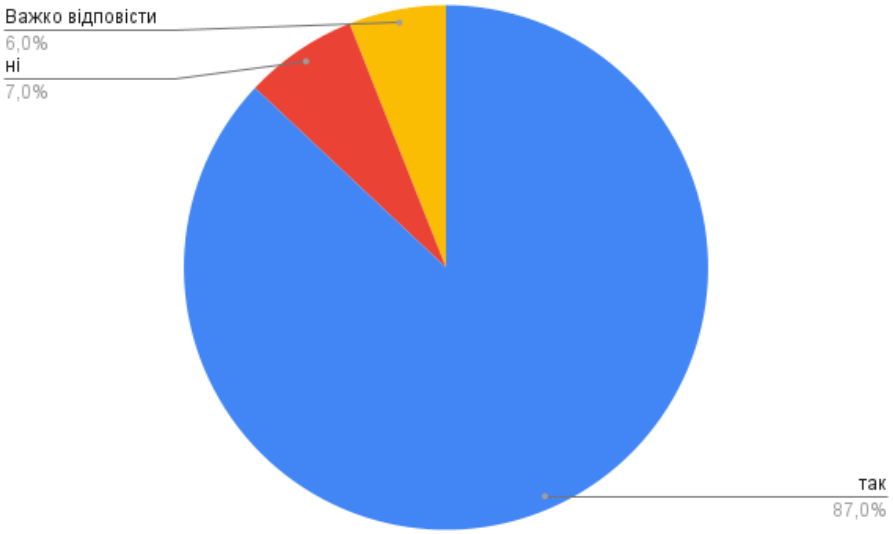

Рисунок 2.15 Як ви вважаєте потрібно законодавчо закріпити партнерство поліції та громади?

Те, що взаємодія кіберполіці з громадянами на сучасному етапі знаходиться на низькому рівні, висловилося 61% респондентів, 20% вважають, що така взаємодія є

зараз на середньому рівні і лише 3% опитаних сказало, що взаємодія зараз здійснюється на високому рівні. Проте 16% громадян не змогли точно дати відповідь(рис.2.16).

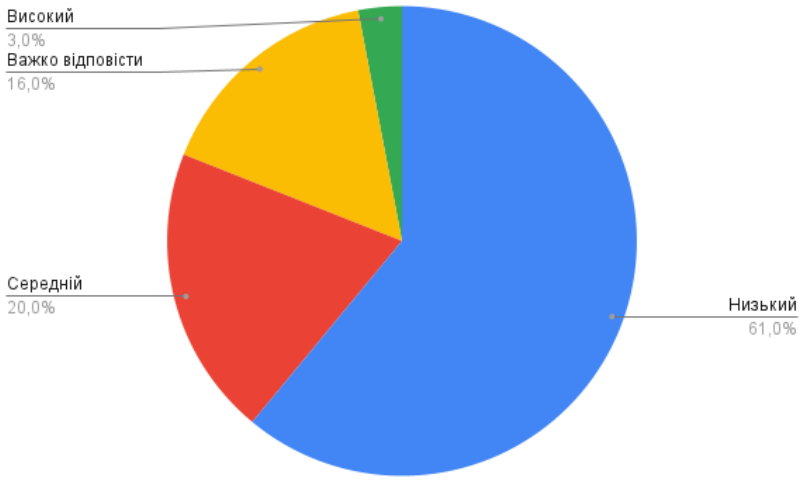

Рисунок 2.16 Який на вашу думку, зараз рівень взаємодії кіберполіції та громадян?

Згідно до опитування, 36% громадян вважають, що взаємодія між поліцією і органами місцевого саморядування існує на даному етапі, 30% висловило свою думку про відсутність такої взаємодії і 34 % опитаних не змогли відповісти (рис.2.17).

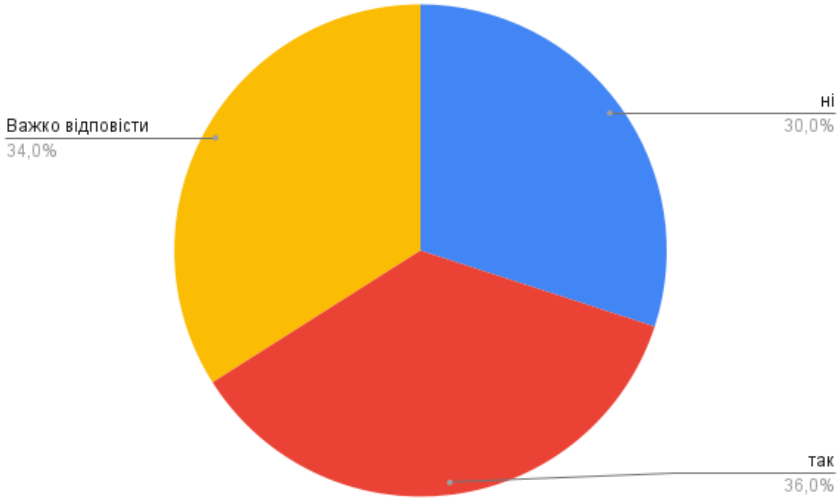

Рисунок 2.17 Чи на вашу думку, є взаємодія між кіберполіцією та органами місцевого самоврядування?

На запитання «Чи зустрічали ви інформацію в інтернеті/телебаченні/газетах про затримання кіберзлочинців?» 81% опитаних дали відповідь «так», і лише 19% дали відповідь «ні»(рис.2.18).

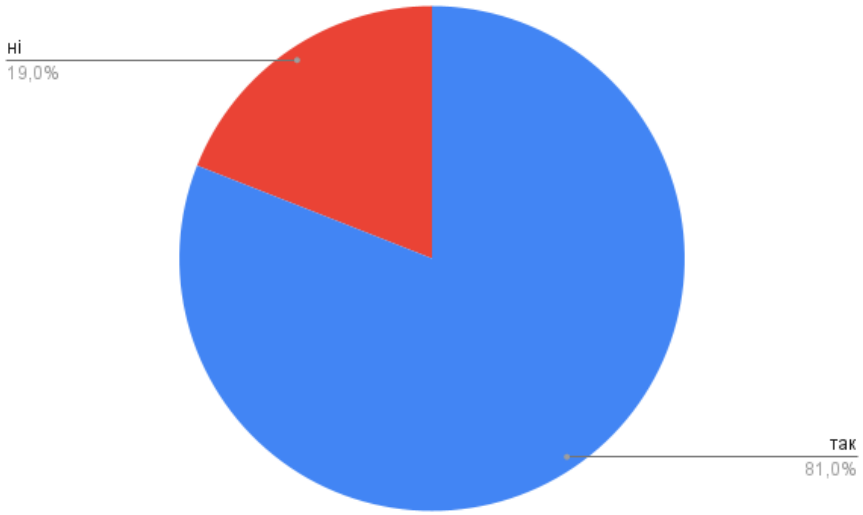

Рисунок 2.18 Чи зустрічали ви інформацію в інтернеті/телебаченні/газетах про затримання кіберзлочинців?

З рис.2.19 можна сказати, що 69% громадян схильні до думки, що інформація про кіберзлочини для громадян висвітлюється не в повному обсязі, 18% відповіли, що все таки інформація доноситься в хороших обсягах і 18% громадян не змогли відповісти конкретно на це питання.

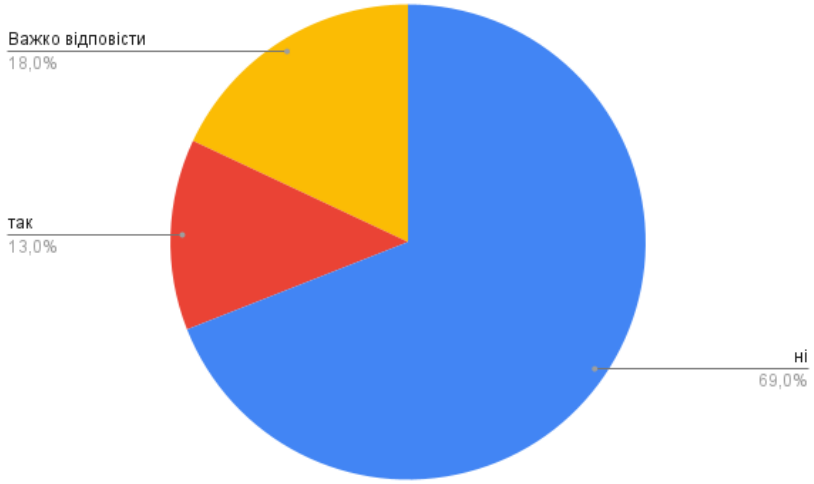

Рисунок 2.19 На вашу думку інформація про кіберзлочини висвітлюється для громадян в повному обсязі?

88% громадян висловились, що взаємодія кіберполіції та громади позитивно вплине на роботу правоохоронного органу, 11% опитаних не змогли відповісти і лише 1% осіб вважають, що дана взаємодія не вплине на ефективність роботи кіберполіції (рис.2.20).

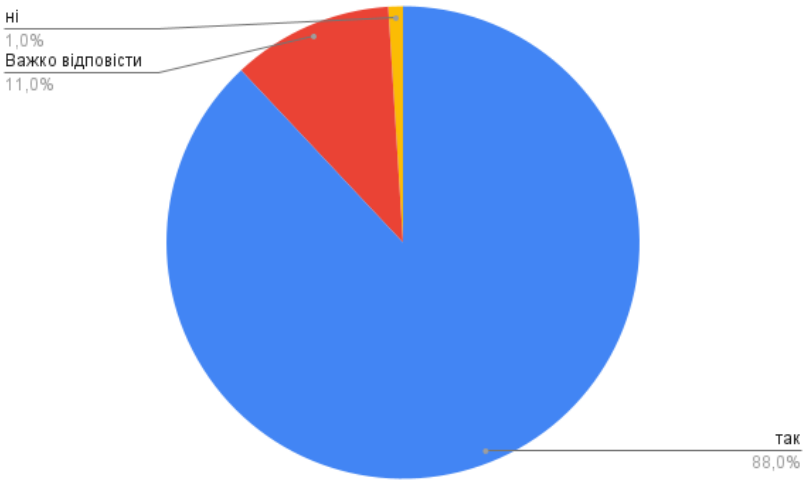

Рисунок 2.20 Скажіть чи вплине на ефективність роботи кіберполіції співпраця з громадянами?

