Підопригора К.Б. – слухачка магістратури юридичного факультету;
Косиченко О.О. – науковий керівник, доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент (Дніпропетровський державний університет внутрішніх справ).

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОСОБИСТОСТІ, ТОВАРИСТВА І ДЕРЖАВИ

Сучасний розвиток суспільства породжує безліч загроз природного, техногенного, екологічного, конфліктного характеру, а також в частині поширення внутрішнього і міжнародного тероризму, погіршення транспортної безпеки, управлінських ризиків. Особливе місце з цього переліку відводиться загрозам інформаційної безпеки, до яких відносяться:

- порушення інформаційного забезпечення діяльності органів державної влади, муніципальних підприємств і служб;
- перехоплення трансляцій телерадіомовлення, систем оповіщення та інформування населення;
- несанкціонований доступ до інформації про діяльність органів державної влади, муніципальних підприємств і служб;
- несанкціонований доступ до управління інформаційними ресурсами;
- надання цілеспрямованого негативного інформаційного впливу на населення через засоби масової інформації і інформаційно-телекомунікаційну мережу Інтернет;
- неповна реалізація прав громадян в області отримання і обміну достовірної інформації, в тому числі маніпулювання масовою свідомістю з використанням інформаційно-психологічного впливу;
- провокування соціальної, міжнаціональної і релігійної напруженості через діяльність окремих (в тому числі електронних) засобів масової інформації;
- поширення зловживань в кредитно-фінансовій сфері, пов'язаних з проникненням в комп'ютерні системи і мережі.

В умовах таких загроз і ризиків громадяни потребують підвищення загального рівня суспільної безпеки, правопорядку і безпеки середовища проживання за рахунок істотного поліпшення координації діяльності сил і служб, відповідальних за рішення цих задач.

Завдання по нейтралізації загроз, мінімізації ризиків, запобігання збиткам в умовах інформаційного суспільства необхідно вирішувати шляхом

впровадження комплексної інформаційної системи, що забезпечує прогнозування, моніторинг, попередження і ліквідацію можливих загроз. Інформаційні технології необхідні для контролю і усунення наслідків надзвичайних ситуацій і правопорушень з інтеграцією під її управлінням дій інформаційно-керуючих підсистем чергових, диспетчерських, муніципальних служб для їх оперативної взаємодії в інтересах муніципальної освіти. [2]

Однією з основних невідкладних причин впровадження інформаційних технологій в управлінську та правоохоронну діяльність є інформаційно-технічний характер сучасної злочинності. Правозастосовна практика свідчить про те, що з кожним роком зростає число злочинів як в сфері комп'ютерної інформації, так і злочинів з використанням комп'ютерних технологій, в результаті чого формуються цифрові сліди злочинів. Із цього випливає, що розкривати і розслідувати злочини з використанням інформаційних технологій можливо тільки з використанням правоохоронними органами інформаційних технологій. Необхідність розвитку і впровадження інформаційних технологій пов'язана зі швидкістю прийняття рішень. В умовах динамічної економіки, всіх видів людської діяльності, заснованої на інформаційних технологіях, в критичних ситуаціях необхідно приймати грамотні управлінські рішення в найкоротші терміни. Названі і неназвані причини впровадження інформаційних технологій ставлять перед правоохоронними органами та органами державної, муніципальної влади завдання формування комунікаційної платформи з метою запобігання і усунення ризиків громадської безпеки, правопорядку і створення безпечного середовища проживання на базі міжвідомчої взаємодії. Для цього необхідно визначити потенційні точки уразливості, своєчасно реагувати на виникаючі загрози в надзвичайних ситуаціях. [1].

У сфері правоохоронної діяльності планується більш інтенсивно розвивати інформаційно-керуючі системи, системи обробки та ідентифікації дактилоскопічної, генної, балістичної та іншої криміналістично значимої інформації, програмне і інформаційне забезпечення перспективних та сучасних автоматизованих систем управління, інформаційно-довідкову роботу в інтересах підрозділів МВС.

Серед діючих ефективних інформаційних технологій, що забезпечують безпеку, слід назвати відеоспостереження і відео фіксацію, в тому числі зняття, обробку і передачу відео потоку з камер відеоспостереження про правопорушення і ситуаціях надзвичайного характеру, в тому числі пошкодження комунікацій, інфраструктури і майна. У цьому випадку проводиться аналіз відео- та аудіо потоків, включаючи: автоматичну реєстрацію подій на базі системи відео аналізу потоку; відео аналіз подій; аналітику відео-потоку в режимі реального часу; ідентифікацію і розпізнавання осіб.

