УДК 342.95
DOI https://doi.org/10.32841/2307-1745.2020.48.28

Мамедова Е. А.
ад'юнкт кафедри адміністративного права, процесу та адміністративної діяльності Дніпропетровського державного університету внутрішніх справ

СОЦІАЛЬНІ МЕРЕЖІ ТА КІБЕРБЕЗПЕКА ПАТРУЛЬНОЇ ПОЛІЦІЇ

Анотація. Стаття присвячена дослідженню теорії і практики використання соціальних мереж працівниками патрульної поліції в аспекті забезпечення кібербезпеки службових інформаційних ресурсів та формулювання авторської позиції щодо вирішення наявних теоретичних і практичних питань. Звернена увага на те, що ступінь наукової розробленості окремих питань забезпечення кібербезпеки діяльності Національної поліції та використання соціальних мереж в їх роботі недостатній і потребує переосмислення й удосконалення. Доведено, що правоохоронні органи все частіше використовують аналіз соціальних мереж, щоб зрозуміти організацію злочинної діяльності, щоб виявити їх взаємозв'язок, а також для аналізу даних, які можуть бути використані для концентрації зусиль щодо попередження злочинності. Однак, за офіційними даними, кількість злочинних кібератак та неправдивих повідомлень про правопорушення у соціальних мережах збільшується, а працівники патрульної поліції не мають інструментарію та методики для протидії їм. Для удосконалення правового регулювання використання соціальних мереж в роботі патрульної поліції із дотриманням засад кібербезпеки запропоновано : розширювати співпрацю з іншими правоохоронними органами та зацікавленими сторонами в боротьбі зі злочинами у сфері технологій, а особливо підрозділами кіберполіції; посилити координацію та обмін досвідом у боротьбі з технологічними злочинами і їх розслідуванні; розробити та затвердити концепцію кібербезпеки МВС; закріпити у проекті Закону України «Про електронні комунікації» визначення поняття електронні соціальні мережі та зальні засади їх використання; у Правилах етичної поведінки поліцейських закріпити положення про принципи розміщення в соціальних мережах інформації; внести зміни до посадових інструкцій працівників відповідних підрозділів патрульної поліції, з метою конкретизації їх повноважень щодо висвітлення інформації про діяльність підрозділу в соціальних мережах та правоохоронного моніторингу, дотримання правил кібербезпеки і процесі такої комунікації; розробити методичні рекомендації та пам'ятки для працівників поліції щодо використання соціальних мереж та дотримання правил кібербезпеки.

Ключові слова*:* патрульна поліція, кібербезпека, соціальні мережі.

Постановка проблеми. Кібербезпека необхідна для захисту поліцейських управлінь від відключень, відволікаючих чинників, крадіжки даних і безлічі інших серйозних загроз. Сьогоднішні реалії такі, що департамент патрульної поліції і управління патрульної поліції в областях повинні бути готові до всіх загроз, і в сучасних умовах це можуть бути віруси, хакери тощо. Кібербезпека має вирішальне значення для поліцейських управлінь, щоб вони могли належним чином виконувати свою роботу і захищати населення. Адже інформаційні та комунікаційні технології є невід'ємною частиною нашого повсякденного життя. Незалежно від того, чи є у людей вдома комп'ютер, чи користуються вони послугами онлайн-банкінгу або просто отримують електроенергію, залежність спільноти від технологій зростає. Безпечна і надійне онлайн-середовище підвищує довіру і впевненість і сприяє стабільному і продуктивному суспільству.

Г.О. Блінова наголошує, що Конституція України забезпечення інформаційної безпеки відносить до найважливіших функцій держави. Вчена зазначає, що Концепція розвитку електронного урядування в Україні визначила недостатній рівень інформаційної безпеки та захисту інформації в інформаційно-телекомунікаційних системах органів влади, що вимагає вдосконалення державної політики в цій сфері та її першочергове рішення. Г.О. Блінова вказує на те, що Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки закріплює принцип цифровізації, тобто підвищення рівня довіри та безпеки, який визначає інформаційну, кібербезпеку, захист персональних даних, недоторканість особистого життя та права користувачів цифрових технологій, зміцнення та захист довіри в кіберпросторі передумовами цифрового розвитку та протидії супутнім ризикам [1, с. 26]. Такі ризики можуть проявлятись по різному та бути пов'язані із шкідливим програмним забезпеченням.