96 % громадян висловились за те, що потрібно поліпшувати взаємодію кіберполіції та громади , 3% опитаних не змогли відповісти і лише 1% вважає, що не варто поліпшувати дану взаємодію (рис.2.21).

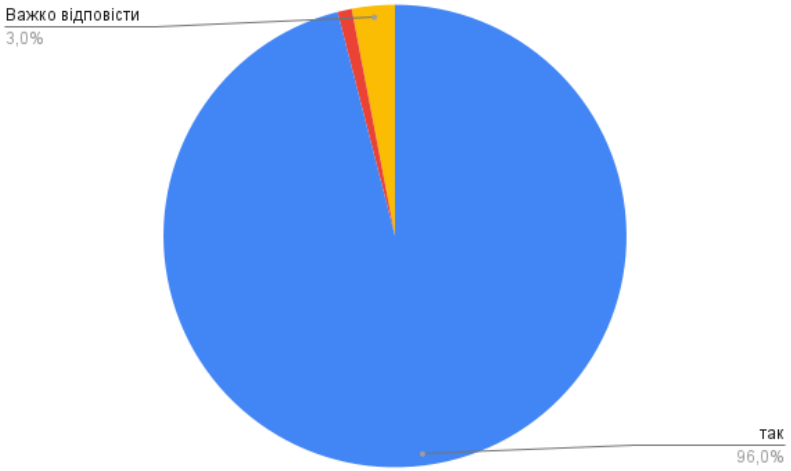

Рисунок 2.21 Чи варто на вашу думку поліпшувати взаємовідносини громади (органів місцевого самоврядування, громадян і бізнесу) та поліції?

Більшість респондентів вважають, що у школах та університетах потрібно запроваджувати дисципліну кібербезпеки – 91%, 5% вважають, що цього робити не варто і 4% опитаних не змогли дати віповідь на зазначене питання (рис.2.22).

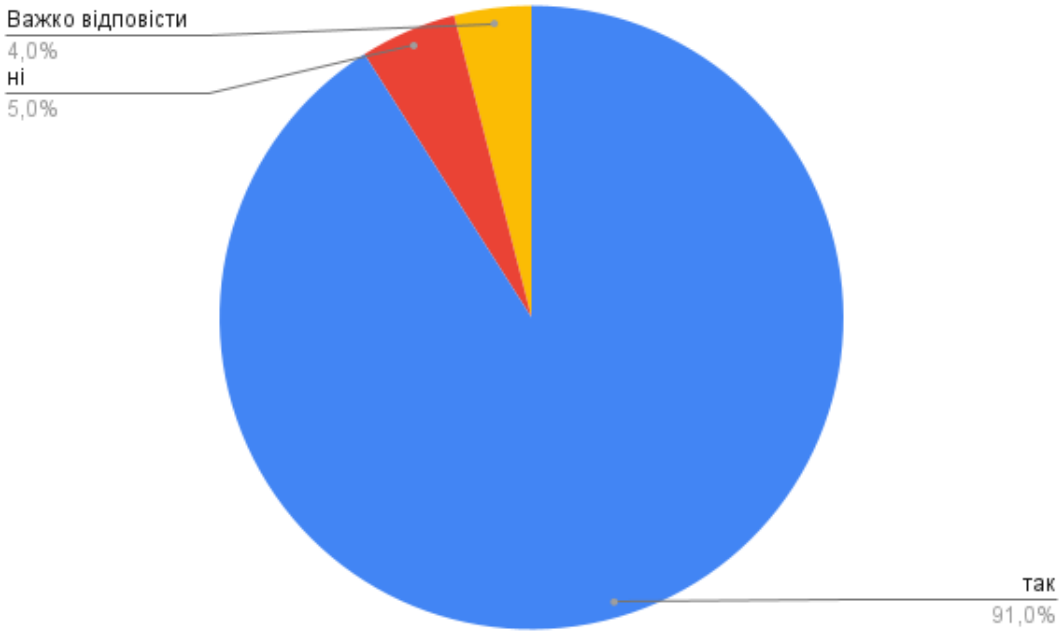

Рисунок 2.22 Чи варто запроваджувати у школах/університетах обов'язкову дисципліну кібербезпеки?

Найдієвішим інструментом поліпшення взаємодії кіберполіції та громади респонденти визначили спільні заходи(тренінги, лекції та форуми). Другу сходинку віддали інформовуванню громадян. На третій сходинці ж опинились законодавче закріплення такої взаємодії та комунікація в соцмережах.

За результатами дослідження ми чітко прослідковуємо те, що громадяни готові до співпраці і мають бажання допомагати, проте зараз немає ефективних інструментів для цієї взаємодії і тому як довіра до кіберполіції так і ефективність її роботи оцінюється громадянами на низькому рівні. Варто зазначити, що і самі громадяни бажають законодавчого закріплення взаємодії кіберполіції з громадою, а також пошуку нових інструментів і побудови ефективного механізму взаємодії, який би давав хороші результати. Дослідження також показало, що громадяни не бачуть суттєвої взаємодії між органами місцевого саморядування та кіберполіцією. Усе це дає нам хороші підстави для подальших пропозицій щодо удосконалення даних механізмів.

РОЗДІЛ 3

НАПРЯМИ ПОКРАЩЕННЯ МЕХАНІЗМІВ ВЗАЄМОДІЇ КІБЕРПОЛІЦІЇ ТА ГРОМАДИ

3.1 Шляхи вдосконалення механізмів взаємодії кіберполіції з громадою

Основною передумовою партнерства між поліцією та суспільством є теза про необхідність підвищення ступеня участі місцевого населення у зміцненні безпеки та громадського порядку, а також у вирішенні проблем злочинності у місцях проживання, оскільки поліція не в змозі вирішити це завдання своїми власними силами.

Як ми уже зазначали раніше, жоден з механізмів взаємодії поліції та громади не запроваджений повністю, а економічний механізм є відсутнім взагалі в українській практиці, тому аби досягти певних ефективних результатів, варто прийняти і провести деяке реформування як у внутрішній структурі так і у зовнішньому середовищі.

Проаналізувавши усі наявні компоненти механізму взаємодії ми виділили основні проблематичні питання, над якими потрібно працювати, для того аби в майбутньому побудувати справді ефективну систему взаємодії між кіберполіцією та громадою.

Якщо взаємодію з Президентом України, Кабінетом Міністрів визначено на законодавчому рівні і вона не потребує як таких змін на нашу думку, то питання з органом місцевого самоврядування, приватним сектором та громадянами є досить проблематичним. Ми вважаємо, що взагалі взаємодія кіберполіції з органами місцевого самоврядування є досить низькою, що спричинено саме узагальненим його законодавчим визначенням та відсутністю порядку цієї взаємодії. Варто наголосити, що кіберполіція в ході роботи з органом місцевого самоврядування наштовхується навіть на певні проблеми. До них можна віднести:

- низьку обізнаність працівників місцевого самоврядування в сфері кіберзлочинності;

- латентність (приховання злочинів всередині структури, перешкоджання документуванню злочинів);

- застарілі форми отримання інформації (отримання інформації за довгий проміжок часу);

- відсутність механізму, який зобов'язував би орган місцевого самоврядування зберігати інформацію довгий час.

Саме усе з вищеперерахованого досить перешкоджає роботі кіберполіцейських та збільшує обсяг часу, за який розкривається сам злочин.

Якщо ми говоримо про приватний сектор, то в загальному поширеною є практика підписання різних меморандумів співпраці. Приватний ІТ-сектор немає існуючих стимулів співпрацювати з поліцією та допомагати. Ця взаємодія є досить проблематичною і потребує нових підходів до розробки справді ефективних важелів впливу, які б могли заохочувати ІТ-сферу до діалогу та співпраці. Про таку взаємодію досить влучно сказав у інтерв'ю головний інспектор Департаменту кіберполіції Національної поліції України Андрій Врублевський: «Часто чи то через людський фактор співробітників ІТ-компаній, чи через неготовність співпрацювати, але в більшості ситуацій, навіть коли мова йде про статтю 162 статті КПКУ, по рішенню суду, не надається інформація, або не в повному обсязі, або надаються файли з уже потертими логами, які видно неозброєним оком. І на прохання дати хоч щось, що можна відновити і отримати інформацію, відповідають – все, що могли, дали, беріть нове рішення суду. З одного боку, ми розуміємо, що правовий механізм ніхто не відміняв, з іншого – провайдери, які не ведуть логи, не зобов'язані їх вести, і слідство заходить в кут [1].

Багато інновацій в свою чергу пробують запроваджувати для того аби налагодити взаємодію поліції та громадян. До цього як ми вже казали раніше відносимо: розробку різних проєктів, проведення тренінгів, лекцій тощо. Проте, як показує практика цього всеодно недостатньо, що говорить про необхідність пошуку шляхів удосконалення цього механізму.

Але цей механізм потребує організаційної стратегії, яка зможе гарантувати, що кожен працівник буде застосовувати цю філософію на практиці. Це також потребує відповідних змін у поліцейській організації, особливо традиційній та ієрархічній, де влада залежить від посади та звання. Така зміна має передбачати надання

оперативним працівникам більшої автономії в прийнятті рішень, що зможе в подальшому слугувати зростанням поваги до їх суджень, як професіоналів. Проте і самі громадяни мають розділяти не лише права, але й обов'язки, які безумовно є встановленні та визначені пріоритети на вирішенні проблем відповідно до «партнерського» підходу.

