Таким чином, виходячи з вищеозначеного доходимо висновку, що в межах ЄС створено низку органів, діяльність яких спрямована на забезпечення високих стандартів забезпечення інформаційної безпеки.

**Список використаних джерел**

1. Regulation (EU) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. URL: https://publications.europa.eu/en/publication-detail/-/publication/0177e751-7cb7-404b-98d8-79a564ddc629/language-en.

2. Regulation (EU) No 526/2013 of the european parliament and of the council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0526.

*Одержано 02.11.2018*

УДК 341

**Максим Сергійович ХАВРАТ,**
*аспірант кафедри міжнародного і європейського права*
*юридичного факультету*
*Харківського національного університету імені В. Н. Каразіна*

## ДЕЯКІ АСПЕКТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЄВРОПОЛОМ

Необхідність забезпечення належного рівня захисту персональних даних відіграє важливу роль у сучасному цифровому світі. Інформація все частіше обробляється з використанням автоматизованих систем, що, у свою чергу, може мати наслідком можливість стороннього незаконного втручання до таких систем з метою заволодіння персональними даними, їх зміни або пошкодження. Збір та обробка даних є невід'ємними складовими діяльності більшості міжнародних органів та організацій, не є виключенням і Європейське поліцейське відомство (далі – Європол).

Діяльність Європолу, який функціонує з метою підтримання та зміцнення дій компетентних органів держав-членів та їх співпраці у запобіганні та протидії серйозним злочинам, тероризму та іншим формам злочинності, що зачіпають загальний інтерес, безпосередньо пов'язана з опрацюванням персональної інформації. З цією метою в межах Європолу було створено інформаційну систему (далі – ІСЄ), яка представляє собою центральну базу даних для обміну розвідувальними даними та інформацією між державами-членами. ІСЄ містить інформацію про серйозні міжнародні злочини, підозрюваних і засуджених, злочинні структури та злочини і засоби, що використовуються для їх скоєння. ІСЄ може використовуватися для надання доступу до даних, що стосуються осіб, які є підозрюваними або яких було засуджено за скоєння кримінального правопорушення, що відноситься до компетенції Європолу; або осіб, факти щодо яких

вказують на те, що вони готуються скоїти такі правопорушення [1, с. 166].

Однак, функціонування такої системи вимагає застосування сучасних та ефективних заходів, спрямованих на запобігання та недопущення несанкціонованого доступу до неї. Так, задля належного опрацювання персональних даних, які перебувають у розпорядженні Європолу, Регламентом (ЕС) 2016/794 було закріплено низку положень, якими врегульовано порядок збору, зберігання та використання таких відомостей. Зокрема, Регламентом (ЕС) 2016/794 визначено загальні принципи обробки персональних даних, серед яких: справедливість і законність, дотримання цільового призначення тощо (ст. 28). З метою захисту інформації передбачено проведення оцінки надійності джерела інформації (ст. 29) [2].

Вищеозначеним Регламентом закріплено особливості опрацювання спеціальних категорій персональних даних, зокрема, таких, що стосуються жертв і свідків злочинів та осіб, які не досягли 18 років та ін. З огляду на ту обставину, що в розпорядженні Європолу перебуває значний масив інформації, в тому числі чутливої, існує об'єктивна необхідність у здійсненні технічних та організаційних заходів з метою їх захисту від випадкового або незаконного знищення, втрати, несанкціонованого розкриття, зміни або доступу. Такі заходи мають бути спрямовані на контроль доступу до обладнання, що використовується з метою опрацювання персональних даних; управління носіями даних (попередження або недопущення несанкціонованого зчитування, копіювання, зміни, видалення); попередження несанкціонованого вводу даних, їх модифікації; попередження використання автоматизованих систем обробки даних неавторизованими особами; забезпечення того, щоб, уповноважені особи мали доступ тільки до тих даних, що охоплюються їх повноваженнями на доступ (контроль доступу до даних); забезпечення несанкціонованого зчитування, копіювання, зміни або видалення персональних даних під час передачі персональних даних або при транспортуванні носіїв даних; створення умов для можливості невідкладного відновлення системи, яка використовується для зберігання інформації тощо (ст. 32) [2].

З метою захисту таких персональних даних також встановлено строки їх зберігання. За загальним правилом, інформація має зберігається до тих пір, доки це є необхідним для цілей, для яких вона обробляється. Однак у будь-якому випадку Європол розглядає питання необхідності подовження зберігання таких відомостей не пізніше, ніж через три роки після їх первинної обробки (ст. 31).

У тому випадку, якщо відбулося порушення цілісності персональних даних, Європол має повідомити Європейського інспектора із захисту даних, компетентні органи зацікавлених держав-членів, а також постачальника таких даних про це порушення без невиправданої затримки. Європейський інспектор несе відповідальність за моніторинг і забезпечення застосування положень Регламенту, що стосуються захисту основних прав і свобод фізичних

осіб щодо обробки персональних даних у межах Європолу. Задля досягнення означеної мети, Інспектор здійснює такі функції: заслуховує і розслідує скарги та інформує суб'єкта даних про результати розгляду; веде розслідування (за власною ініціативою або на підставі скарги) й інформує суб'єкта даних про підсумки; консультує Європол в усіх питаннях, що стосуються опрацювання персональних даних; веде реєстр нових видів операцій з обробки; проводить попередню консультації щодо опрацювання тощо. Крім цього, Європейський інспектор може доручити Європолу здійснити виправлення, обмеження, стирання або знищення персональних даних, які були оброблені з порушенням і повідомити про такі дії третіх осіб, яким були розкриті дані; накласти тимчасову або остаточну заборону на обробку Європолом операцій, які порушують положення, що регулюють обробку персональних даних тощо. За підсумками своєї роботи Інспектор, у консультації з національними наглядовими органами, готує щорічний звіт, який повинен містити статистичну інформацію про скарги, розслідування, передачу персональних даних третім державам і міжнародним організаціям, випадки попередніх консультацій тощо (ст. 43).

У межах Європолу також запроваджено посаду Співробітника з питань захисту даних. Така особа є членом персоналу та наділений такими повноваженнями: забезпечення збереження запису про передачу й отримання персональних даних; забезпечення інформування суб'єктів даних про їхні права; проведення консультацій щодо обробки даних; співробітництво з Європейським інспектором із захисту даних; ведення реєстру порушень обробки персональних даних тощо. Крім цього кожна держава-член призначає національний наглядовий орган, який має контролювати, відповідно до свого національного законодавства, допустимість передачі персональних даних до Європолу (ст. 42).

Таким чином, виходячи з означеного, доходимо висновку, що забезпечення незалежної та ефективної діяльності Європолу вимагає застосування необхідних заходів інформаційної безпеки. Так, Регламентом (ЕС) 2016/794 закріплено низку положень щодо загальних принципів опрацювання інформації Європолом. Крім того, суттєвий внесок у забезпечення захисту персональних даних роблять Європейський інспектор із захисту даних, Співробітник з питань захисту даних та відповідні національні наглядові органи держав.

**Список бібліографічних посилань**

1. Посібник з європейського права у сфері захисту персональних даних. К. : К.І.С., 2015. 216 с. URL: https://rm.coe.int/168044e84e (дата звернення: 31.10.2018).

2. Regulation (EU) 2016/794 of the European Parliament and of the CounciL of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

*Одержано 01.11.2018*