Віруси можуть відключати цілі комп'ютерні системи або окремі функціональні параметри. Управління та департаменти зберігають в своїх комп'ютерних системах конфіденційні дані про злочинців, поліцейських і цивільних осіб. З огляду на те, наскільки співробітники патрульної поліції покладаються і залежать від комп'ютерів, які використовують для спілкування з населенням та один з одним, це може серйозно підірвати їх здатність виконувати свою роботу. Навіть якщо передбачені дублюючі системи, для їх активації потрібен час. У результаті втрачається зв'язок між громадянами та правоохоронними органами. У такому випадку поліція повинна витрачати час, сили і фінансові кошти на усунення шкоди, завданої шкідливим комп'ютерними програмами, та відновлювати належний рівень інформаційного зв'язку між підрозділами та громадянами.

Проблеми кібербезпеки та використання соціальних мереж в службовій діяльності займались такі вчені, як О.А. Криклій та Л.Д. Павленко, О. Д. Довгань, Ю. В. Борсуковський, В. Ю. Биков, Г.О. Блінова, О.Ю. Буров, Н. П. Дементієвська, А. А. Стрєлкіна, Д. Д. Узун, Г. В. Форос, В. С. Жогов, Н.В. Коваленко, Л. В. Єрьоміна та інші. Праці вітчизняних та зарубіжних учених мають велике теоретичне і практичне значення. Однак ступінь наукової розробленості окремих питань забезпечення кібербезпеки діяльності Національної поліції та використання соціальних мереж в їх роботі недостатній і потребує переосмислення й удосконалення.

Метою статті є дослідження теорії і практики використання соціальних мереж працівниками Патрульної поліції

в аспекті забезпечення кібербезпеки службових інформаційних ресурсів та формулювання авторської позиції щодо вирішення наявних теоретичних і практичних питань. Дослідження розглядається як новаторське, що перевіряє організаційні теорії, пов'язані з використанням соціальних мереж патрульною поліцією, поточне дослідження викладає результати, які допомагають поглибити колективне розуміння теорії непередбачених обставин, інституціональної теорії і теорії залежності від ресурсів як основи для пояснення організаційної поведінки при роботі поліцейських.

Виклад основного матеріалу дослідження. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», МВС було включено до національної системи суб'єктів забезпечення кібербезпеки [2, с. 11]. У зв'язку з цим, на МВС було покладено повноваження щодо: створення і забезпечення функціонування підрозділів з протидії кіберзлочинності; розробки та реалізації комплексу організаційних і практичних заходів, спрямованих на боротьбу з кіберзлочинами; створення і забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги у розслідуванні кіберзлочинів, тощо [3]. В положеннях Закону «Про основи забезпечення кібербезпеки України» МВС віднесено до загальних суб'єктів забезпечення інституту [4; 5]. Водночас науковці не достатньо приділяють уваги визначенню змісту поняття кібербепека поліції, якого наразі не сформульовано. Проте питання кібербезпеки Патрульної поліції мають дуже актуальний характер.

Патрульна поліція часто має справу з помилковими викликами, з розіграшами та іншими відволікаючими факторами, але незахищений комп'ютерний зв'язок різко збільшує цей ризик. Наприклад, одна згубна програма може надіслати поліції помилкові повідомлення про злочини, підроблені інструкції керівників або інформацію, яка не має нічого спільного з роботою поліції. Це може спонукати патрульних відправитися в райони, де злочин фактично не здійснюється, відволікаючи їх від реальних проблем. Навіть якщо поліцейські зрозуміє, що їх службові інформаційні пристрої були зламані, вони не зможуть відрізнити справжні повідомлення від помилкових, що змусить їх ігнорувати законні накази про припинення злочинів. Таким чином, вони не зможуть правильно виконувати свою роботу, і їм доведеться витрачати час, гроші й зусилля на усунення проблеми. Правоохоронні органи все частіше використовують аналіз соціальних мереж, щоб зрозуміти організацію банд та інших злочинних мереж, щоб виявити їх відносин, а також для аналізу даних, які можуть бути використані для концентрації зусиль із запобігання злочинам.

