Лілія Олексюк

*кандидат наук з державного управління, юрист, член Української сторони
Платформи громадянського суспільства та голова громадської організації,
«Всеукраїнська асоціація «Інформаційна безпека та інформаційні технології»
старший викладач ІВК КНТЕУ м. Київ, Україна,
e-mail: lylyaol7@gmail.com
<https://orcid.org/0000-0002-9006-2592>*

Андрій Ніколаєв

*експерт із захисту персональних даних та приватності,
засновник юридичної компанії Privacy Advisers*

ПРИНЦИПИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА РИЗИКИ ЇХ ПОРУШЕННЯ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЙ ЗВ'ЯЗКУ 5G

Анотація. Визначено, що політика та законодавство ЄС, в поєднанні з практичним досвідом його держав-членів щодо розгортання мереж 5G, можуть бути використані українською владою та іншими зацікавленими сторонами як цінне джерело передового досвіду, законодавчих підходів та ключових проблем, включно з кібербезпекою.

Доведено, що ефективне здійснення захисту персональних даних має пряму залежність від чіткого дотримання принципів, які становлять фундаментальну структуру захисту персональних даних.

Відмічено, що п'яте покоління мобільного зв'язку несе більше інновацій ніж усі попередні. І це стосується не лише технічних характеристик але й самої побудови системи зв'язку.

Обґрунтовано, що технічні та технологічні особливості бездротових технологій 5G, з точки зору принципів захисту персональних даних, спричиняють низку ризиків, зокрема пов'язаних із збільшенням кількості та якості даних, що обробляються, розвитком сервісів автоматизованого прийняття рішень, зокрема на базі технологій штучного інтелекту, розмиванням відповідальності між зростаючою кількістю осіб, що обробляють персональні дані. У цьому контексті викликає занепокоєння можливість втрати людиною контролю над своїми персональними даними.

Ключові слова: персональні дані, бездротові технології 5G, обробка персональних даних, принципи захисту персональних даних, інновації, ризики.

Lilia Oleksiuk

*Candidate of Science in Public Administration, Lawyer,
Member of the Ukrainian side of the Civil Society Platform and Chairman
of the All-Ukrainian Association "Information Security and Information
Technologies" Senior Lecturer, KNTEU, Kyiv, Ukraine
e-mail: lylyaol7@gmail.com
<https://orcid.org/0000-0002-9006-2592>*

Andrey Nikolaev

*Expert on personal data protection and privacy,
founder of the law firm Privacy Advisers*

PRINCIPLES OF PERSONAL DATA PROTECTION AND THEIR RISKS WHEN USING 5G COMMUNICATION TECHNOLOGIES

Abstract. It is identified that EU policy and legislation, combined with the practical experience of its Member States in deploying 5G networks, can be used by the Ukrainian authorities and other stakeholders as a valuable source of best practices, legislative approaches and key issues, including cybersecurity.

It is proved that the effective implementation of personal data protection is directly dependent on strict adherence to the principles that constitute the fundamental structure of personal data protection.

It is noted that the fifth generation of mobile communications brings more innovation than all previous ones. And this applies not only to the technical characteristics, but also to the design of the communication system itself.

It is substantiated that technical and technological features of 5G wireless technology, in terms of principles of personal data protection, cause a number of risks, including related to increasing the quantity and quality of processed data, development of automated decision-making services (including built on basis of artificial intelligence technologies), the blurring of responsibilities between the growing number of data controllers and processors. In this context, the possibility of a person losing control of their personal data is a matter of concern.

Keywords: personal data, 5G wireless technologies, personal data processing, risks, principles of data protection.

Постановка проблеми. Стрімкий розвиток технологій та здійснення інтенсивної передачі даних під час обігу інформації призвели до виникнення нових видів бездротових мережевих технологій, які не були можливими раніше. Саме тому акцент на захист персональних даних користувачів, дотримання стандартів та правових актів, а також приведення національного

законодавства у відповідність з міжнародними орієнтирами є важливим завданням сьогодення.

