http://www.bhiva.org/documents/Guidelines/Pregnancy/2012/hiv1030_6.pdf. (дата звернення: 04.12.2022).

2. ВІЛ/СНІД та права людини. Міжнародні керівні принципи». ООН, ЮНЕЙДС. 1996 р. 31 с.

3. Керівні принципи для виявлення та ведення випадків споживання хімічних речовин та пов'язаних з цим розладів здоров'я під час вагітності. ВООЗ. 2014. 39 с.

4. Соціально-демографічні та медичні детермінанти ризику передачі ВІЛ від матері до дитини в Україні» (анотований звіт ДУ «Український центр контролю за соцхворобами МОЗ України», ЮНІСЕФ, Інститут соціології НАН України»), 2013.

УДК 342.9

Мамедова Е.А., ад'юнкт Дніпропетровського державного університету внутрішніх справ

(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

Науковий керівник: Блінова Г.О., д.ю.н., доцентка, професорка кафедри цивільного, господарського та екологічного права

(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

КІБЕРБЕЗПЕКА ПАТРУЛЬНОЇ ПОЛІЦІЇ: ПІДХОДИ ДО ВИЗНАЧЕННЯ ПОНЯТТЯ НАУКОВЦЯМИ ТА ПРАКТИКАМИ

У галузі забезпечення кібербезпеки, вважає В. В. Бухарев, Національна поліція України наділена повноваженнями щодо забезпечення прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі [1]. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», МВС було включено до національної системи суб'єктів забезпечення кібербезпеки, через що 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 [1]. В положеннях Закону «Про основні засади забезпечення кібербезпеки України» МВС віднесено до загальних суб'єктів забезпечення інституту [2]. Водночас науковці не достатньо приділяють уваги визначенню змісту поняття кібербезпека поліції, якого на сьогодні не сформульовано.

Відсутність достатньої уваги до питань організаційно-правового забезпечення кібербезпеки патрульної поліції призводить до реалізації загроз у цій сфері. Одна з останніх таких кібератак сталася 23 вересня 2020 року, коли на деяких інтернет-сторінках обласних управлінь Національної поліції була поширена неправдива інформація, у якій повідомлялося про викид радіоактивних речовин на 3-му енергоблоці Рівненської АЕС [3]. На той момент сайт Національної поліції та відповідно інтернет-сайти інших головних управлінь поліції були відключені. Департамент патрульної поліції був змушений відключити базу ІПС «Армор», що не давало змоги патрульним поліцейським здійснювати перевірку осіб, транспортних засобів, також виносити електронні постанови правопорушникам. На той момент виклики на спеціальну лінію «102» приймалися і передавалися до чергової частини, своєю чергою, чергова частина патрульної поліції також виявилася без зв'язку. Не бачивши на моніторі карти знаходження патрулів, черговий був змушений відправляти будь-який й орієнтуватися тільки на квадрат прив'язки патруля, в якому екіпаж не завжди знаходився. Виклики спецлінії «102» оголошувалися по радіозв'язку, який, як ми знаємо, не є захищеним,

також в телефонному режимі. Черговий не бачив рапорту про виконану роботу на виклик і час завершення виклику, щоб направити екіпаж за наступною адресою. Це призвело до черги необслуговуваних викликів, громадяни не отримали ту допомогу, якої потребували в ту хвилину.

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення кібербезпеки: це є захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [2].

Кібербезпеку як об'єкт адміністративно-правової охорони В. В. Бухарев визначає як певний правовий інститут, охорона якого відбувається в межах норм адміністративного права та здійснюється окремими державними органами на засадах імперативності та ієрархічності. Цей науковець визначає такі особливості кібербезпеки як об'єкта адміністративно-правової охорони: а) відсутність чіткого визначення змісту адміністративно-правової охорони кібербезпеки; б) адміністративно-правова охорона кібербезпеки хоча і являє собою єдиний юридичний інститут, проте закріплюється у нормах різних нормативно-правових актів, якими регулюється діяльність відповідних органів державної влади; в) її забезпечення здійснюється не тільки у правовідносинах, які виникають у сфері вчинення адміністративних правопорушень. Інститут має більш широкий обсяг застосування, який передбачає не тільки припинення відповідних порушень, а також їх попередження; г) основні засади забезпечення кібербезпеки лише нещодавно знайшли своє закріплення у відповідному нормативно-правовому акті – Законі України «Про основні засади забезпечення кібербезпеки України»; ґ) має місце спеціальний понятійний апарат [5, с. 94]. Науковий стан вивчення змісту поняття кібербезпека патрульної поліції не дозволяє дослідити сформульовані відповідні поняття через їх відсутність.

Водночас поняття кібербезпеки тісно пов'язано із поняттям інформаційної безпеки, оскільки є похідним від останнього. В. А. Веклич та Д. П. Кисленко, визначили інформаційну безпеку поліції охорони як захист інформаційної сфери поліції охорони від внутрішніх та зовнішніх загроз. На їх думку, інформаційна безпека поліції охорони полягає у спроможності працівників поліції охорони убезпечити інформаційні ресурси від несанкціонованого доступу до них, та унеможливити витоки службової інформації. Забезпечення інформаційної безпеки в діяльності поліції охорони здійснюється через: організаційно-аналітичне управління; управління технічної охорони; відділ правового забезпечення; режимно-секретний сектор Департаменту поліції охорони – структурні служби Департаменту поліції охорони, які забезпечують правове та організаційнотехнічне забезпечення інформаційної безпеки в діяльності поліції охорони. Поліція охорони Національної поліції України, зазначають В.А. Веклич та Д.П. Кисленко, є складовою частиною системи інформаційної безпеки. Забезпечення інформаційної безпеки поліції охорони здійснюється відповідно до встановлених законом повноважень та спрямоване на своєчасне виявлення, запобігання та припинення загроз в її інформаційному просторі [6, с. 59].