На нашу думку, дані зміни варто робити на основі класичної моделі взаємодії поліції з громадою. Саме дана модель застосовується більшістю розвинутих країн і показує свою ефективність на сучасному етапі розвитку суспільства (Додаток Е).

Класична модель Community policing складається з трьох ключових компонентів (рис.3.1):

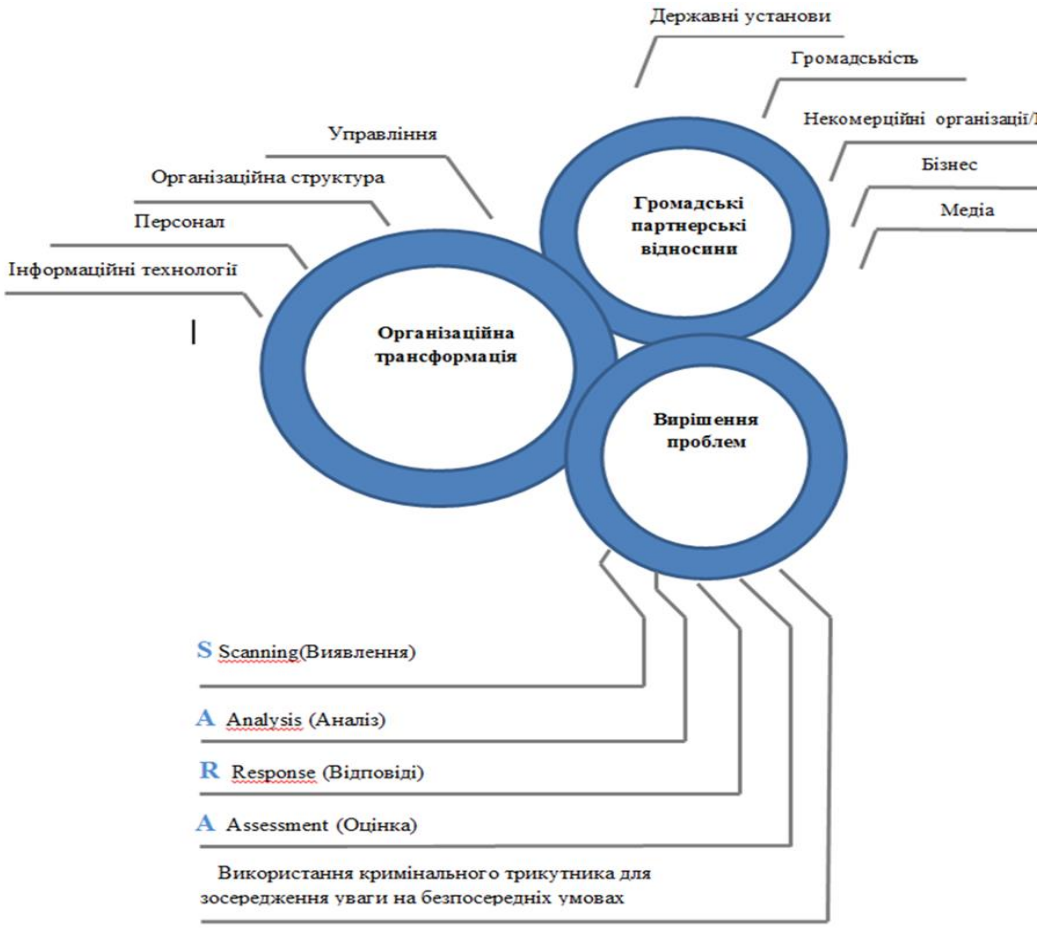

Рисунок 3.1 Основні елементи класичної моделі «community policing»[47]

1. Громадські партнерські відносини. Співробітництво між правоохоронними органами і організаціями, які допомагають вирішувати проблеми і підвищувати рівень довіри до поліції. До цих організацій належать:

- державні установи;

- громадяни;
- бізнес;
- медіа;
- некомерційні організації.

2. Організаційна трансформація. Погодження організаційного управління, структури, персоналу та інформаційних систем для підтримки партнерства з спільнотами і проактивне вирішення проблем.

3. Вирішення проблем. Процес участі в проактивних та систематичних оглядах виявлень проблем та оцінки ефективного їх вирішення.

Дана система досить легко імплементується та є простою у своїй структурі. Вона потребує незначних обсягів ресурсів і доводить свою ефективність по всьому світу. На нашу думку, така система була б досить ефективною при виробленні системи взаємодії кіберполіції та громади [53].

Для досягнення подібного партнерства поліції слід краще інтегруватися в суспільство і зміцнити свою легітимність (у суспільстві) через здійснення діяльності на основі узгодженості своїх дій та покращення якості наданих населенню послуг. Таким чином, вона повинна:

- бути легко впізнаваною та доступною для місцевого населення;
- знати місцевих жителів та бути відомою для них;
- реагувати на потреби населення;
- вислуховувати проблеми населення;
- залучати та мобілізувати місцеве населення;
- звітувати про свої дії та досягнуті результати.

В рамках цього процесу ми можемо детальніше розглянути основні напрями вдосконалення механізму взаємодії кіберполіції:

- з органами місцевого самоврядування;
- з приватним сектором;
- з громадянами.

Вивчивши думку громадян щодо поліпшення співпраці поліції з громадою, а також проаналізувавши досвід інших країн, ми виокремили найефективніші шляхи покращення даної взаємодії.

Для налаштування ефективної взаємодії з органами місцевого самоврядування на нашу думку, необхідно виконати ряд важливих заходів, а саме:

1) визначення на державному рівні порядку взаємодії між кіберполіцією та органами місцевого самоврядування та законодавче визначення поняття «взаємодія поліції з громадою»;

2) удосконалення нормативно-правової бази щодо питання взаємодії поліції та органів місцевого самоврядування;

3)за прикладом інших держав в обов'язковому порядку розробка «Стратегії взаємодії поліції та громади»;

4) в рамках децентралізації за прикладом інших держав можливе запровадження часткового фінансування з місцевих бюджетів, що дозволить більш повно враховувати потреби місцевого населення при здійсненні правоохоронної діяльності;

5) впровадження організаційних механізмів взаємодії з місцевими органами влади та самоврядування;

6) реалізація принципу community policing в операційній та управлінській діяльності кіберполіції;

7) побудова ефективної системи комунікації, пов'язаної з наданням державних послуг;

8) запровадження нових видів заходів-конференцій, де б поліція, органи місцевого самоврядування, активісти змогли обговорювати болючі питання та пропонувати шляхи їх вирішення;

9) проведення спільних форумів із залученням приватних ІТ-фірм;

Задля співпраці з громадянами, що є досить важливим елементом, варто забезпечити реалізацію саме таких заходів:

1) запровадження функціонування загального форуму для обговорення та консультацій на теми, пов'язані з кіберзлочинністю;

2) спільна розробка та виконання проєктів;

3) надання фінансової та іншої необхідної підтримки особам, залученим до вирішення завдань, пов'язаних зі скороченням злочинності та підвищенням безпеки.

4) використання добровольців. Community policing заохочує використання людських ресурсів поза правоохоронними органами. Добровільна діяльність передбачає активну участь громадян у роботі правоохоронних органів. Правоохоронні органи ознайомлюють громадськість зі способами такого партнерства з метою посилення ролі community policing та забезпечують ефективні засоби залучення громадян. Зусилля добровольців можуть допомогти зменшити затрати часу працівників поліції і дозволити постійному особовому складу зосередитись на превентивній діяльності [52,с.9].

Розробка заходів для якісної співпраці з приватним сектором є досить важким завданням. Основними завданнями які варто поставити перед собою насамперед є:

- розробка кіберстандартів для приватного сектора;
- збільшення частки інформування ІТ-компаній про відповідальність за кіберзлочини;
- запровадження відповідальності за збиток спричинений незахищеними послугами та продуктами;
- пошук нових заохочень для співпраці ІТ-компаній та кіберполіції
- надання приватному та державному сектору фінансових стимулів для поліпшення кібернетичної безпеки;
- впровадження форми співпраці ІТ-компанії з кіберполіцією на основі своєрідної реклами компанії (тобто використання назви компанії, яка допомогла в розкритті злочину в заголовках новин).

Крім роботи по вищевказаних напрямках поліція має використовувати різні форуми для обміну думками з населенням з питань, що становлять предмет загальної стурбованості.

Прикладами таких офіційних та неформальних інтерактивних форумів для спілкування зазвичай служать місцеві консультативні комітети, спільні робочі семінари, збори представників громадськості або відкриті дні поліції (створення сайтів з інфографіками офіційних даних).

Подібні форуми громадськості дають змогу обговорити дії поліції (включаючи обмін поліцейських та представників громадськості особистим досвідом) і дозволяють населенню прийняти активну участь у вирішенні проблем, що стосуються охорони їх безпеки, поділитися інформацією про свої труднощі та пріоритети, а також своїми уявленнями про те, як слід розв'язати існуючу проблему.

Залучення всіх зацікавлених державних відомств. До заходів щодо вирішення проблем слід також активно залучати інші державні структури, такі, як місцеві органи влади та адміністрацію, суди, прокуратуру, а також соціальні та охорони здоров'я та природоохоронні служби, оскільки вони можуть надати додаткові ресурси для вирішення деяких проблем боротьби зі злочинністю та забезпечення безпеки, якими не володіє поліція. Як приклад можна згадати зусилля міської влади щодо вдосконалення системи подачі електроенергії та покращення вуличного освітлення в районах де поширені написи «нарко-реклами». Також на нашу думку, варто спробувати запровадити пілотний проєкт «бюджетної децентралізації» по частковому фінансуванню місцевого органу поліції за рахунок місцевого бюджету, це допоможе зблизити орган місцевого самоврядування та правоохоронний орган і дасть змогу їм обєднати свої зусилля задля вирішення проблем на місцевому рівні [51].