За даними досліджень Worldwide broadband speed league 2021, проведеного агентством cable.co.uk Україна займає 77 місце серед 224 країн світу в рейтингу швидкості інтернету. Його середня швидкість становить 25,26 Мбіт/с. Зазначається, що швидкість інтернету в Польщі — 63,84 Мбіт/с, в Румунії — 67,4 Мбіт/с, у Словаччині — 54,92 Мбіт/с, в Угорщині — 104,07 Мбіт/с. Самоврядна британська провінція Джерсі пропонує найшвидший широкорядний зв'язок в Європі (і світі) — середня швидкість якого 274,27 мбіт/с. Дослідники роз'яснюють цей факт розгортанням мереж п'ятого покоління.

Мережі дуже високої пропускну здатності, такі як 5G є ключовим активом для конкуренції на світовому ринку. 5G може сприяти розвитку промислової трансформації, застосуванню технологій Інтернету речей і дозволяє створювати інноваційні бізнес моделі в багатьох секторах. Однак, цифрова трансформація суспільства несе нові загрози інформаційної безпеки. Все це визначає актуальність даної теми та потребу у розкритті принципів захисту персональних даних та їх ризиків.

Аналіз останніх досліджень і публікацій. Актуальними питаннями захисту персональних даних у своїх роботах опікуються В.М. Брижко, С.Л. Гнатюк, М.А. Ожеван, В.Г. Пилипчук та інші. Загальні питання нормативно-правового забезпечення під час обробки персональних даних висвітлені в Законі України «Про захист персональних даних» [1]. Найдосконалішим правовим актом з питань захисту фізичних осіб у зв'язку з опрацюванням персональних даних в світі, на сьогоднішній день, вважається Регламент Європейського парламенту та Ради (ЄС) 2016/679 від 27.04.2016 року [3].

Мета статті. Аналіз ризиків для захисту персональних даних при впровадженні п'ятого покоління мобільного зв'язку, відомого як 5G, а також технології та сервісів, які на ньому побудовані. Ризики розглядаються в контексті дотримання принципів захисту персональних даних під час використання цієї технології.

Виклад основного матеріалу. Перш за все варто розкрити зміст поняття «персональних даних». Відповідно до визначення, яке міститься в Законі України «Про захист персональних даних» [1], а також у Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [2] (далі – Конвенція 108), персональні дані – це відомості або сукупність відомостей про фізичну особу, яка ідентифікована, або може бути ідентифікована. Тобто, перш за все, персональні дані – це інформація/відомості про фізичних осіб. В контексті використання технології зв'язку 5G це можуть бути відомості про: абонентів телекомунікаційних мереж; користувачів сервісів, які підключені до

телекомунікаційної мережі або побудовані з використанням технології 5G; інших осіб, які не є ні користувачами комунікаційної мережі, ні користувачами сервісів, але відомості про яких передаються телекомунікаційною мережею сервісами тощо; відомості про фізичних осіб, яких уже ідентифіковано; відомості про фізичних осіб, які можуть бути ідентифіковані.

Також розкриємо зміст поняття «обробка персональних даних». Його визначення можна знайти у статті 2 Закону України «Про захист персональних даних», де вказується, що обробка персональних даних – це будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

Більш ґрунтовне та структуроване визначення терміну обробка персональних даних можна знайти у Регламенті Європейського парламенту та Ради (ЄС) 2016/679 від 27 квітня 2016 року [3] про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС4 (далі – Загальний регламент ЄС про захист даних або GDPR), який, на сьогодні, вважається «золотим стандартом» захисту персональних даних. Відповідно до статті 4 GDPR, обробка – це будь-яка дія (операція) або сукупність дій (операцій), що здійснюються з персональними даними з використанням засобів автоматизації або без використання таких засобів, включаючи збір, запис, організацію, структурування, накопичення, зберігання, адаптацію або зміну, завантаження, перегляд, використання, розкриття через передачу, розповсюдження або інший вид надання доступу, зіставлення або комбінування, скорочення, видалення або знищення.

Для того, щоб мати можливість оцінити вплив будь-якої технології на захист персональних даних – доцільно ознайомитися з принципами захисту персональних даних [5].

В Україні ці принципи частково відображені у статті 6 Закону України «Про захист персональних даних». У Європейському Союзі ці принципи встановлені статтею 5 GDPR [3]. Загально прийнято виділяти 7 таких принципів, які становлять фундаментальну структуру захисту персональних даних.

