«49) спільно з Міністерством внутрішніх справ України організовує боротьбу з тероризмом шляхом антитерористичного забезпечення об'єктів можливих терористичних посягань;

50) здійснює контроль за дотриманням фізичними та юридичними особами вимог антитерористичного забезпечення об'єктів можливих терористичних посягань».

1. Про Концепцію боротьби з тероризмом в Україні : Указ Президента України від 05.03.2019 р. № 53/2019. URL : https://zakon.rada.gov.ua/laws/show/53/2019#Text.

2. Проект Закону про внесення змін до Кодексу України про адміністративні правопорушення та Закону України «Про боротьбу з тероризмом» щодо вдосконалення заходів, спрямованих на запобігання тероризму від 20.02.2024 № 11030. *Верховна Рада України*. URL : https://itd.rada.gov.ua/billInfo/Bills/Card/43735.

3. Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984. URL : https://zakon.rada.gov.ua/laws/show/80731-10.

4. Про боротьбу з тероризмом : Закон України 20 березня 2003 р. URL : https://zakon.rada.gov.ua/laws/show/638-15#Text.

5. Про Національну поліцію : Закон України від 02.07.2015. URL : https://zakon.rada.gov.ua/laws/show/580-19/conv#Text.

УДК 342.95+351.74
DOI: 10.31733/15-03-2024/1/84-86

**Катерина ГЛУХОВЕРЯ**
начальник відділу
докторантури та аспірантури
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук

## МЕХАНІЗМИ ЗАПОБІГАННЯ ПОШИРЕННЮ СЕКРЕТНОЇ ІНФОРМАЦІЇ

В умовах збройної агресії та війни інформація набуває суттєво іншої питомої ваги, ніж у мирний час. Фактично вона сама собою перетворюється на один із видів зброї. Власне, тому ми і живемо в умовах нового виду війни – гібридної, де саме інформаційна складова є активною як на етапах підготовки (наприклад, суспільної думки, деморалізації противника і населення відповідних територій, завдання морально-психологічних втрат тощо), так і у самому процесі. Як відомо, існують фейки, інформаційно-психологічні операції, пропаганда, контрпропаганда тощо, однак у інформації є й інша сторона – її захист, оскільки саме достовірність інформації про ворога становить ключовий інтерес військових та військово-політичного керівництва у прийнятті тих чи інших рішень. Це інформація з обмеженим доступом, яка відсутня у публічному просторі, а тому вона має чітке і лаконічне визначення – секретна.

Відповідно до термінології, визначеної Законом України «Про державну таємницю», секретною є інформація, що належить до таємної та охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом, державною таємницею і підлягають охороні державою [1]. Це є вичерпний перелік масиву даних, що обов'язково і передусім враховується ворогом, а також становить оперативний інтерес для добування відповідними розвідувальними службами. З іншого боку, така інформація перебуває під особливим захистом держави та відповідних осіб, що є її носіями, а розповсюдження її веде до певних наслідків.

Загалом чинне законодавство передбачає, що порушення режиму секретності може призводити до усього спектра видів відповідальності. Так, дисциплінарна відповідальність наступає згідно з наказом МВС України № 893 від 07.11.2018 «Про реалізацію окремих положень Дисциплінарного статуту Національної поліції України», де у п. 2 Розділу ІІ відмічається: «Службове розслідування призначається, зокрема, за наявності даних про (в т.ч): «втрату поліцейським… матеріалів досудового розслідування, справ оперативного

обліку та справ про адміністративні правопорушення, речових доказів…»; «розголошення конфіденційної, таємної, службової або іншої інформації, яка містить таємницю, що охороняється законом» [2].

Щодо адміністративної відповідальності, то доцільно згадати ст. 212-2 Кодексу України про адміністративні правопорушення, яка визначає, що «порушення законодавства про державну таємницю тягне за собою накладення штрафу на громадян від десяти до тридцяти неоподатковуваних мінімумів доходів громадян і на посадових осіб – від тридцяти до ста неоподатковуваних мінімумів доходів громадян» [3].

Також передбачена і кримінальна відповідальність згідно зі ст. ст. 328–330 Кримінального кодексу України, а саме: «Розголошення державної таємниці», «Втрата документів, що містять державну таємницю», «Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни» [4].

Однак слід розуміти, що відповідальність – це передусім про наслідки за фактами втрати такої інформації, однак не про превенцію, протидію і, тим більше, її захист. Проте, якщо навіть просто оцінити новинну стрічку, такі випадки далеко не поодинокі, а мають системний характер, причини чому названі нами ще на самому початку. І надалі державні органи продовжуватимуть стикатися з поширенням саме секретної інформації, тим більше що вона все більше цифровізується, а отже, набуває більш доступної форми, ще і за умов більшої анонімізації. За таких умов, доцільно звернути увагу як на міжнародний досвід, так і на рекомендації наукової спільноти щодо посилення захисту і запобігання витокам:

1) аутентифікація та управління доступом. Так, зважаючи на те, що загальноприйняті схеми аутентифікації та управління доступом у більшості своїй вже є застарілими та не забезпечують належний рівень захисту, доцільним буде використання спеціалізованих сервісів управління правами доступу до електронних документів, які вже досить широко представлені і мають різну доступність і складність;

2) RMS (Rights Management Services, або сервіси управління правами доступу). Являють собою технології, що використовуються для захисту цифрових документів від несанкціонованого використання. Основною відмінністю зазначеного рішення є те, що відповідно визначені обмеження зберігаються в тілі самого документа, а також працюють незалежно від його місцезнаходження. Також на користь технології працює і те, що шифрування, реалізоване в ній, забороняє отримувати доступ до їхнього змісту будь-якими обхідними шляхами;