Організаційні зміни, необхідні для реалізації концепції та стратегій роботи поліції з населенням за місцем проживання стосуються, насамперед, питань управління, внутрішніх структур поліції, а також структур інших державних установ та місцевої громадськості.

Децентралізація тісно пов'язана з перерозподілом сфер відповідальності всіх співробітників поліції, при якому співробітники нижчої ланки набувають великої самостійності, а їх безпосереднє начальство бере на себе функції координації, керівництва та підтримки, заохочуючи поліцейських, які працюють безпосередньо

серед населення, до раціонального, але творчого підходу в реалізації власних ініціатив, та забезпечуючи наявність ресурсів, необхідних для ефективного вирішення проблем.

Крім того, система передачі інформації в поліцейських службах повинна перейти від переважно використовуваної низхідної моделі потоку інформації (зверху-вниз) до стилю, орієнтованого переважно на висхідну модель (знизу-вгору), при якій поліцейські, які працюють з населенням, передають інформацію про проблеми та побажання населення своїй безпосередній і вищій ланці керівництва.

Подібна двостороння модель комунікації має також привести до колективного стилю прийняття рішень.

Оцінка ефективності діяльності працівника поліції повинна в першу чергу враховувати його здатність успішно працювати з проблемами місцевого населення та вміння залучати місцевих жителів до реалізації цих зусиль.

Слід застосовувати метод, заснований швидше на поєднанні кількісних та якісних критеріїв, що оцінюють (у довгостроковій перспективі) такі результати роботи співробітника, як, наприклад, ступінь ефективності заходів, вжитих у процесі вирішення проблем, рівень задоволеності населення поліцейським обслуговуванням або ступінь співпраці громади з поліцією, а також відчуття безпеки у населення. В такому випадку варто передбачати фінансові заохочення для працівника, який показує хороші результати по запропонованих критеріях. Процес реалізації можна поділити на чотири етапи, які слід розглядати як циклічно відновлювані(рис.3.2):

- Стадія підготовки;
- Стадія реалізації;
- Стадія оцінки;
- Стадія коригування.

За умови успішної реалізації концепції, поліція та суспільство отримають ряд переваг, деякі з яких перераховані нижче.

Місцеві жителі зможуть повідомляти про свої проблеми поліції та стати партнерами у процесі пошуку індивідуалізованих рішень своїх проблем. Це, у свою чергу, сприятиме поліпшенню ситуації із запобіганням злочинності,

підвищення рівня безпеки та забезпечення більш глибокого розуміння проблем безпеки.

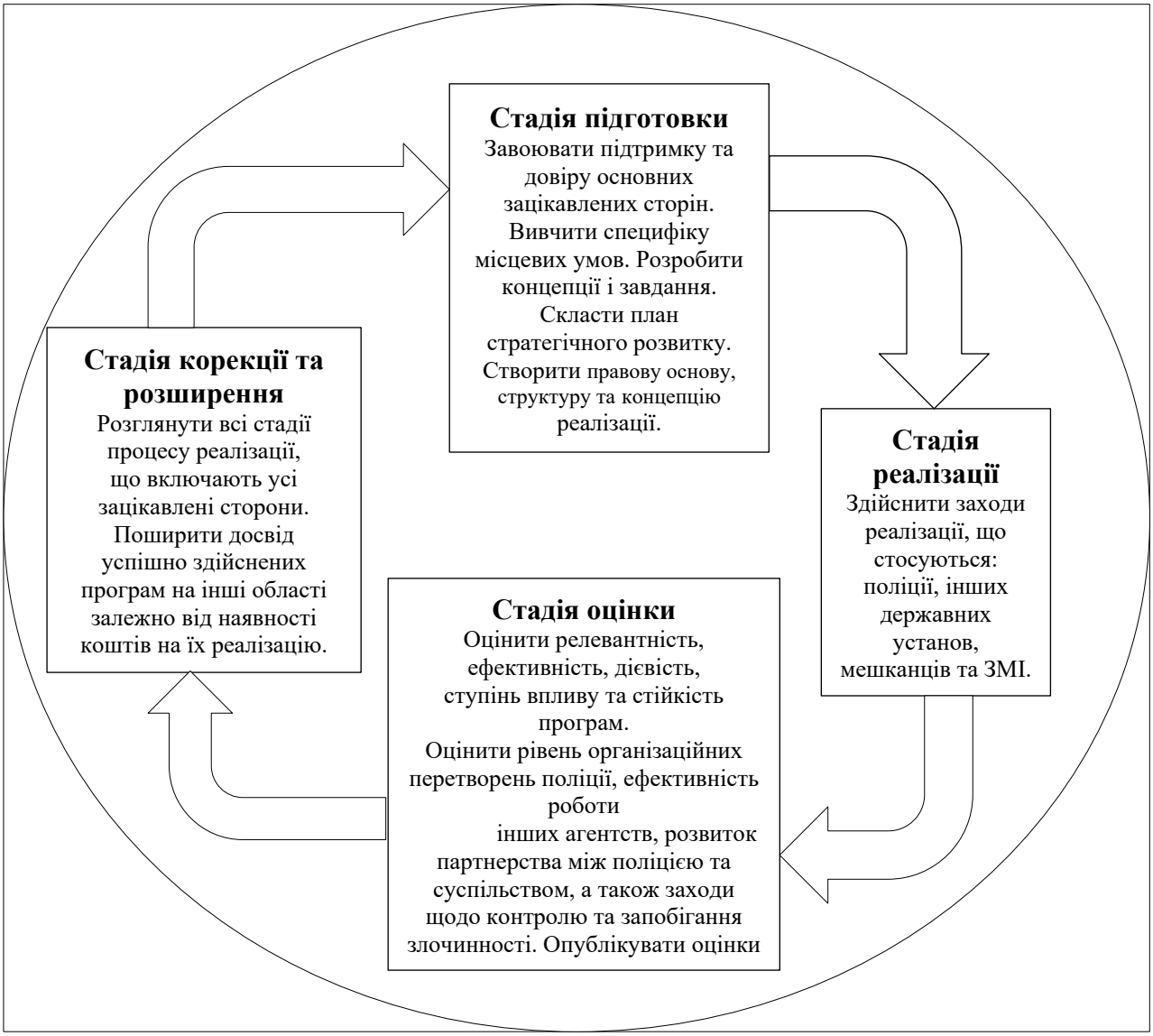

Рисунок 3.2 Цикл реалізації [49]

Інші громадські структури також отримують вигоду від участі у вигляді поліцейської діяльності. Створюючи відносини з іншими організаціями на основі гармонійної взаємодії, і вносячи свій внесок у їхні зусилля, можуть заощадити ресурси під час вирішення соціальних проблем. Більше того, успішне вирішення соціальних проблем дозволяє суттєву економію видатків.

Колективна відповідальність співробітників департаменту кіберполіції та зміцнення зв’язків та співпраці між департаментами, а також між поліцейськими, на

оперативній роботі та їх безпосереднім керівництвом, сприяє загальному покращенню для робітника клімату.

Нарешті, велике розмаїття поставлених завдань і коло функцій, що розширилося, з одного боку, роблять роботу більш цікавою, і, з іншого боку, надають більш широкі можливості просування по службі у зв'язку з тим, що співробітник є цінним у багатьох відношеннях [49].

3.2. Впровадження концепції «community policing» у взаємодії кіберполіції та громади

«Робота поліції з громадськістю – це філософія, а не тактика»
Кеннет Фортьє, колишній начальник поліції Ріверсайду, Каліфорнія

Робота поліції з громадськістю передбачає зміну ставлення до ролі поліції у суспільстві.

Найпростіше питання поліцейської діяльності: «Хто визначає, який порядок слід підтримувати і як його потрібно підтримувати? » Під патронажем громади розуміються деякі заходи щодо підтримання правопорядку, які надають значну роль «громади» у визначенні та керівництві роботою поліції. Це ґрунтується на демократичному принципі «будь-хто, хто користується владою від імені спільноти несе відповідальність перед спільнотою за здійснення цих повноважень».

Робота поліції у суспільстві передбачає, що громадськість хоче партнерства з поліцією. Це часто не так. Особливо у ситуаціях, коли громадська поліція застосовується, щоб відреагувати на непорозуміння між поліцією та громадськістю. В таких випадках поліцейські мають продемонструвати, що вони є гідними партнерами.

У Сполучених Штатах поліція використовує одну тактику для поліпшення таких відносин , а саме участь спільноти у посиленні боротьби зі злочинністю на місцевому рівні, зосередивши увагу на невелику цільову тему, таку як проблема банди, а потім залучення і до інших проблематичних питань.

Поширеними проблемами, що виникають при взаємодії із громадою, є:

- подолання скептицизму спільноти та відчуття, що вони все це чули раніше;
- подолання первісної громадської думки щодо м’якого підходу до злочинності;
- забезпечення ресурсів та структур, які потрібні спільноті для теорії на практиці, особливо з соціальними послугами, необхідними для проблемно-орієнтованих поліцейських підходів;
- подолання побоювань людей, що вони зіткнуться з репресіями з боку злочинців, якщо вони співпрацюватимуть із поліцією [50].

Основні принципи розвитку сучасної поліції у світі збігаються з принципами, визначеними англійцем Р.Пілом. Однак варто зазначити, що ще задовго до нього, на півночі США, вже були спроби створення організації з поліцейськими функціями. Усе почалося з об’єднань “Нічний Вартовий”, які формувались з волонтерів та активістів. Основним обов’язком цих організацій було спостереження за вулицями та

запобігання злочинами, однак ці добровільні підрозділи відрізнялись низьким рівнем дисциплінованості та недобросовісно виконували свої обов'язки (пиячили, самовільно припиняли чергування тощо), а тому їхня діяльність виявилася малоефективною.