Принцип перший: «lawfulness, fairness and transparency». Персональні дані повинні оброблятися у законний, правомірний і прозорий спосіб відносно до суб'єкта даних («законність, правомірність і прозорість»). Будь-яка обробка персональних даних має бути законною та справедливою. До фізичної особи має бути прозоро донесено те, що її персональні дані збираються, використовуються, переглядаються або іншим чином обробляються, а також те, в якому обсязі персональні дані обробляються або та будуть оброблятися. Також передбачається необхідність інформування суб'єктів персональних

даних про особу контролера, про цілі (мету) обробки персональних даних, та додаткове інформування для забезпечення справедливої та прозорої обробки в частині, що стосується відповідних фізичних осіб та права на отримання підтвердження, та відомостей про ті персональні дані, які обробляються на їх основі.

Принцип другий: «purpose limitation». Персональні дані можуть збиратися лише для конкретних, чітких і законних цілей, і не повинні оброблятися в подальшому у спосіб, що є несумісним із визначеними цілями («конкретність цілей»). Мета обробки обов'язково має бути чітко визначеною до початку обробки також необхідно переконатися, що дії, які планується здійснювати з персональними даними є цілком законними. Також мета має бути задокументована, тобто прописана у відповідних документах, які регламентують обробку (порядок обробки, політика конфіденційності тощо). Можна обробляти персональні дані з іншою метою тільки якщо вона сумісна з початковою метою, або отримано згоду суб'єкта на обробку з новою метою, або обробка необхідна для виконання зобов'язання встановленого законом, або обробка здійснюється для реалізації повноважень встановлених законом.

Принцип третій: «data minimisation». Персональні дані повинні бути адекватними, відповідними та ненадмірними, та обмежуватися тим, що є необхідним для цілей, з якими вони обробляються («мінімізація персональних даних»). Можна виділити такі показники: дані є адекватними, якщо вони є достатніми для досягнення мети обробки; дані є відповідними, якщо вони мають раціональний зв'язок із метою обробки та сприяють її досягненню; дані є ненадмірними, якщо їх обсяг не більший, ніж це необхідно для досягнення мети обробки; не можна збирати дані «про всяк випадок».

Принцип четвертий: «accuracy». Персональні дані мають бути точними, достовірними та оновлюватися, якщо це необхідно для мети їх обробки («точність»). Необхідно вживати всіх раціональних заходів для того, щоб забезпечити точність персональних даних, які обробляються, а також усіх відповідних заходів для того, щоб неточні персональні дані було негайно видалено або виправлено.

Принцип п'ятий: «storage limitation» Персональні дані не повинні зберігатися довше ніж вони потрібні для цілей, для яких ці дані обробляються («обмеження строків зберігання»). Після того, як мета була досягнута, персональні дані повинні бути знищені, або знеособлені. Знеособлені персональні дані – це дані, зі складу яких вилучили усі відомості, та які вже не дають змогу будь-яким чином ідентифікувати конкретну особу – суб'єкта персональних даних. Персональні дані можуть зберігатися протягом більш тривалого часу винятково для досягнення цілей суспільних інтересів, наукового чи історичного дослідження або статистичних цілей за умов вжиття відповідних технічних і організаційних заходів, передбачених законодавством,

для гарантування прав і свобод суб'єкта даних. Щоб гарантувати, що персональні дані не зберігатимуться довше, ніж це необхідно, контролер повинен встановити терміни, після яких вони видаляються або переглядаються.

Принцип шостий: «integrity and confidentiality» Персональні дані повинні оброблятися таким чином, щоб забезпечити їх цілісність та конфіденційність. Персональні дані повинні оброблятися таким чином, щоб забезпечити належний рівень безпеки та конфіденційності цих персональних даних, у тому числі для запобігання несанкціонованому доступу або несанкціонованого використання персональних даних та обладнання, що використовується для обробки. Володільці та розпорядники зобов'язані вживати технічні та організаційні заходи безпеки, на рівні, що відповідає законодавчим вимогам.