Патрульна поліція України, як і багато інших організацій, знаходять способи використання соціальних мереж для поширення інформації серед населення. Представники поліції у великих містах виявляють, що їх громадяни очікують від них присутності в Інтернеті на таких платформах, як Twitter, Facebook і YouTube.

Наразі Інтернет використовують понад 4,5 мільярда людей, тоді як кількість користувачів соціальних мереж перетнула позначку в 3,8 мільярда. Майже 60% населення світу вже користується Інтернетом і понад 50% використовує соціальні мережі. Кількість користувачів соцмереж у 2020 році зросла на 9% або 321 мільйон нових користувачів в порівнянні з минулим роком [6]. Соціальні мережі використовуються для того щоб залишатися на зв'язку з друзями, родиною, колегами, клієнтами тощо. Соціальні мережі можуть мати соціальну мету, бізнес-мету або і те, і інше через такі сайти, як Facebook, Twitter, LinkedIn і Instagram тощо. Люди, котрі залучені до соціальних мереж, можуть робити це в особистих або ділових цілях. Ті, хто спілкуються на сайтах соціальних мереж в особистих цілях, спілкуються за допомогою різних засобів масової інформації для обговорення свого життя і інтересів. На відміну від традиційних соціальних структур, мережі здатні сприймати та самостійно створювати нові конфігурації спілкування, недоступні для традиційних установ. Основою такої компанії є мережева комунікація, однією з форм вираження є значне збільшення кількості соціальних мереж в Інтернеті [6].

Більшість відділів поліції України заявляють, що вони використовують соціальні мережі, і таке використання привертає велику увагу вчених. Правоохоронні органи все частіше використовують аналіз соціальних мереж, щоб зрозуміти організацію злочинної діяльності, щоб виявити їх взаємозв'язок, а також для аналізу даних, які можуть бути використані для концентрації зусиль щодо попередження злочинності. Аналіз соціальних мереж має безліч поточних і потенційних застосувань у правоохоронній діяльності, адже служба поліції, особливо після реформування стала більш технологічно залежної. Відповідно, процеси комунікації між поліцією, громадськістю, зацікавленими сторонами стали одним з найважливіших аспектів сучасної поліцейської діяльності. Правоохоронні органи вже використовують аналіз соціальних мереж в кримінальних розслідуваннях, збору розвідданих, моніторинг поведінки в соціальних мережах і прогнозну аналітику. Більшість сучасних способів використання Інтернет є продовженням історично сформованих методів роботи поліції і розслідувань, які були зосереджені навколо зв'язків між людьми, місцями та подіями.

На наш погляд, сьогодні роль правоохоронних органів розширилась внаслідок соціальних мереж, що дозволяють визначати місце перебування зниклих безвісти дітей, попереджати сусідів про підозрілу діяльність і навіть інформувати громадськість про злочини, що здійснюються в їх околицях. Наприклад, повідомити про ДТП, підпільну роботу грального автоматів, домашнє насильство або якийсь інший злочин чи інцидент можна без телефонного дзвінка на лінію «102», а пославши відповідну інформацію в соціальних мережах Патрульної поліції. Для оперативного повідомлення про різні події було створено додаток для екстреного виклику поліції My Pol, що запрацював у Києві. З його допомогою можна відправити сигнал SOS і викликати наряд поліції. Після підключення столиці, додаток покриває 23 обласних центри. Додаток My Pol - безкоштовний додаток, завантажити його можна в Google Play і Apple Store. Воно дозволяє швидко викликати правоохоронців навіть без дзвінка на 102. Додаток повноцінно працює у всіх областях України, крім Донецької, Луганської області та АР Крим. В My Pol доступні такі функції: кнопка SOS для екстреного виклику поліції; оцінка роботи поліцейських, можливість залишити відгук про конкретний оперативники; новинний розділ; повідомлення про екстрені ситуації й інших повідомленнях від Національної поліції України (НПУ); інтерактивна карта з усіма відділеннями поліції та лікарнями [7].

