Загуменна Ю.О.
Харківський національний університет внутрішніх справ

Інституційні засади забезпечення європейської інформаційної безпеки

Становлення та розвиток інформаційної безпеки на європейському регіональному рівні, складовою якої є потужні правова та інституційна основа, відбувається упродовж багатьох років. На сьогодні, запроваджено посаду та створено низку спеціалізованих структур, наділених компетенцією у цій сфері. Так, Європейський інспектор із захисту даних гарантує дотримання установами й органами ЄС права на приватне життя при обробці особистої інформації громадян в електронному, письмовому або візуальному форматі - під час виконання своїх обов'язків (обробка включає в себе зібрання, запис, збереження, вилучення, передачу, блокування або видалення даних). Завдання Європейського інспектора полягає в дотриманні суворих правил конфіденційності, що регулюють цю діяльність і гарантування дотримання установами й органами ЄС права на приватне життя та його повагу. Слід зазначити, що правила захисту фізичних осіб під час обробки їхніх персональних даних установами, органами, службами та агенціями Союзу і державами-членами під час провадження діяльності в межах, охоплених законодавством Союзу, а також правила щодо вільного руху таких даних, встановлюються Європейським Парламентом і Радою, відповідно до звичайної законодавчої процедури (ст. 16 ДЄС).

Європейський інспектор консультує органи та інститути ЄС з усіх аспектів обробки персональних даних і пов'язаних з ними політики і законодавства; розглядає скарги і проводить розслідування; співпрацює з національними органами влади держав-членів ЄС з метою забезпечення послідовності у захисті даних; проводить моніторинг нових технологій, що сприятимуть захисту даних (посада передбачена Регламентом 45/2001) .

Установи та органи ЄС не повинні обробляти персональні дані, які стосуються расового або етнічного походження, політичних поглядів, релігійних або філософських поглядів, профспілкового членства; дані про стан здоров'я або сексуальної орієнтації, якщо вони не потрібні з метою охорони здоров'я. У такому випадку це повинно бути зроблено медичним працівником або іншою особою, яка присягалася зберігати професійну таємницю. У випадку порушення права на недоторканність приватного життя установою або органом ЄС особа має право звернутися зі скаргою до Європейського інспектора або до органу, який, на думку особи, скоїв порушення. Європейський інспектор повинен прийняти заходи щодо проведення розслідування (з'ясування обставин, розгляду обставин справи), результати розслідування повинні бути повідомлені особі, якщо результат розгляду скарги Інспектором не задовольняє особу, то вона має право звернутися до Суду ЄС.

Європейське агентство з питань мережевої та інформаційної безпеки (далі - ENISA) - є експертним центром кібербезпеки в Європі. Допомагає державам-членам ЄС і ЄС в оснащенні (устаткуванні) і підготовці з метою попередження,

виявлення і реагування на проблеми інформаційної безпеки. Вона надає практичні рекомендації державному і приватному сектору в державах-членах ЄС, а також інститутам ЄС шляхом: розробки стратегій кібербезпеки, сприяння співробітництву між групами реагування на комп'ютерні злочини; нарощування потенціалу; публікації доповідей і проведення досліджень з питань кібербезпеки (Регламент ЕС №460/2004 і 526/2013).

Задля виконання покладених на нього завдань Агентство прагне прогнозувати і підтримувати Європу у вирішенні проблем, що виникають у сфері безпеки мереж та інформації з урахуванням еволюції цифрового середовища (експертиза); акцентує увагу на наданні допомоги державам-членам та інституціям і Союзу в розробці і здійсненні політики та дотриманні законодавчих і нормативних вимог; прагне підтримувати Європу в укріпленні в найбільш сучасних інформаційних можливостей безпеки; акцентує увагу на розширенні співпраці між державами-членами та між пов'язаними співтовариствами.

Основна цільова група обслуговування Агентства - це організації державного сектору, зокрема уряди держав-членів ЄС, інститути ЄС. Агентство також надає послуги (допомогу) у сфері ІКТ (телекомунікації, інтернет-провайдери та ІТ компанії), бізнес-співтовариствам, особливо малому бізнесу, спеціалістам мережевої та інформаційної безпеки, таким як команди комп'ютерного реагування на надзвичайні ситуації тощо.