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

У результаті опитування 231 патрульного поліцейського, що проводилося методом анкетного он-лайн опитування за допомогою Google форм, було виявлено наступні тенденції у розумінні ними змісту поняття «кібербезпека» та її правового регулювання в діяльності патрульної поліції.

Документи, в яких визначені правила дотримання кібербезпеки в роботі патрульної поліції, на думку опитаних працінників, це перш за все Закон України «Про захист інформації в інформаційно-комунікаційних системах» - зазначили 71,9% опитаних та Закон України «Про основні засади забезпечення кібербезпеки України» - так вважають 68,8% поліцейських. В Конституції України та в Законі України «Про Національну поліцію» також на думку опитаних зазначені правила – 36,8% та 34,2% відповідно. Менше опитаних вважають, що ці правила визначені в документі «Стратегія інформаційної безпеки» - 24,2%. В таких документах як «Дисциплінарний статут Національної поліції України» та «Внутрішні правила та інструкції патрульної поліції» менше всього визначені правила дотримання кібербезпеки в роботі патрульної поліції – 7,8% та 5,2% відповідно.

Думки опитаних щодо розуміння поняття «кібербезпека» розділилися майже порівну між такими поняттями: «сукупність методів захисту у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами і їх впровадження з точки зору конфіденційності, цілісності і доступності» - 46,8% та «стан захищеності життєво важливих інтересів громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій» - 42,0%. Лише для 10,4% поліцейських «кібербезпека» - це «здатність людини, суспільства і держави запобігати та протидіяти цілеспрямованим негативним впливам і несанкціонованому управлінню інформаційними ресурсами із застосуванням телекомунікаційних та інформаційно-комунікаційних систем і мереж».

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

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

Отже, ми робимо висновки, що патрульна поліція повинна не відставати від технологічного розвитку і мати необхідні знання та навички для боротьби з цифровою злочинністю, що зростає, на національному, регіональному та міжнародному рівнях. Вирішення проблеми інформаційного супроводження, а саме налагодження комунікації між поліцейськими, поліпшення радіозв’язку, мобільного устаткування, забезпечення кібербезпеки патрульної поліції повинно стати пріоритетами державної політики у сфері інформаційного забезпечення правоохоронних органів України. Удосконалення

законодавчого регулювання механізму пошуку, фіксації, блокування і видалення з інформаційного простору держави, зокрема з українського сегмента мережі «Інтернет», інформації, яка загрожує життю або здоров'ю громадян України, сприятиме також створенню в патрульній поліції України інтегрованої інформаційної системи оцінки загроз та швидкого реагування на них.

Список використаних джерел:

1. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. Відомості Верховної Ради України. 2015. № 40–41. С. 1970. Ст. 379.

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

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

4. Бухарев В. В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. … канд. юрид наук. Суми, 2018. 221 с. URL: https://core.ac.uk/download/pdf/324216462.pdf

5. Бухарев В. В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. … канд. юрид наук. Суми, 2018. 221 с. URL: https://core.ac.uk/download/pdf/324216462.pdf

6. Веклич В. А., Кисленко Д. П. Інформаційна безпека майбутніх фахівців поліції охорони. Наукові записки Центральноукраїнського державного педагогічного університету імені Володимира Винниченка. Серія : Педагогічні науки. 2017. Вип. 159. С. 57–61. URL: http://nbuv.gov.ua/UJRN/Nz_p_2017_159_10.

УДК 342.9

Чалик В.Р., викладач кафедри загальноправових дисциплін
(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)
Науковий керівник: Блінова Г.О., д.ю.н., доцентка, професорка кафедри цивільного, господарського та екологічного права
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

ПРАВОВЕ РЕГУЛЮВАННЯ ТРАНСФОРМАЦІЇ ІНФОРМАЦІЙНИХ ВІДНОСИН У СОЦІАЛЬНІЙ СФЕРІ

Чинна система надання соціальних послуг, соціального захисту населення має недоліки різного характеру, що спричиняє зниження рівня реалізації соціальних прав громадян. Одним з таких чинників є недоліки інформаційного забезпечення соціальної сфери. На необхідність удосконалення цього аспекту функціонування соціальної інфраструктури вказують як нормативно-правові акти так і науковці. Так, у Концепції реалізації державної політики щодо соціального захисту населення та захисту прав дітей [1] серед кола проблем соціальної сфери виокремлено і необхідність удосконалення правового регулювання інформаційних відносин у соціальній сфері. На проблему неналежного рівня інформаційної взаємодії влади та населення у процесі функціонування системи надання соціальних послуг, вказують також науковці, наприклад М.В. Кравченко у своїй монографії [2, с. 244-255]. Таким чином інформаційні відносини є невід'ємною частиною механізму реалізації та захисту соціальних прав громадян.

Інформаційний складник, вважає С. Семяніста, є безумовною характеристикою усіх соціальних систем суспільства [3, с. 104]. Особливо це твердження в сучасний період справедливе для публічного управління. З урахуванням загальної тенденції цифровізації в України було прийнято Стратегію цифрової трансформації соціальної