різних складів кримінальних правопорушень, але не здатна захистити особу, яка потерпіла від насильства на ґрунті нетерпимості. У міжнародному праві прийнято розділяти такі поняття як дискримінація, злочини на ґрунті ненависті та мову ворожнечі, а у вітчизняному кримінальному законодавстві всі ці склади об'єднані в одній статті, що створює труднощі правильної кваліфікації цього злочинного діяння та ставить під загрозу належний захист права людини на рівність, та умови для приховування цих правопорушень, неможливості їх ефективного розслідування. Тому вважаємо доцільним продовжити подальшу розробку пропозицій щодо внесення змін до ст. 161 ККУ.

1. Загальна декларація прав людини [Електронний ресурс] // Верхвона Рада України Законодавство України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/995_015#Text

2. Конвенція про захист прав людини і основоположних свобод [Електронний ресурс] // Верховна Рада України Законодавство України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/995_004#Text

3. Конституція України [Електронний ресурс] // Верховна Рада України Законодавство України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

4. Закон України «Про засади запобігання та протидії дискримінації в Україні» [Електронний ресурс] // Верховна Рада України Законодавство України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/5207-17#Text

5. Кримінальний кодекс України [Електронний ресурс] // Верховна Рада України Законодавство України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2341-14#Text

6. «Міланович проти Сербії» (Milanovic v. Serbia) від 20.06.2011 № 44614/07; «Ангелова та Ілієв проти Болгарії» (Angelova and Iliev v. Bulgaria) від 26.07.2007 № 55523/00 [Електронний ресурс] // Европейская Конвенция о защите прав человека: право и практика – Режим доступу до ресурсу: http://www.echr.ru/documents/doc/2471244/2471244-005.htm

Юлія Самойленко,
аспірант кафедри адміністративного права,
процесу та адміністративної діяльності
Дніпропетровського державного
університету внутрішніх справ

СИСТЕМА АДМІНІСТРАТИВНО-ПРАВОВИХ ЗАСОБІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Аналіз законодавства дає можливість засвідчити, що нормативного визначення поняття та системи адміністративно-правових засобів захисту персональних даних відсутнє. Так, Закон України «Про захист персональних даних» [1] визначає тільки: в ст.5 об'єкти такого захисту - персональні дані, обходячи стороною суб'єктів їх захисту, та частково в ст. 24 визначає структу-

рно-організаційну форму забезпечення захисту персональних даних, вказуючи, що «в органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці» не вказуючи при цьому засоби та способи захисту персональних

Якщо ж вести мову про адміністративно-правові засоби забезпечення захисту персональних даних, то під ними, на нашу думку, слід розуміти систему заходів попередження (превентивних заходів), припинення порушень, що посягають на право володіння та розпорядження персональними даними та застосування заходів адміністративної відповідальності органами публічної влади, які відповідно до законодавства мають забезпечувати їх захист.

Основним суб'єктом, який уповноважений застосовувати заходи попередження порушень законодавства у сфері захисту персональних данихє Уповноважений Верховної Ради України з прав людини (далі - Уповноважений), такі повноваження щодо контролю за додержанням законодавства про захист персональних даних було надано цьому інституту державної служби Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», який набув чинності 1 січня 2014 року, прийнятим з метою забезпечення незалежності уповноваженого органу з питань захисту персональних даних, як того вимагає Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних[2].Слід зауважити, що Законом не визначено систему заходів попередження порушень законодавства у сфері захисту персональних даних, однак його аналіз дає можливість виділити дві групи попереджувальних (превентивних) заходів, зокрема ті, які застосовуються володільцями, розпорядниками персональних даних та ті, які застосовують посадові особи Уповноваженого.Так володільці та розпорядники персональних данихстворюють (визначають) структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, яківживають такі заходи попередження порушень законодавства у сфері захисту персональних даних:- зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних; інформують та консультують володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних; взаємодіють з Уповноваженим та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних. В свою чергу Уповноважений вживає такі заходи попередження порушень законодавства у сфері захисту персональних даних: отримує пропозиції та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду; проводить

на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних; отримує на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом;затверджує нормативно-правові акти у сфері захисту персональних даних;за підсумками перевірки, розгляду звернення видає обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних та ін.

Наступними за логікою та доцільністю застосування є заходи адміністративно-правовогоприпинення порушення законодавства щодо захисту персональних даних, до яких слід віднести:безпосереднє усунення володільцем або розпорядником персональних даних порушень законодавства про захист персональних даних; отримання Уповноваженим скарг фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду; здійснення Уповноваженим позапланових перевірок володільців або розпорядників персональних даних із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних; видання Уповноваженим вимоги (припису) про усунення порушень законодавства про захист персональних даних та підстав які зумовлювали таке порушення.Метою внесення припису є припинення порушення законодавства про захист персональних даних та по мірі можливості йоговиправлення, а також усунення обставин, що сприяли його виникненню, чи інших, що можуть призвести до його виникнення вмайбутньому. З цією метою припис може містити, серед іншого,вказівки щодо: 1) зміни, 2) видалення або 3) знищення персональних даних, 4) забезпечення доступу до них, 5) надання чи 6) заборони їх надання третій особі, 7) зупинення або припинення обробки персональних даних. Вказані вимоги є зрозумілими і т. досяг на'яснення не потребують. Їх метою є припинити порушення Закону (наприклад, видалити дані, що обробляються незаконно), відновити порушені права (наприклад, надати суб'єкту доступ до т. досяг нальних даних чи змінити його персональні дані, що не відповідають дійсності) або запобігти потенційним порушенням в майбутньому (наприклад, припинити обробку (зокрема, збір, зберігання та використання) персональних даних, що не є необхідними т. досягнення задекларованої легітимної мети їх обробки, запровадити додаткові заходи захисту персональних даних).

Невід'ємною складовою дієвих засобів адміністративно-правового за-

хисту персональних даних є застосування заходів адміністративної відповідальностіза такі правопорушення: неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей; невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних; повторне протягом року вчинення порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративному стягненню; недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних; повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню(т.. 188-39 КупАП) [3].

Окрім цього, одним із дієвих засобів адміністративно-правового захисту персональних даних є позасудове та судове оскарження рішення про відстрочення або відмову в доступі до персональних даних. Так, т.. 18 Закону визначено можливість оскарження рішення про відстрочення або відмову у доступі до персональних даних: позасудове – до Уповноваженого Верховної Ради України з прав людини, підстави якого визначено т.. 23 Закону; судове – до адміністративного суду, у порядку визначеному КАСУ [4]. При цьому слід врахувати те, що якщо запит зроблено суб'єктом персональних даних щодо даних про себе, обов'язок доведення в суді законності відмови у доступі покладається на володільця персональних даних, до якого подано запит.

---

1. Про захист персональних даних: Закон України від 1 черв. 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34.Ст. 481.

2. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон України від 3 липня 2013 року№ 383-VII. *Відомості Верховної Ради України.* 2014. № 14. Ст.252.

3. Кодекс України про адміністративні правопорушення від 7 груд. 1984 р. № 8073-X. *Відомості Верховної Ради УРСР*. 1984. Додаток до № 51. Ст. 1122.

4. Кодекс адміністративного судочинства України: Закон України від 06.07.2005 року. *Відомості Верховної Ради України*. 2005. №35–36, №37. Ст. 446.