3) Сервіси безпеки. Інструменти, які використовуються для обмеження доступу до інформації, належної фіксації фактів такого доступу, а також контролю інформаційної активності. Вони дозволяють попередити та запобігти, виявити та у відповідний спосіб реагувати на ситуації, що пов’язані з витоком інформації;

4) Фільтрація контенту. Це метод аналізу змісту інформаційного масиву даних за ключовими словами, що за вмілого застосування може бути досить ефективним. Складність полягає у досить затратному часовому ресурсі, який передбачає суттєву роботу зі вдосконалення системи фільтрації контенту, оскільки динаміка потоків інформації вимагає і не менш динамічного вдосконалення самої системи. Навіть блискуче і ефективно налагоджена система фільтрації буде вимагати через певний час втручання і регулювання з боку адміністратора безпеки;

5) Шифрування інформації. Вже понад дві тисячі років саме цей метод вважається одним із найбільш ефективних і надійних способів забезпечення конфіденційності інформації. Криптографічні методи представлені дуже широко у світі, від найпростіших (алфавітних) до складних цифрових. Однак слабкою ланкою є ключі дешифровки, які теж будуть об’єктом посиленої уваги як тих, хто намагатиметься заволодіти інформацією, так і стороною, що хоче її вберегти;

6) Аудит безпеки. Ця процедура є останнім етапом комплексної системи запобігання витоку інформації та підсистемою аудиту інформаційної безпеки. Вона дає можливість достатньо якісно і оперативно виявляти та реагувати на порушення цілісності безпекового контору та отримувати матеріали для проведення розслідувань відповідних інцидентів. Такий аудит має охоплювати всі види подій, пов’язаних із набуттям доступу до секретних (таємних грифованих) даних та здійсненням комплексу дій, які можуть призвести до їх несанкціонованого розкриття, включаючи зміну прав доступу, копіювання та роздруківку.

Безумовно, що це є лише загальними напрямами для вдосконалення систем безпеки захисту інформації, однак саме вони є найбільш стабільними і перевіреними навіть в умовах

війни. Водночас посилення відповідальності за подібні дії вбачається нами найменш перспективним заходом, особливо зважаючи на те, що намагання заволодіти інформацією може здійснюватися з будь-якої точки світу.

1. Про державну таємницю : Закон України від 21.01.1994. URL : https://zakon.rada.gov.ua/laws/show/3855-12#Text.
2. Про реалізацію окремих положень Дисциплінарного статуту Національної поліції України : наказ МВС України від 07.11.2018 № 893. URL : https://zakon.rada.gov.ua/laws/show/z1355-18#Text.
3. Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984. URL : https://zakon.rada.gov.ua/laws/show/80731-10.
4. Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

УДК 351.74
DOI: 10.31733/15-03-2024/1/86-88

**Олексій КАМИШАНСЬКИЙ**
декан факультету підготовки
фахівців для підрозділів
превентивної діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук

## ТРАНСФОРМАЦІЯ СИСТЕМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ

З початком повномасштабної збройної агресії, розпочатої росією проти України 24 лютого 2022 р., система Національної поліції України зазнає впливу дестабілізуючих чинників та змушена адаптуватися до нових викликів та реалій. Значною мірою це пов'язане із тим, що чинний курс на розвиток Національної поліції як правоохоронної інституції, заснованої на європейських стандартах і принципах «Community Policing», не відповідає існуючим загрозам для публічної безпеки і порядку в умовах воєнного стану.

Як наслідок, було внесено низку змін і доповнень до Закону України «Про Національну поліцію» від 02.07.2015 [1], які стосувалися переважно трансформації функціонування поліції в особливих правових умовах воєнного стану. До таких новел можна віднести припинення громадського контролю за діяльністю поліції на такий період (ст. 90-1 «Особливості громадського контролю за діяльністю поліції під час дії воєнного стану») [1]. Сюди ж слід віднести зміну парадигми взаємодії поліції та суспільства на засадах партнерства, яка знайшла широку підтримку у вітчизняних наукових колах [2].

Не відкидаючи важливості законодавчих змін і доповнень до Закону України «Про Національну поліцію» у зв'язку із дією воєнного стану, зосередимо увагу на проблемних питаннях трансформації системи Національної поліції України.

Насамперед слід вказати, що відповідно до ст. 13 Закону України «Про Національну поліцію» систему поліції складають: 1) центральний орган управління поліції (апарат); 2) територіальні органи поліції. При цьому у складі поліції функціонують: кримінальна поліція; патрульна поліція; органи досудового розслідування; поліція охорони; спеціальна поліція; поліція особливого призначення та інші підрозділи, діяльність яких спрямована на виконання завдань поліції або на забезпечення її функціонування, рішення про створення яких приймається керівником поліції за погодженням з Міністром внутрішніх справ [1]. Також відповідно до ст. 1 вищезгаданого закону Національна поліція України (поліція) є центральним органом виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку. Натомість діяльність поліції, що залишається самостійним центральним органом виконавчої влади, спрямовується та координується урядом через Міністра внутрішніх справ України [1].

Проте у чинному поліцейському законі не конкретизовано, яку саме систему (модель) організації взято в Україні за основу. Приміром, в Україні діють міжрегіональні органи, які визначаються як «територіальні органи». У складі поліції наявна патрульна