Робота поліції з громадськістю чи її різновиди, стали національною мантрою американської поліції. Одним з найбільш важливих аспектів ефективної поліцейської діяльності є залучення громадськості. Для зміцнення довіри і поваги необхідна співпраця із суспільством [46].

Сполучені Штати Америки для проведення реформи «community policing» робили основне порівняння традиційної форми поліцейської діяльності та особливі ще не запроваджені на практиці її різновиди (Додаток Г).

Традиційна поліція передбачала, що інституційно та індивідуально поліція прагне мінімізувати зовнішнє втручання в роботу та адміністрацію поліції.

Здебільшого це робиться за рахунок того, що поліція перейняла професійну мантію, тобто вони ідентифікували себе як авторитетно незалежні від своїх клієнтів. Професійна модель, прийнята тут, розглядає клієнта як пасивну сутність, на яку слід спрямовувати роботу поліції. Більше того, поліція як інституція і як робоча група культури прагне відмежуватися від усього політичного та політиків.

У контексті традиційної поліцейської діяльності представлено поліцейську організацію у класичних веберівських термінах, у яких розмежування між організацією та оточенням є остаточними та ретельно підтримуються.

Отже, поліцейська організація робить навколишнє середовище нездатним змінити свою внутрішню динаміку і забезпечує собі певне відчуття контролю над навколишнім середовищем.

Для досягнення ефективної взаємодії з громадою поліція США пройшла певні етапи для трансформації традиційної системи поліцейської діяльності в проблемно-орієнтовну (Додаток Д).

Громадська поліція з самого початку намагалася залучити громаду до питання громадської безпеки при створенні та зміцненні спроможності громад протистояти злочинності. Наприклад, операція Weed and Seed фокусувалася на створення видимої

та активної присутності поліції, щоб впливати на проблемні райони, а також нарощування потенціалу у цих же мікрорайонах для підтримки досягнутих цілей. Багато операцій були успішними в штатах та призвели до скорочення обігу наркотиків на певних територіях. Це і є складовою частиною вказаного нами раніше соціального механізму, що дійсно на практиці доводить свою ефективність.

Поліцейські агенції по всій території Сполучених Штатів взяли на озброєння моделі організації та навчання, які сприяють співпраці з населенням та орієнтуються на проблеми місцевих громад. Чжао, Турман і Ловрич (1995) виділили три фактори навколо поліції орієнтованої на проблеми громади яка організаційної реформи. Перший фактор зосереджений щодо підвищення кваліфікації поліцейського. Другий фактор спрямований на покращення середнього рівня керівництва в органах поліції, і третій фактор пов'язаний із впровадженням поліцейських програм, орієнтованих на громаду, культурних заходів з метою покращення взаємодії поліції з громадянами та відносин з громадою.

Реформа органів поліції за принципом громадської та проблемно-орієнтованої поліції не була безперешкодною. Насправді все навпаки. Зміни внутрішніх поліцейських процедур та структури порівнюються з «вигинанням граніту»

Гайо , Чжао та його колеги виявили кілька перешкод до організаційних змін за нормами громади та проблемно-орієнтованої поліції. Вони включають опір керівників середньої ланки та лінійних офіцерів, внутрішню плутанину щодо оперативного визначення поліцейської діяльності орієнтованої на громаду, занепокоєння, що поліція, орієнтована на громаду, може бути м'якою щодо злочинності, відсутність навчання офіцерів поліції та опір поліцейських профспілок [8].

Основними способами взаємодії поліції та громадян в США на даний момент є (рис.3.3):

Примітка. Складено автором на основі джерела [47]

Рисунок 3.3 Основні способи взаємодії поліції та громадян в США

1. **Волонтерство.** Дві цивільних людини допомагають поліції багатьма способами. Робота добровольців може включати:
   - виконання канцелярських завдань;
   - допомога в пошуково-рятувальних роботах;
   - написання довідок про порушення правил паркування;
   - патрулювання для забезпечення додаткової видимості поліції;
   - повідомлення про графіті;
   - допомога в інвентаризації майна та обладнання.

2. Служба в цивільній консультативній раді. У багатьох департаментах поліції є ради у справах громадян, які консультують і допомагають в реалізації ефективних стратегій щодо зниження злочинності і порушень, зміни уявлень і

сприяння позитивній взаємодії. До таких організацій можуть входити представники місцевих підприємств, церков, громадських груп, молодіжних груп, місцевих органів влади та правоохоронних органів.

3. Цивільна поліцейська академія. Інформаційні заняття в класах, що проводяться поліцією для громадян, дозволяють жителям дізнатися про цінності та місії місцевих правоохоронних органів, а також про діяльність Департаменту. Цивільні поліцейські Академії дають громадянам можливість краще зрозуміти різні аспекти роботи та причини, через які співробітники виконують певні дії.

4. Похвала або скарга. Якщо у людини була позитивна взаємодія з співробітником поліції у громаді, яка заслуговує на похвалу, вона ділиться ним з офісом начальника. Точно ж така ж сама схема діє з скаргою. Більшість департаментів розміщують на своїх веб-сайтах інформацію про те, як подавати скарги та подяки, а також про те, як обробляється ця інформація.

5. Участь в ініціативах, програмах та проєктах. Правоохоронні органи часто залучають свої громади до проведення заходів протягом усього року. Приклади включають в себе барбекю по сусідству та каву з поліцейським.

6. Відвідування зборів громади. Збори громади-це ще один спосіб взаємодії зацікавлених сторін спільноти, власників бізнесу з місцевими органами влади та правоохоронними органами. Жителі можуть спілкуватися з представниками поліції на цих зустрічах, щоб допомогти вирішити проблеми спільноти та сприяти позитивним відносинам співпраці.

7. Опитування. Правоохоронні органи можуть запросити думку членів спільноти, щоб допомогти направляти зусилля з охорони громадського порядку.
Члени громади можуть допомагати правоохоронним органам та взаємодіяти з ними, беручи участь у цих опитуваннях та надаючи чесні відгуки.

8. Взаємодія з дітьми. Програми, які залучають молодь до роботи правоохоронних органів, є відмінним способом познайомити дітей та їх сім'ї з місцевими співробітниками правоохоронних органів. Такі програми, як поліцейські дослідники/курсанти, поліцейські спортивні ліги, цивільні поліцейські академії, спеціально призначені для молоді, і програми наставництва, є хорошими прикладами

того, як молодь може співпрацювати з правоохоронними органами в позитивному ключі.

9. Робота в соціальних мережах. Багато поліцейських відомств використовують соціальні мережі для спілкування з громадськістю. Члени спільноти також можуть спілкуватися з правоохоронними органами через соціальні мережі [47].

Хорошим прикладом запровадження партнерських відносин поліції з громадою є Албанія.

Стратегія взаємодії поліції та громади на 2007-2013 роки була заснована на трьох чинниках «Community Policing» з кінцевою метою створити безпечне навколишнє середовище через встановлення партнерських відносин.

Прийняття партнерських відносин на початковому етапі відбувалося через нормативно-правовий підхід, а саме: внесення змін до закону про державну поліцію та Стратегію взаємодії поліції та громади 2007- 2013 р., що дозволило запустити важливі організаційні перетворення і встановило створення «громадського партнерства з поліцією» на законодавчому рівні.

З іншого боку, в Албанії існувало безліч законів, що підтримували громадську поліцію та співпрацю між поліцією та громадою.

І хоча немає закону, який зобов'язує муніципалітети та комуни співпрацювати з державною поліцією, закон делегує відповідальність префекту відповідно до закону № 8927/2002, «Про префект» (статті 6, 8, 10 та 16). Префект відповідає за координацію стосунків між органами місцевого самоврядування та державною поліцією. Крім того, префект відповідає за взаємодію між місцевими державними установами та поліцією.

З іншого боку, самі органи місцевого самоврядування, як передбачено законом № 8652/2000 «Про організацію та функціонування місцевого самоврядування» (статті 3, 4, 10 та 72) несуть відповідальність за підтримання громадського порядку та безпеки і це виступає однією з їхніх головних функцій.

При цьому закон подає певні межі, і говорить , що поліція має співпрацювати з муніципалітетами та комунами сама. Деякі документи подають наступне: Стратегія взаємодії поліції та громади включає в себе цілі та інструменти для досягнення

співпраці. Щоб налагодити успішну співпрацю, стратегія передбачає, що є необхідність у визначенні рамок спілкування, які допоможуть процесу, а також створять систему взаємодії між місцевими органами влади та місцевою поліцією.

Крім того, стратегія наголошує про важливість вдосконалення соціального механізму взаємодії поліції з громадою через:

1. Загальне навчання між поліцією та громадянами з метою полегшити процес співпраці.

2. Підготовка існуючих та нових поліцейських сил щоб наблизити їх до спільноти поліції та навчити комунікативним навичкам. Передбачене навчання має бути теоретичним та практичним.

3. Навчання менеджерів та директорів з метою покращення їхніх навичок та схиляють їх до стратегічного планування.

Інфраструктура та технології також вважаються важливими, включаючи реформу будівель та обладнання поліції. Стратегія припускає, що для досягнення довіри громади, відділення невідкладної допомоги повинно бути готовими відповісти на запитання. Їхня інфраструктура і потужність також має бути покращена [50].

Швеція підтримує Албанську державну поліцію (ASP) та Міністерство внутрішніх справ (MBC) з березня 2012 року з метою розвитку громадської поліції.