Як було визначено науковцем Волох О.К. у своєму дослідженні, що кібернетична безпека є складовою інформаційної безпеки. У свою чергу, інформаційна безпека є одним з елемен-

тів національної безпеки держави. На сьогодні у вітчизняній науці та юриспруденції немає єдиного підходу до визначення терміну «кібербезпека» [8, с. 106].

Закон України «Про Національну поліцію» у ст. 9 визначає засади відкритості та прозорості, згідно з якою поліція забезпечує постійне інформування органів державної влади та органів місцевого самоврядування, а також громадськості про свою діяльність у сфері охорони та захисту прав і свобод людини, протидії злочинності, забезпечення публічної безпеки та порядку [3]. Згідно з цим положення на офіційному веб-сайт МВС та НПУ розміщуються в актуальному стані інформаційні матеріали про діяльність підрозділів, нормативно-правова база, звіти, корисна інформація, а також новини. За допомогою вебсайта МВС та соціальних мереж є можливість повідомити про факти вчинення правопорушень. Також на офіційному каналі Нацполіції у YouTube, сторінках у соціальних мережах розміщуються коментарі щодо викриття злочинів та правопорушень вчиненими працівниками поліції. Відповідальними структурами здійснюється постійний моніторинг та аналіз матеріалів, розміщених у засобах масової інформації про антикорупційну діяльність органів та підрозділів НПУ. У випадках виявлення інформації про вчинення правоохоронцями правопорушень, фактів бездіяльності, неналежного виконання професійних обов'язків, а також фактів корупції та хабарництва з боку посадових осіб поліції систематично інформується Департамент кадрового забезпечення та Департамент внутрішньої безпеки НПУ. Так, у Департаменті патрульної поліції ця функція покладена на Управління моніторингу та аналітичного забезпечення ДПП. Випадки вчинення поліцейськими злочинів, зловживань не приховуються і висвітлюються у ЗМІ, зокрема відомчих [9], а також соціальних мережах.

На наш погляд, соціальні мережі - це двосічний інструмент. Терористи вербують членів і планують атаки за допомогою соціальних мереж, педофіли використовують платформи соціальних мереж для обміну фотографіями й відео. Соціальні мережі - це від 140-символьного твіту до 56-мегабайтного відеокліпу - сила, яку не можна заперечувати або ігнорувати. Але соціальні мережі теж роблять позитивний вплив. Платформи можуть використовуватися правоохоронними органами для розширення збору розвідданих і заручитися їхньою підтримкою. Технологія моніторингу соціальних мереж дає можливість постійно відстежувати і архівувати інформацію про діяльність мільйонів людей, і її можуть використовувати правоохоронні органи для перевірки повідомлень на предмет інформації про протести, потенційні загрози, останні новини та багато іншого.

Наприклад патрульний поліцейський приїжджаючи на виклик про зникнення людини, крім основних заходів з пошуку, поліцейський може звернутися до соціальних мереж, щоб встановити час останнього відвідування зниклого, встановити близьких друзів, місце останнього візиту і тощо.

Г.О. Блінова зазначає, що логічно побудована на єдиних засадах, з урахуванням європейських та міжнародних принципів, система інформаційного забезпечення органів публічної адміністрації, що включає усі державні електронні інформаційні ресурси, є основою цифрової держави в Україні. Ця вчена навіть запропонувала прийняти Закон України «інформаційного забезпечення органів публічної адміністрації» з метою систематизацію, упорядкування, удосконалення адміністративно-правових засад інформаційного забезпечення органів публічної адміністрації та стандартизації використання електронних засобів та ресурсів органами публічної адміністрації, удосконалення норм чинного та перспективного законодавства України у цій сфері, а також гармонізація із законодавством Європейського Союзу. Цей нормативно-правовий акт, на думку Блінової Г.О., повинен містити розділ присвячений засадам кібербезпеки України та включати такі принципи: відкритості, доступності, стабільності та захищеності кіберпростору; пріоритетності запобіжних заходів; консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущенні використання кіберпростору в протиправних та воєнних цілях; забезпечення демократичного цивільного контролю над утвореними, відповідно до законів України, військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки тощо [10, с. 67-68]. Удосконалення інформаційного законодавства, що регулює відносини кібербезпеки, на зазначених засадах повинно охоплювати і сферу діяльності ЗМІ.