Комп'ютерна група реагування на надзвичайні ситуації (далі - CERT) розпочала своє функціонування з у 2012 р. До сфери компетенції віднесено надання допомоги в попереджені і ліквідації загроз комп'ютерній системі інститутів ЄС - щодо керування загроз - підтримка груп ІТ безпеки в кожній установі ЄС та взаємодія з колегами з комп'ютерних груп реагування на надзвичайні ситуації в державах-членах ЄС.

Питанню захисту персональних даних також приділено значну увагу в діяльності Європолу - правоохоронного органу, метою якого є надання допомоги у запобіганні та розслідуванні організованої злочинності, тероризму та інших тяжких злочинів. Європолом створено Інформаційну систему (Europol Information System), яка функціонує в якості бази даних для обміну розвідувальними даними та інформацією державами-членами через свої Національні підрозділи Європолу (далі - НЦБ). Інформаційна система Європолу містить інформацію про злочини, злочинні структури, підозрюваних і засуджених, а також засоби, які використовуються для скоєння відповідних злочинів. Система використовується посадовими особами Європолу, офіцерами зв'язку держав-членів, співробітниками національних підрозділів Європолу та компетентними органами держав-членів.

У 2013 році відбулося офіційне відкриття Європейського центру по боротьбі з кіберзлочинністю (далі - ЄСЗ). Новий підрозділ Європолу покликаний відігравати провідну роль у боротьбі з кіберзлочинністю на території Європейського Союзу. ЕСЗ займається створенням оперативних і аналітичних потужностей, необхідних для забезпечення швидкого реагування на кіберзлочини, а також організацією взаємодії офіційних відомств ЄС і країн-

членів з міжнародними партнерами. Мандат Центру визначає такі сфери відповідальності: боротьба зі злочинами, які вчиняються організованими злочинними групами та тягнуть за собою отримання незаконних доходів в особливо великих розмірах (шахрайство з кредитними картками або банківськими операціями); боротьба зі злочинами, що завдають серйозної шкоди жертві, зокрема з розбещенням малолітніх; боротьба з діями, спрямованими на спричинення шкоди або виведення з ладу інфраструктури та інформаційних систем ЄС. Центр відповідальний за збір та обробку даних, надання інформаційної, технічної та криміналістичної підтримки відповідним підрозділам правоохоронних органів країн-членів ЄС, координацію спільних розслідувань, навчання і підготовку фахівців (у співпраці з CEPOL). Центр сприяє проведенню необхідних досліджень і створенню програмного забезпечення, опікується оцінкою і аналізом існуючих і потенційних загроз, складанням прогнозів і випуском завчасних попереджень. До сфери діяльності Центру також входить допомога суддям і прокурорам [8].

Європейське бюро судової співпраці (далі - Євроюст) - агентство ЄС, створене в 2002 р. (рішення Ради 2002/187/ЈНА зі змінами, внесеними рішеннями Ради 2003/659/Ш і 2009/426/ ЈНА) з метою покращення боротьби із серйозними злочинами. Завданням Євроюсту є підтримання зміцнення координації та співробітництва між національними органами слідства та обвинувачення у сфері тяжких злочинів, що зачіпають інтереси двох або більше держав-членів або потребують спільного обвинувачення, що ґрунтується на проведених операціях та інформації, наданій органами держав-членів та Європолом (ст.88 ч.І ДФЄС). Євроюст наділений повноваженнями, в межах своєї компетенції і для виконання своїх завдань, обробляти персональні дані за допомогою автоматизованих засобів або в структурованих ручних файлах. Під час здійснення такого опрацювання Євроюст повинен вживати необхідні заходи задля гарантування рівня захисту персональних даних, який буде, щонайменше, еквівалентним тому, що випливає із застосування принципів Конвенції № 108.

Таким чином, можна підвести підсумок, що в межах Ради Європи і Європейського союзу створена потужна правова та інституційна основа для забезпечення інформаційної безпеки об’єктом регулювання якої є захист персональних даних фізичних осіб, а також інформації, що обробляється відповідними органами, інституціями означених міжнародних структур, пов’язаної із забезпеченням безпеки. Нові виклики, що постають перед міжнародним співтовариством, зокрема, тероризм, кіберзлочинність, корупція тощо, спонукають до постійного удосконалення норм, методів і засобів захисту відповідної інформації та своєчасного і належного реагування на ці виклики.