Унікальні можливості використання інформаційних технологій в правозастосовній діяльності містяться в позиціонуванні рухомих об'єктів (геолокація). Геоінформаційні системи МВС - це складні інформаційні системи, створювані завдяки інтеграції баз даних звичайних інформаційних систем, функціонуючих в підрозділах МВС на певному рівні з базами даних відпові-

дної картографічної інформації, з метою представлення інформації певних об'єктів наочно в просторовому їх розташуванні на картах або планах. [3]

З метою розвитку геолокації і технологічної інфраструктури системи в інтересах державних та інших інформаційних систем, які здійснюють збір і обробку навігаційної інформації, що надходить від транспортних засобів, оснащених апаратурою супутникової навігації державою вживаються заходи щодо реалізації цих технологій. Для цього повинна бути створена комунікаційна платформа або єдиний інформаційний простір з урахуванням розмежування прав доступу до інформації різного характеру дозволить забезпечити інформаційний обмін між учасниками всіх державних і муніципальних органів виконавчої влади в області забезпечення безпеки.

В сучасних умовах інформаційні технології відіграють ключову роль в інформаційному забезпеченні розслідування злочинів. З інформаційних позицій інформаційне забезпечення - це сукупність єдиної системи збору та отримання інформації з зовнішніх і внутрішніх джерел, схем інформаційних потоків, що циркулюють в ході розкриття і розслідування злочинів, а також методологія використання наявних баз даних і побудови нових баз даних.

Нові інформаційні технології розширили не тільки слідчу картину злочинів, а й перелік предметів і документів речових доказів, що підлягають криміналістичної реєстрації. Реєстрація та довготривале зберігання інтернет-трафіку, всіх телефонних з'єднань, наявність взаємозв'язку абонента і базової станції, а також технічні можливості сучасних комп'ютерних засобів і систем управління базами даних дозволяють досить оперативно обробити колосальні обсяги комунікаційної інформації та отримати відомості, які полегшують розслідування злочинів. [1]

Крім цього, існують проблеми відомчої роз'єднаності, недостатності фінансування для закупівлі та впровадження інформаційних технологій. Названі проблеми необхідно враховувати всім зацікавленим суб'єктам інформаційних технологій і в зв'язку з цим формувати нові інформаційні правовідносини.

Узагальнюючи вищевикладене, можна сказати, що в сучасному інформаційному суспільстві, в умовах зростання загальних і інформаційних загроз, зростання комп'ютерної злочинності, повсюдного поширення штучного інтелекту, застосування інформаційних технологій у всіх сферах правоохоронної, економічної, регулятивної діяльності є необхідним, неминучим і найперспективнішим напрямом діяльності для забезпечення безпеки особистості, суспільства і держави. Для цього потрібне створення єдиного інформаційного середовища, що забезпечує ефективну і негайну взаємодію всіх сил і служб, відповідальних за громадську безпеку і правопорядок. Для підвищення ефективності діяльності по розкриттю і розслідування злочинів необхідно створити інтегровані банки даних криміналістично значимої інформації, досягти більш високого рівня інформатизації правоохоронних органів. Ступінь технічної оснащеності всіх органів попереднього розслідування телекомунікаційної інфраструктурою та інформаційними ресурсами повинен відповідати су-

часним викликам і технічним вимогам. При впровадженні інформаційних технологій в усі сфери державної і правоохоронної діяльності в гонитві за забезпеченням безпеки суспільства і держави не можна допустити перегинів, нехтування конституційними гарантіями прав особистості в сфері приватного життя. У новій структурі інформаційних правовідносин необхідно враховувати існуючі інформаційні загрози і ризики, забезпечувати гарантії права особи на приватне життя, безпеку суспільства і держави.

Використані джерела:

1. Белова Л. Г., Стриженко А. А. Информационное общество: трансформация экономических отношений в мировой экономике. М.; Барнаул: МГУ им. М. В. Ломоносова; Азбука, 2007. 387 с.
2. Петренко С.А., Курбатов В.А. Политика информационной безопасности. – М.: Компания АйТи, 2006.

Рец В.В. - курсант 3-го курсу факультету підготовки фахівців для органів досудового розслідування;
Прокопов С.О. - науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ЯК ІНСТРУМЕНТАРІЙ У БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ

Сучасна діяльність Національної поліції, пов’язана із виконанням базових завдань центрального органу виконавчої влади, в подальшому потребує вдосконаленого інформаційного забезпечення і розгалуженої системи інформаційних систем, які виконуватимуть, перш за все, превентивну функцію.

«Інформаційне забезпечення» є ключовою категорією в управлінській діяльності Національної поліції, ключовим її інструментом є поняття «інформація», за допомогою чого, власне, реалізується вся адміністративна функція та виконуються базові завдання правоохоронного органу. Тому цілком очевидно, що дана категорія привертає увагу багатьох фахівців у сфері інформатизації правозахисної і правозабезпечувальної діяльності поліції.

Під поняттям «інформаційне забезпечення» можна розуміти на тільки процес забезпечення інформацією, але і сукупність форм документів, нормативної бази та реалізованих рішень щодо обсягів, розміщення та форм існування інформації, яка знаходиться в системі і використовується у процесі функціонування інформаційне наповненого ядра [1, с. 299]. Таким чином інформаційне забезпечення має неоднозначну природу, тому що може бути