спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. В кожному із зазначених органів діють відповідні підрозділи. Але при цьому кожна людина що використовує кіберпростір грає певну роль в забезпеченні своєї кібербезпеки кіберпростору, включаючи пристрої та мережі, які вона використовує.

УДК 351.741:343.45:342.721

ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
ЄЛИЗАВЕТА ГЕОРГІЇВНА БЄЛЯЄВА
курсант 4 курсу факультету № 4 Харківського національного університету внутрішніх справ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Одним із напрямків розвитку України є підвищення захисту персональних даних та забезпечення прав осіб на недоторканність приватного життя. Захист основоположних прав і свобод людини щодо обробки персональних даних безпосередньо впливає на авторитет держави, зокрема, її здатність реалізовувати ефективну внутрішню і зовнішню політику в галузі прав людини. Як показує практика, процес гармонізації національного законодавства у сфері захисту персональних даних є складним, тому повинен бути безперервним і слідувати постійним змінам, які відбуваються в цій області. В даний час кожен володілець та розпорядник персональних даних визначає власну політику безпеки щодо обробки даних, яка має відповідати вимогам законодавства [2].

У 2015 році був прийнятий Закон України «Про Національну поліцію», який передбачає повноваження поліції в безпрецедентному масштабі формувати і використовувати інформаційні ресурси (бази даних). Сучасні інформаційні технології та законодавство відкривають можливості для правоохоронних органів обробляти величезний обсяг персональних даних. Проте, з огляду на численні переваги цих технологій, слід визнати, що при несанкціонованому їх використанні (без дотримання вимог закону), це може призвести до серйозних наслідків [3].

Серед поширених порушень можна виділити [1]:

– Доступ до персональних даних за відсутності повноважень, законної підстави і обґрунтованої мети такого доступу.

– На практиці поширеними є випадки, коли працівники підрозділів з протидії наркозлочинності масово витребовують з медичних закладів дані

щодо осіб, які стоять на обліку як такі для формування баз даних про цих осіб. Суспільство так і не отримало відповідь, яка мета і законна підстава збирати інформацію про здоров‘я людини, яка не вичинила правопорушення.

– Залишається відкритим питання щодо обробки відеозаписів з нагрудних камер поліцейських, а також систем відеоспостереження (збір, доступ, формування баз, порядок та термін зберігання такої інформації). Зокрема, як відеозаписи з камер з‘являються в мережі Інтернет, без дотримання вимог законодавства про захист персональних даних.

– Відсутність належної політики безпеки персональних даних розпорядником таких даних, затвердженої шляхом розробки та прийняття відповідної внутрівідомчої нормативно-правової бази.

– Відсутність прозорого управління у сфері захисту даних. Міжнародними стандартами визначено, що суспільство має право знати, яку інформацію збирають, які умови безпеки, зберігання та знищення персональних даних.

– У більшості випадків інформація, яка збирається і використовується в поліції не архівується в формати, які забезпечують певний рівень безпеки та конфіденційності, а також не ведеться належний її облік.

Однією з причин, яка призводить до порушення вимог законодавства у сфері захисту персональних даних є низки знання співробітників зобов’язань щодо забезпечення конфіденційності і заходів безпеки під час обробки даних.

Особливим випадком до порушення вимог законодавства є обробка «чутливої» категорії персональних даних (про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров’я, статевого життя, біометричних або генетичних даних).

Серед причин порушень безпеки обробки персональних даних можна виділити [1]:

– відсутність розроблених і затверджених положень щодо безпеки персональних даних, які б відповідали потребам даного відомства/структурного підрозділу, а також національним і міжнародним стандартам у сфері захисту персональних даних;

– низький кваліфікаційний рівень співробітників у сфері захисту персональних даних;

– передача персональних даних по незахищених каналах зв’язку;

– відсутність осіб, відповідальних за захист персональних даних;

– не ведеться належний облік зібраної або переглянутої інформації.

Для підвищення рівня захисту персональних даних про особу в базах даних Національної поліції необхідно: визначити порядок (постанова, інструкція, наказ) захисту та збереження інформації, оброблення та накопичення персональних даних про особу в базах персональних даних; визначити вповноважений орган з питань захисту персональних даних і притягнення до відповідальності за незаконну обробку й доступ до них без

письмової згоди фізичної чи юридичної особи; розробити кодекс України про захист персональних даних.

Список використаних джерел:

1. Костенко І. В. Проблеми правового захисту персональних даних у діяльності Національної поліції. Юридичний часопис Національної академії внутрішніх справ. 2018. № 1 (15). С. 296–302.
2. Про захист персональних даних. Закон України від 1 черв. 2010 р. № 2297-VI. URL: http://zakon1.rada.gov.ua/laws/show/2297-17.
3. Про Національну поліцію. Закон України від 2 лип. 2015 р. № 580-VIII. URL: http://zakon1.rada.gov.ua/laws/main/580-19.

УДК 004.056

КСЕНІЯ ОЛЕКСАНДРІВНА КРАТАСЮК
курсант 4 курсу факультету №4 Харківського національного університету внутрішніх справ
ВОЛОДИМИР ВОЛОДИМИРОВИЧ ТУЛУПОВ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВТОРГНЕНЬ В СУЧАСНИХ СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

На теперішній час в Україні на державному та регіональних рівнях впроваджуються різні програми, проекти та заходи публічної безпеки. Так, у більшості міст в Україні створюються проекти забезпечення публічної безпеки й порядку та протидії злочинності. Наприклад, у місті Києві в рамках проекту Kyiv Smart City «Безпечне місто» у загальноміській системі відеоспостереження працює 5823 камер та створені програмні модулі розпізнавання обличчя і номерів автомобілів. Також відкрито три ситуаційні центри та налагоджена взаємодія з оперативними частинами МВС та СБУ. У майбутньому до системи підключать пожежну, рятувальну, медичну, дорожню й інші комунальні та державні служби [2].

Серед завдань таких проектів і програм є: удосконалення науково-методичного, матеріально-технічного та інформаційного забезпечення правоохоронних та інших органів, що беруть участь у забезпеченні публічної безпеки та порядку; безперервний моніторинг криміногенної ситуації в області, в т.ч. за рахунок соціологічних технологій та забезпечення своєчасного реагування на негативні зміни; здійснення посиленого контролю за ситуацією у публічних місцях, передусім при проведення заходів за участю значної кількості громадян; запобігання правопорушенням, що вчиняються з використанням телекомунікаційних мереж та мережі Інтернет.

На теперішній час у системі Міністерства внутрішніх справ впроваджено низку аналітичних систем з можливістю проведення глибокого