У період з червня 2010 року до квітня 2011 року ISSAT/DCAF допомагала Sida у підтримці MBC та ASP у розробці програми з посилення роботи поліції в громадах в Албанії. Перший етап співпраці розпочався у березні 2012 року та тривав до 2015 року. На жаль, проект не було запущено знову, поки другий етап не розпочався у січні 2017 року. Через кадрові зміни влітку 2017 року програму було припинено. По призначенню нового керівника програми та нових міжнародних експертів, програма була відновлена пізно восени 2017 року.

Підтримка SCPA полягала в наступному:

Підтримка охорони громадського порядку регіональними поліцейськими управліннями (RPD-CPS).

Компонент «Підтримка охорони громадського порядку регіональними поліцейськими департаментами» призначений для задоволення потреб у покращенні охорони громадського порядку на місцевому рівні. Області підтримки зосереджені на:

A. Аналіз прогалин у наданні послуг на місцевому рівні(нормативно-правовий механізм)

Було надано підтримку у проведенні аналізу прогалин у системі підпорядкування (наприклад, навички та процедури, пов'язані зі співробітниками громадської поліції, приймальні, відділами боротьби з побутовим насильством тощо).

B. Конкретні проекти для усунення цих прогалин(нормативно-правовий механізм)

Конкретні області, які можна розглянути, можуть включати: професійні навички, оперативні навички, навички управління та адміністрування, міжгалузеві вміння.

C. Матеріальна підтримка (економічний механізм)

Ця область зосереджена на зміцненні зусиль щодо покращення інфраструктури та може включати такі аспекти, як: підтримка у визначенні способів розміщення поліцейських станцій у існуючих громадських об'єктах (наприклад, офіси місцевих органів влади або громади, медичні установи, молодіжні центри тощо), допомога у покращенні інфраструктури.

D. Підвищення підзвітності поліції(інформаційно-комунікаційний механізм)

Це передбачає створення/зміцнення громадських груп для взаємодії з поліцією з метою обговорення місцевих проблем безпеки та охорони, визначення пріоритетів та притягнення поліції до відповідальності на місцевому рівні за свою роботу.

E. Кошти для підтримки поширення та тиражування успішних підходів в інших поліцейських організаціях. Включає в себе процедури та підходи для нових керівників поліції.(організаційний механізм)

F. Підтримка стратегічного управління (SMS)(організаційний механізм)

1. Розвиток потенціалу в галузі моніторингу та оцінки

Підтримка зосереджена на розвитку потенціалу в галузі моніторингу та оцінк), комунікацій та координації. На центральному рівні має бути підтримка у розвитку їх потенціалу зі збирання, аналізу та використання даних для обґрунтування управлінських та стратегічних рішень, а також для кращого інформування про свої досягнення інших установ та населення Албанії.

2. Комунікаційна підтримка

Зокрема, підтримка повинна бути надана для інституціоналізації процесу комунікації, необхідного для визначення місцевих пріоритетів, та запровадження більш децентралізованої системи комунікації, включаючи навички працівників поліції щодо роботи з населенням.

3. Координаційна підтримка

Зусилля мають бути зосереджені на підтримці координації різних місцевих суб'єктів, які працюють у сфері громадської безпеки та охорони.

Крім того програма реалізовує систему грантів для проєктів громадських організацій щодо покращення взаємодії поліції та громадян.

Робота поліції з населенням не є новою стратегією для албанської поліції (ASP), але уряд, у тому числі керівництво Міністерства внутрішніх справ та албанської поліції, приділяє йому дедалі більше уваги. Прийнято правові, політичні та адміністративні рішення.

У багатьох країнах взаємодія поліції з громадою є визнаною стратегією попередження злочинності, що має взаємопов'язані цілі: покращити сприйняття громадянами безпеки та захищеності, а також зміцнити інституційну та міжособистісну довіру у суспільстві.

Згідно з PSS опитування від травня 2018 року, 63% громадян Албанії вважають, що поліція виконує «хорошу» або «дуже хорошу» роботу. Той самий показник в опитуванні 2013 року становив 36%, а наступне опитування 2014 року показало, що покращення було досить суттєвим, і це також було пов'язано з масовими залученнями до роботи поліції громадян, проведеними шведським проєктом на першому етапі – 73%.

75% громадян Албанії заявляють, що почуваються «у безпеці» або «дуже безпечно», гуляючи своїми нічними районами. Той самий показник в опитуванні 2013 року становив 63%, а наступне опитування 2014 року показало покращення до 76%.

Основні фактори, що вплинули на гарний прогрес у досягненні деяких результатів на рівні кінцевих результатів, легко помітити:

- процес підготовки програми був ретельним із докладним техніко-економічним обґрунтуванням, за яким слідувала початкова фаза. Як керівництво Головних управлінь поліції, так і МВС брали активну участь, якщо не у всіх, то в багатьох кроках, що ведуть до міцного закріплення програми.

- у програми був перший етап, на якому було зроблено багато уроків.

- управлінська команда базується в Албанії, її очолюють албанці та доповнюють її міжнародні експерти, які мають ґрунтовні знання та досвід програм підвищення потенціалу поліції в різних умовах [48].

Усі вищеперераховані напрямки покращення взаємодії поліції з громадою показали свою ефективність на практиці. Тому можна з впевненістю говорити, що варто даний досвід пробувати запроваджувати в Україні, проте усе має бути детально проаналізовано і підлаштовано під українську культуру та громадян. На нашу думку, усі заходи мають бути апробовані поступово у вигляді пілотних проектів, аби не піддавати жодну з організацій під стрес і не спричинити як матеріальних ,так і фінансових втрат.

ВИСНОВКИ

У магістерській роботі з’ясовано теоретичні засади здійснення взаємодії кіберполіції та громади, проаналізовано механізми взаємодії кіберполіції та громати, здійснено характеристику даної взаємодії та визначено напрями покращення взаємодії кіберполіції та громади. Узагальнення зроблені в ході дослідження дозволили зробити та виділити ряд наукових положень:

1. Досліджено основні поняття та особливості взаємодії кіберполіції з громадою. Зокрема ми визначили суть понять «інформація», «кібербезпека», «кіберзлочин» а також місце кібербезпеки в системі національної безпеки. Описали характерні особливості зазначених понять та їх ознаки.

2. Охарактеризовано нормативно-правове забезпечення механізмів взаємодії кіберполіції та громади.

3. Проаналізовано основні показники роботи Департаменту кіберполіції за 2017-2020 роки. Відповідно до проаналізованих звітів нами було встановлено, що у 2018 році кількість викритих кіберзлочинів перевищувала 2019 та 2020 роки. Також нами було визначено, що кіберзлочинцями в більшості випадків стають чоловіки віком 25-40 років. Ми зазначили, що у 2020 році від здійснення кіберзлочинів державі було завдано матеріальних збитків на 241 млн. гривень, в той час як в 2019 році було завдано шкоди на 28 млн. гривень.

4. Охарактеризовано механізми взаємодії кіберполіції та громади та здійснено оцінку рівня взаємодії громадянами. Зокрема нами було виявлено, що система партнерської взаємодії інститутів громадянського суспільства і держави у сфері забезпечення кібербезпеки передбачає наявність:

- нормативно-правового механізму;
- соціального механізму;
- економічного механізму;
- інформаційно-комунікаційного механізму;
- організаційного механізму.

Також в рамках цього питання нами була розроблена анкета та проведено соціологічне опитування за допомогою гугл форми в соціальних мережах.

5. Досліджено шляхи вдосконалення механізмів взаємодії кіберполіції та громади. Було визначено, що проблемними є взаємодії з громадянами, органами місцевого самоврядування та приватним сектором.

6.Описано впровадження концепції «community policing» у взаємодії кіберполіції та громади. Зокрема ми розглянули та описали досвід успіщних реалізацій даної концепції у таких країнах як США та Албанія.

Відповідно до цього, було запропоновано основні шляхи поліпшення взаємодії, а саме:

Для налаштування ефективної взаємодії з органами місцевого самоврядування на нашу думку, необхідно виконати ряд важливих заходів, а саме:

1) визначення на державному рівні порядку взаємодії між кіберполіцією та органами місцевого самоврядування;
2) удосконалення нормативно-правової бази щодо питання взаємодії поліції та органів місцевого самоврядування;
3) в рамках децентралізації за прикладом інших держав можливе запровадження часткового фінансування з місцевих бюджетів, що дозволить більш повно враховувати потреби місцевого населення при здійсненні правоохоронної діяльності;
4) впровадження організаційних механізмів взаємодії з місцевими органами влади та самоврядування;
5) реалізація принципу community policing в операційній та управлінській діяльності кіберполіції;
6) побудова ефективної системи комунікації, пов’язаної з наданням державних послуг;
7) запровадження нових видів заходів-конференцій, де б поліція, органи місцевого самоврядування, активісти змогли обговорювати болючі питання та пропонувати шляхи їх вирішення;
8) проведення спільних форумів із залученням приватних ІТ-фірм;

9) запровадження функціонування загального форуму для обговорення та консультацій на теми, пов’язані з кіберзлочинністю;
10) спільна розробка та виконання проєктів;
11) надання фінансової та іншої необхідної підтримки особам, залученим до вирішення завдань, пов’язаних зі скороченням злочинності та підвищенням безпеки.
12) використання добровольців [34,с.9].
13) розробка кіберстандартів для приватного сектора;
14) збільшення частки інформування ІТ-компаній про відповідальність за кіберзлочини;
15) запровадження відповідальності за збиток спричинений незахищеними послугами та продуктами;
16) пошук нових заохочень для співпраці ІТ-компаній та кіберполіції
17) надання приватному та державному сектору фінансових стимулів для поліпшення кібернетичної безпеки;
18) впровадження форми співпраці ІТ-компанії з кіберполіцією на основі своєрідної реклами компанії (тобто використання назви компанії, яка допомогла в розкритті злочину в заголовках новин).