На сьогодні основними нормативно-правовими актами, що визначають правові засади діяльності мас-медіа в інтернеті є Закони України «Про інформацію» [11], «Про телебачення і радіомовлення» [12], «Про друковані засоби масової інформації (пресу) в Україні» [13], «Про пресу та інші засоби масової інформації» [14], «Про електронні комунікації» [15]. Закон України «Про інформацію» визначає, що засоби масової інформації це засоби, призначені для публічного поширення друкованої або аудіовізуальної інформації [11]. Закон «Про пресу та інші засоби масової інформації» під масовою інформацією розуміє публічно розповсюджувані друковані, аудіо- та аудіовізуальні повідомлення і матеріали; під засобами масової інформації розуміються газети, журнали, теле- і радіопрограми, кінодокументалістика, інші періодичні форми публічного розповсюдження масової інформації. Згідно з цим нормативно-правового акту засоби масової інформації репрезентуються редакціями періодичної преси, теле- і радіомовлення (інформаційними агентствами, іншими установами, які здійснюють випуск масової інформації) [11; 12]. Таким чином, можна підсумувати, що соціальні мережі мають ознаки засобів масової інформації, а саме: 1) здійснюються періодичне публічне розповсюдження масової інформації; 2) поширюють масову інформацію, тобто публічно розповсюджують друковані, аудіо- та аудіовізуальні повідомлення і матеріали; 3) висвітлюють інформацію періодично, тобто не рідше одного разу на рік.

Висновки. Для удосконалення правового регулювання використання соціальних мереж в роботі патрульної поліції із дотриманням засад кібербезпеки ми пропонуємо: 1) розширювати співпрацю з іншими правоохоронними органами та зацікавленими сторонами в боротьбі зі злочинами у сфері технологій; 2) посилити координацію та обмін досвідом у боротьбі з технологічними злочинами і їх розслідуванні; 3) розробити та затвердити відповідну концепцію МВС; 4) закріпити у проекті Закону України «Про електронні комунікації» визначення поняття електронні соціальні мережі та загальні засади їх використання; 5) у Правилах етичної поведінки поліцейських закріпити положення про принципи розміщення в соціальних мережах інформації; 6) ввести зміни до посадових інструкцій працівників відповідних підрозділів патрульної поліції, з метою конкретизації їх повноважень щодо висвітлення інформації про діяльність підрозділу в соціальних мережах та пра-

воохоронного моніторингу, дотримання правил кібербезпеки і процесі такої комунікації; 7) розробити методичні рекомендації та пам'ятки для працівників поліції щодо використання соціальних мереж.

Організаційними заходами, що сприятимуть підвищенню ефективності використання соціальних мереж в роботі патрульної поліції є розробка відповідного навчального тренінгу для поліцейських, а також проведення тренінгів, інструктажів та роз'яснювальної роботи серед працівників поліції щодо розміщення інформації на своїх сторінках соцмереж відомостей із врахуванням вимог етичної поведінки, кібербезпеки та норм вітчизняного законодавства.

Література:

1. Блинова А.А. Информационная безопасность органов публичной администрации в Украине. Legea si Viata. № 2. 2019 p. P. 26 – 30.
2. Бочковий О.В., Блінова Г.О., Прокопов С.О., Мамедова Є.А. Інформаційне забезпечення діяльності патрульної поліції: науково-практичні рекомендації. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 112 с.
3. Про Національну поліцію: Закон України від 2 липня 2015 року № 580-VIII. *Відомості Верховної Ради*. 2015. № 40-41. ст.379
4. Бухарев В.В. Адміністративно-правові засади забезпечення кібербезпеки України .дис на здобут наук ступ канд. юрид наук. Суми. 2018. 221 с. URL: https://core.ac.uk/download/pdf/324216462.pdf
5. Про основи забезпечення кібербезпеки України. Закон Укріани від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Що переможе – цифра або слово? 2020. URL: http://universe.zp.ua/?p=27150.
7. В Україні запрацював додаток для термінового виклику поліції My Pol. 2019 Інформаційне агентство ASPI. URL: https://aspi.com.ua/news/suspilstvo/v-ukraini-zapracyuvav-dodatok-dlya-terminovogo-vikliku-policii-my-pol#gsc.tab=0.
8. Волох О.К. Питання кібернетичної безпеки в умовах розбудови інформаційного суспільства. *Юридичний науковий електронний журнал*. № 4, 2016. С. 104-107. URL: http://www.lsej.org.ua/4_2016/29.pdf.
9. Розбудова цілісності і доброчесності під час реформування поліції. Досвід України : аналіт. доп. та матер. спеціаліз. Міжнар. конф. (17 квіт. 2019 р., м. Київ) / [за ред. О. Д. Маркєєвої та Л. І. Полякова] ; Національний інститут стратегічних досліджень ; Центр досліджень армії, конверсії та роззброєння ; Женевський центр безпекового урядування. Київ : НІСД, 2019. 112 с.
10. Блінова Г.О. Адмінітративно-правові засади інформаційного забезпечення органів публічної адмінітсрації в Україні: актуальні питання теорії та практики. Дис. на здобут. наук. ступ. докт. Юрид. наук. Запоріжжя. 2019. 458 с. С. 67-68
11. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
12. Про телебачення і радіомовлення: Закон України від 21 грудня 1993 року № 3759-XII. URL: https://zakon.rada.gov.ua/laws/show/3759-12/print
13. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16 листопада 1992 року № 2782-XII. *Голос України* від 08.12.1992
14. Про пресу та інші засоби масової інформації: Закон СРСР від 12 червня 1990 р. N 1552-I. URL: https://zakon.rada.gov.ua/laws/show/v1552400-90#Text
15. Про електронні комунікації : Проект Закон України від 05 лютого 2020 року № 3014 . URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68059

Mamedova E. Social networks and cybersecurity of the patrol police.

Summary. The article is devoted to the study of the theory and practice of using social networks by patrol police officers in terms of cybersecurity of official information resources and the formulation of the author's position on addressing existing theoretical and practical issues. Attention is drawn to the fact that the degree of scientific development of certain issues of cybersecurity of the National Police and the use of social networks in their work is insufficient and needs to be rethought and improved. It has been shown that law enforcement agencies are increasingly using social media analysis to understand the organization of criminal activity, to identify their relationship, as well as to analyze data that can be used to concentrate efforts to prevent crime. However, according to official data, the number of criminal cyberattacks and false reports of offenses on social networks is increasing, and patrol police officers do not have the tools and techniques to counter them. To improve the legal regulation of the use of social networks in the work of patrol police in compliance with the principles of cybersecurity, it is proposed: to expand cooperation with other law enforcement agencies and stakeholders in combating crimes in technology, especially cyberpolice units; strengthen coordination and exchange of experience in the fight against technological crimes and their investigation; develop and approve the concept of cybersecurity of the Ministry of Internal Affairs; to enshrine in the draft Law of Ukraine "On Electronic Communications" the definition of electronic social networks and the general principles of their use; to enshrine in the Rules of Ethical Conduct of Police Officers the principles of posting information on social networks; make changes to the job descriptions of employees of the relevant patrol police units, in order to specify their powers to cover information about the activities of the unit on social networks and law enforcement monitoring, compliance with cybersecurity rules and the process of such communication; develop guidelines and guides for police officers on the use of social networks and compliance with cybersecurity rules.

Key words: patrol police, cybersecurity, social networks.