Завдяки цим заходам ми зможемо удосконалити механізм взаємодії з громадою та поліпшити процес розкриття кіберзлочинів. Що в подальшому дозволить зміцнити кібербезпеку країни, уникнути великих збитків та захистити кожного громадянина.

За умови успішної реалізації концепції, поліція та суспільство отримають ряд переваг, деякі з яких перераховані нижче.

Місцеві жителі зможуть повідомляти про свої проблеми поліції та стати партнерами у процесі пошуку індивідуалізованих рішень своїх проблем. Це, у свою чергу, сприятиме поліпшенню ситуації із запобіганням злочинності, підвищення рівня безпеки та забезпечення більш глибокого розуміння проблем безпеки.

Інші громадські структури також отримують вигоду від участі у вигляді поліцейської діяльності. Створюючи відносини з іншими організаціями на основі гармонійної взаємодії, і вносячи свій внесок у їхні зусилля, можуть заощадити

ресурси під час вирішення соціальних проблем. Більше того, успішне вирішення соціальних проблем дозволяє суттєву економію видатків.

Колективна відповідальність співробітників департаменту кіберполіції та зміцнення зв'язків та співпраці між департаментами, а також між поліцейськими, на оперативній роботі та їх безпосереднім керівництвом, сприяє загальному покращенню для робітника клімату.

Нарешті, велике розмаїття поставлених завдань і коло функцій, що розширилося, з одного боку, роблять роботу більш цікавою, і, з іншого боку, надають більш широкі можливості просування по службі у зв'язку з тим, що співробітник є цінним у багатьох відношеннях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Блокування небезпечного контенту в Україні: позиція кіберполіції:[сайт]. URL:https://24tv.ua/blokuvannya_nebezpechnogo_kontentu_v_ukrayini_pozitsiya_kiberpolitsiyi_n898634
2. Бугайчук К.Л., Шорохова Г.М. Забезпечення кібербезпеки як умова протидії терористичній діяльності: нормативно-правові аспекти. Протидія терористичній діяльності : міжнародний досвід і його актуальність для України : матеріали II Міжнародної науково-практичної конференції (15 грудня 2017 р.). Київ : Національна академія прокуратури України, 2018. С. 135–138.
3. Взаємодія органів внутрішніх справ із місцевими органами виконавчої влади та органами місцевого самоврядування у профілактиці адміністративних правопорушень: монографія. Ю.С. Назар. Львів: Львівський державний університет внутрішніх справ, 2012. 160 с.
4. Взаємодія поліції з громадою. Буклет за підтримки програми «Права людини та правосуддя» МФ «Відродження» 5 с.
5. Демкова М. Інформація як основа інформаційного суспільства: визначення поняття та правове регулювання Інформаційне Суспільство. Шлях України. К. : Фонд «Інформаційне суспільство України», 2004. 422 с.
6. Діордіца І.В. Поняття та зміст національної системи кібербезпеки. Національний юридичний журнал: Теорія та практика.2016 р. с. 37-429
7. Жогов В.С. Особливості трактування «кібербезпека» в сучасній юридичній науці. Правова держава. Випуск 33. 2019 р.С.128-134
8. Зарубіжний досвід організації взаємодії поліції з органами місцевого самоврядування в контексті децентралізації державної влади : наук.-метод. рек. К.Л. Бугайчук, В.А. Гузь, І.О. Святокум, В.В. Чумак. Харків : Харк. нац. ун-т. внутр. справ, 2015. 44 с.
9. Звіт Голови Національної поліції України про результати роботи відомства у 2019 році

10. Звіт Голови Національної поліції України С. Князєва про результати роботи відомства за 2018 рік
11. Звіт Національної поліції України про результати роботи у 2020 році
12. Кіберполіція розкрила статистику інтернет-злочинності з початку року.finance.ua:[сайт]. URL: https://news.finance.ua/ua/news/-/483006/kiberpolitsiya-rozkryla-statystyku-internet-zlochynnosti-z-pochatku-roku
13. Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. ратифікована 2005 року
14. Конвенція ООН про боротьбу проти незаконного обігу наркотичних засобів і психотропних речовин від 20 грудня 1998 р. ратифікована 1991 року
15. Конвенція про відмивання, пошук, арешт та конфіскацію доходів отриманих злочинним шляхом від 8 листопада 1990 р., ратифікована 1997 року
16. Конституція України від 28 червня 1996 р. Відомості Верховної Ради України. 1996. №30. Ст.141
17. Кримінальний кодекс України : Закон України від 05 квіт. 2001 р. № 2341-III. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n2
18. Міжнародна конвенція про боротьбу з фінансуванням тероризму від 9 грудня 1999р. ратифікована 2002 року
19. Національне антикорупційне бюро. Розкрадання коштів Міноборони: матеріали розслідування відкрито:[сайт]. URL: https://nabu.gov.ua/novyny/rozkradannya-koshtiv-minoborony-materialy-rozsliduvannya-vidkryto
20. Офіційний сайт Служби безпеки України:[сайт]. URL: https://ssu.gov.ua/novyny/u-2020-rotsi-sbu-neitralizuvala-600-kiberatak-i-vykryla-20-khakerskykh-uhrupovan

21. Про боротьбу з тероризмом: Закон України від 20 березня 2003 року № 638-IV. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text
22. Про Державну службу спеціального зв'язку та захисту інформації :Закон України від 23 лютого 2006 року № 3475-IV. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text
23. Про державну таємницю: Закон України від 21 січня 1994 року № 3855-XII. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
24. Про електронні комунікації : Закон України від 16 грудня 2020 року № 1089-IX. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text
25. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
26. Про заходи із протидії витоку службової інформації: Доручення МВС України від 19.03.2015 № 13155/Ав
27. Про запобігання негативним наслідкам використання інтернет-ресурсів російських провайдерів: Наказ Національної поліції України від 07.12.2015 № 176
28. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650.
29. Про місцеве самоврядування : Закон України від 21 травня 1997 року № 280/97-ВР. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80#Text
30. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

31. Про Національну поліцію : Закон України від 2 лип. 2015 р. № 580-VIII. Відомості Верховної Ради України. 2015. № 40–41. Ст. 379. URL:https://zakon.rada.gov.ua/laws/show/580-19.
32. Про Національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text
33. Про недопущення витоку інформації, що утворюється в службовій діяльності: Доручення МВС України від 24.04.2015 № 19130/Ав
34. Про основні засади забезпечення кібербезпеки: Закон України від 5 жовтня 2017 року № 2163-VIII. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
35. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.
36. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30 червня 1993 року № 3341-XII. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/3341-12#Text
37. Про проведення позачергового атестування осіб начальницького складу підрозділів боротьби з кіберзлочинністю: Наказ Міністерства Внутрішніх Справ від 15.10.2015 №1250
38. Про проведення конкурсу на заміщення вакантних посад старших інспекторів, інспекторів і спеціальних агентів інформаційних технологій міжрегіонального територіального органу Департаменту кіберполіції Національної поліції: Наказ Міністерства Внутрішніх Справ від 15.10.2015 № 1251
39. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": указ Президента України від 26 серпня 2021 року № 447/2021

40. Про телекомунікації: Закон України від 18 листопада 2003 року № 1280-IV. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text
41. Про утворення територіального органу Національної поліції:Наказ Кабінету Міністрів України №831 від 13 жовтня 2015 року
42. Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів Міжнарод. наук.-практ. конф. (27 травня 2020 р., м. Харків): МВС України, Харків. нац. ун-т внутр. справ ; Координатор проєктів ОБСЄ в Україні. Харків : ХНУВС, 2020. 224 с.
43. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації. Київ: BAITE, 2021. 262 с.
44. Шейхет С.О., Карпенко Ю.В. Концепція community policing як інструмент ефективної взаємодії Національної поліції, місцевих органів влади та громад: український та зарубіжний досвід упровадження: Вісник НАДУ. Серія “Державне управління”. 2018 р.
45. Шайхет С. О. Концепція community policing - зарубіжний досвід упровадження. Вісник Національної академії державного управління при Президентові України. Серія : Державне управління.2020.№ 4. С. 78-86. URL:: http://nbuv.gov.ua/UJRN/vnaddy_2018_4_13
46. Community Policing Defined: U.S. Department of Justice Office of Community Oriented Policing Services Washington,12
47. Good Practices in Building Police-Public Partnerships by the Senior Police Adviser to the OSCE Secretary General: Organization for Security and Cooperation in Europe (OSCE).
48. Jack R. Greene. POLICIES, PROCESSES, AND DECISIONS OF THE CRIMINAL JUSTICE SYSTEM: Community Policing in America: Changing the Nature, Structure, and Function of the Police.
49. Jocke Nyberg, PK Eriksson, Ani Plaku, Cajsa Hemström Albanian Police Capacity Building: From repressive force to serve communities with trust

Evaluation of Sweden's support to the programme "Strengthening Community Policing in Albania", second phase 2017–2020: Final Report June 2020

50. Rachel Neild. Themes and debates in public security. A manual for civil society Community Policing.
51. Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union. L 151/15, 7.6.2019
52. Ola Cami An Assessment of the Community Policing Strategy and Cooperation between the Albanian State Police and Local Government Institutions COMMUNITY POLICING IN ALBANIA 2007-2015.
53. 10 Ways Community Members Can Engage with Law Enforcement – URL: https://www.theiacp.org/news/blog-post/10-ways-community-members-can-engage-with-law-enforcement#reciteme-launch

ДОДАТКИ

Додаток А

Основні визначення поняття «інформація»

Автор	**Визначення інформації**
Закон України “Про інформацію”	Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.
Закон України “Про захист економічної конкуренції”	Інформація – це відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп’ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості.
Цивільний Кодекс України	Інформація – відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.
Є. Петров	Інформація – відомості (а не дані) про події та явища, які можуть бути пізнані особою та передані іншій особі у вигляді, придатному для сприйняття.
О. Синєокий	Інформація – відомості, що передаються усним, письмовим або іншим способом, зокрема за допомогою умовних сигналів, технічних засобів і т. п.
ВІНІТІ (1960-і рр.)	Інформація – об’єктивний зміст зв’язку між взаємодіючими матеріальними об’єктами, що виявляється в зміні станів цих об’єктів.
О. Золотар	Інформація – відомості про об’єктивно існуючі явища, які використовуються більш, ніж однією особою, незалежно від форми та способу надання у суспільних відносинах.
О. Підопригора, О. Святоцький	Інформація – певна сума знань про той чи інший об’єкт, які можна використати в доцільній діяльності людини.

Додаток Б

Основні визначення поняття «кібербезпека»

Автор	Визначення поняття «кібербезпека»
Закон України «Про основні засади забезпечення кібербезпеки»	Кібербезпека – це 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.
В. М. Бутузов	Кібербезпека – стан захищеності життєво важливих прав та інтересів людини, суспільства, держави в кіберпросторі від внутрішніх і зовнішніх протиправних посягань та загроз таких посягань.
Д .В. Дубов	Кібербезпека – стан захищеності інтересів людини і громадянина, суспільства та держави в кіберпросторі.
О. А. Баранов	Кібербезпека – це такий стан захищеності інтересів особистості, суспільства і держави в умовах використання комп’ютерних систем

	та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди.
В. М. Панченко	Кібербезпека означає безпеку об’єктів, які пов’язані з комп’ютерни ми технологіями, насамперед цифровими мережами (такими, що забезпечують зв’язок між обчислювальними пристроями – комп’ютерами, смартфонами, комунікаторами тощо); що вона є складовою безпеки інформаційної.
Т. Н. Ворожцова	Кібербезпека – це інформаційна безпека комп’ютерів та мереж, тобто сукупність технологій, процесів, методів, призначених для захисту комп’ютерного обладнання, інформації, програм, послуг від небажаного або несанкціонованого доступу.
В. Л. Бурячок	Кібербезпека – це стан захищеності кіберпростору держави в цілому чи окремих об’єктів її інфраструктури.

Додаток В

Основні визначення поняття «кіберзлочин»

Автор	**Визначення поняття «кіберзлочин»**
Закон України «Про основні засади забезпечення кібербезпеки»	Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України
О. Копатін, Є. Скулишин	Кіберзлочин – злочин, пов'язаний із використанням кібернетичних комп'ютерних систем, та злочин у кіберпросторі.
В.М. Болгов	Кіберзлочини - це сукупність передбачених чинним законодавством кримінально караних суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології,

	права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію
А. Русецький та Д. Куцолабський	Кіберзлочин – це протиправне винне діяння (дія або бездіяльність), яке передбачає втручання в дані персональних комп'ютерів, комп'ютерних програм і комп'ютерних мереж, або діяння, вчинене за допомогою комп'ютерів та інших сучасних технологій, за яке передбачається кримінальна відповідальність та яке може створити особисту небезпеку для громадян, загрозу національній безпеці держави та світовій безпеці.
В. Бєлєнький	Кіберзлочин – це винне, суспільно небезпечне, кримінально каране втручання в сферу безпеки обігу комп'ютерної інформації, роботу комп'ютерів, комп'ютерних програм,

	комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, зроблені за допомогою комп'ютерів, комп'ютерних мереж і програм, а також за допомогою інших пристроїв із вбудованими процесорами і контролерами, які можуть мати доступ до інформаційного простору.
Н. Ахтирська	Кіберзлочини – це кримінальні правопорушення, що вчиняються з використанням комп'ютерної техніки (комп'ютерів, пристроїв та іншого обладнання), інформаційних технологій, комп'ютерних систем та мереж з порушенням встановленого законом порядку інформаційної безпеки, незалежно від предмета посягання та сфери застосування.
О. Копан	Кіберзлочин (комп'ютерний злочин) – протиправне втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер (наприклад, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу й каналу зв'язку, використання шкідливого програмного забезпечення тощо).

Додаток Г

Порівняння соціальних взаємодій та структурних компонентів різних форм поліцейської діяльності

Структурні елементи	Традиційна поліцейська діяльність	Комунікативна поліцейська діяльність	Проблемно-орієнтовна поліцейська діяльність	Політика нульової терпимості поліцейської діяльності
Фокус поліцейської діяльності	Правовий примус	Громадське формування права з профілактикою злочинів	Право, порядок та основні проблеми	Наказовий порядок
Форма втручання	Неактивна, заснована на кримінальному праві	Активна, заснована на цивільному, кримінальному та адміністративному праві	Змішана, заснована на цивільному, кримінальному та адміністративному праві	Активна, використовує кримінальне, цивільне та адміністративне право
Діапазон поліцейської діяльності	Вузький, орієнтований на злочини	Вузький і підпорядкований громадськості та місцевим керівникам	Вузький, в основному підпорядкований поліцейському управлінню	Слабкий, в першу чергу підзвітний поліцейському управлінню
Основний напрямок культури поліції	Внутрішній, відштовхує суспільство	Зовнішній, налагоджує партнерські відносини	Змішаний, в залежності від проблеми, але	Внутрішній, зосереджений на атаці

			фокусується на аналізі	цільової проблеми
Прийняття управлінських рішень	Поліція мінімізує вплив оточуючих	Спільна відповідальність і оцінка	Різне, поліція виявляє проблему але задіює громадськість	Поліція має деякі зв'язки з іншими організаціями при необхідності
Комунікаційний обмін	Спадаючий, від поліції до громадськості	Горизонтальний, між поліцією і громадськістю	Горизонтальний, між поліцією і громадськістю	Спадаючий, від поліції до громадськості
Масштаби участі громадськості	Низький і пасивний	Високий і активний	Змішаний, в залежності від поставлених задач	Низький і пасивний
Зв'язки з іншими установами	Низьке, з перебоями	Участь і інтеграція в процес	Участь і інтеграція, в залежності від установленої проблеми	Помірно і періодично
Тип організаційного і командного напрямку	Централізоване командування і контроль	Децентралізоване із зв'язком з громадськістю	Децентралізоване місцеве командування підпорядковане центральному управлінню	Централізоване чи децентралізоване залежно від проблеми

Оцінка успіху	Кількість арештів і рівень злочинності	Різна, кримінал, дзвінки до служби, використання державних місць, громадські зв’язки і контакти.	Різні, вирішення проблем, їх мінімізація	Арешти, зупинки на місцях,скорочення комплексної діяльності

Додаток Д

Рівні змін в діяльності поліції з громадськістю

Рівень втручання	**Складові**	**Громадська поліція (результат)**
Зовнішнє середовище	Зв'язок з Зовнішніми організаціями і групами Політична і економічна підтримка Визначення і введення організаційного набору	Зниження злочинності Покращення рівня безпеки Більш широка громадська підтримка Зменшення небезпеки Вирішення громадських проблем Покращення зв’язків з місцевими органами влади та органами місцевого самоврядування
Організаційний	Технології Структура Культура Людські ресурси Оцінка ефективності	Зміни потоків інформації Прийняття рішень(стратегія) Прийняття рішень (тактика) Підвищення рівня підготовки Зміни символів і культури Підвищення комунікації Децентралізація Більш якісний аналіз

Груповий	Показники норм Склад групи Міжособистісні відносини Визначення завдань	Єдина команда Спільні рішення Якісні рішення Ефективність групи
Індивідуальний	Завдання особистості Самостійність Зворотній зв'язок Навички	Ефективний ріст поліцейських офіцерів Розширення діяльності Збільшення задоволеності роботою Розширення завдань Більша прив’язаність до роботи

Додаток Е

Анкета для оцінки рівня взаємодії кіберполіції та громади

1.Чи відомо вам, що таке кіберзлочин та яка настає відповідальність за скоєння такого злочину?

- так
- ні

2.Чи знаєте ви, які завдання покладені на кіберполіцію України?

- так
- ні

3.Чи були ви коли не будь залучені до співпраці з кіберполіцією?

- так
- ні

4.Як ви оцінюєте роботу кіберполіції України?

- високо
- середньо
- низько

5.Чи довіряєте ви кіберполіції України?

- так
- ні

6.Чи долучились би ви до співпраці з кіберполіцією якби вам запропонували?

- так
- ні

7. Як ви вважаєте потрібно законодавчо закріпити партнерство поліції та громади?

- так
- ні

8. Який на вашу думку зараз рівень взаємодії кіберполіції та громадян?

- високий

- середній
- низький

9.Чи на вашу думку є взаємодія між кіберполіцією та органами місцевого самоврядування?

- так
- ні

10.Чи зустрічали ви інформацію в інтернеті/телебаченні/газетах про затримання кіберзлочинців?

- так
- ні

11. На вашу думку інформація про кіберзлочини висвітлюється для громадян в широкому обсязі?

- так
- ні

12.Скажіть,чи вплине на ефективність роботи кіберполіції співпраця з громадянами?

- так
- ні

13.Чи варто на вашу думку поліпшувати взаємовідносини громади та поліції?

- так
- ні

14.Чи варто запроваджувати у школах/університетах обов'язкову дисципліну кібербезпеки?

- так
- ні

15. Що на вашу думку могло б поліпшити співпрацю кіберполіції з громадою?

Ваш варіант

Виконала: студентка магістратури за спеціальністю 281 Публічне управління та адміністрування денної форми навчання _____ Т.В. Волошина

Науковий керівник:
доцентка кафедри публічного управління та адміністрування, кандидатка наук з держ.упр., доцентка _____Л.П. Требик

Робота допущена до захисту:
завідувач кафедри публічного управління та адміністрування, д.держ.упр., доцент _____Е.В. Щепанський