Принцип сьомий: «accountability». Володілець (контролер) несе відповідальність за дотримання принципів обробки персональних даних та має бути здатним це довести («підзвітність»). Обов'язок доведення дотримання цих принципів покладається на володільця.

Технологію мобільного зв'язку прийнято поділяти на покоління. Кожне покоління відкривало нові можливості та новий функціонал.

П'яте покоління мобільного зв'язку несе більше інновацій ніж усі попередні. І це стосується як технічних характеристик так і самої побудови системи зв'язку. Найбільш очевидними відмінностями 5G, на сьогоднішній день, є наступні.

1. Неоднорідність швидкості передачі інформації, порівняно з попередніми поколіннями. Виділяють три частоти 5G.

Низькочастотний 5G, який використовує частоти 600-850 МГц (наближений до 4G). Швидкість передачі даних на низькочастотному рівні становить близько 50-250 Мбіт/с.

Середньочастотний 5G, використовує частоти в діапазоні 2.5-3.7 ГГц і забезпечує можливість передачі даних на швидкості 100-900 Мбіт/с.

Високочастотний 5G, який найбільш відповідає очікуванням від п'ятого покоління, використовує частоти в діапазоні 25-39 ГГц та забезпечує можливість передачі інформації на гігабітних швидкостях.

2. Найменша затримка передачі інформації. Затримка – це проміжок часу, необхідний для переміщення пакету інформації між двома точками (пристроями). Затримка присутня під час будь-якої передачі даних. Затримка в мережах 4G становить близько 50 мілісекунд (мс), а в мережах 5G очікується скорочення цього показника до 1 мс.

3. Найбільша пропускна здатність. Пропускна здатність характеризує кількість інформації, яка може бути передана за допомогою бездротової технології в мережі. Спектр частот, що використовуються для 5G, розділений на три різні діапазони. Кожен діапазон має власну смугу частот і швидкість,

тому різнитимуться й варіанти їх використання додатками, споживачами, підприємствами і галузями промисловості.

4. Зменшений радіус покриття базових станцій. Чим вища частота сигналу – тим менший радіус охоплення базової станції. Радіус охоплення базових станцій високочастотного 5G, який працює в частотному діапазоні 25-39 ГГц, не перевищує декількох сотень метрів.

Одна із найбільших інновацій 5G полягає у тому, що для розгортання мережі п'ятого покоління не потрібно спеціалізоване телекомунікаційне обладнання – зв'язок буде забезпечуватися звичайним обладнанням, яке використовується для розгортання мережі Інтернет.

Ці зміни мають значний вплив на розвиток та побудову мережі. Тому варто ширше розглянути наступні інновації, які стосуються побудови самої мережі.

Віртуалізація мережевих функцій (Network Functions Virtualization / NFV) передбачає новий спосіб створення, розгортання та управління мережевими службами на уже наявному обладнанні завдяки програмному забезпеченню. Це дозволяє значно швидше додавати нові мережеві функції та реалізувати потреби користувачів.

Програмно-визначена мережа (Software-Defined Networks / SDN) здійснює керування мережею програмно, в тому числі з можливостями використання хмарних технологій та штучного інтелекту. На сьогодні мережа управляється апаратно, за допомогою спеціального телекомунікаційного обладнання. У разі необхідності впровадження додаткових функцій та сервісів, зміни важливих параметрів системи необхідно провести заміну обладнання, що вимагає значних витрат ресурсів та грошей. Водночас, програмно-визначена мережа дозволяє впровадити такі зміни на рівні програмного забезпечення.

Network Slicing (NS) дозволяє мобільним операторам розгортати логічно ізольовані мережі, кожна з яких буде виділена під певні потреби. Ними можуть керувати різні суб'єкти, тобто віртуальні оператори зв'язку, а також передаватися в оренду чи іншим чином в управління стороннім особам, які не мають прямого відношення до оператора зв'язку.

D2D (Device-to-device) дозволяє пристроям, що знаходяться недалеко один від одного, безпосередньо обмінюватися даними. Процес обміну здійснюватиметься без участі мережі оператора зв'язку.

Аналіз технічних та технологічних особливостей технології 5G, з точки зору принципів захисту персональних даних, дозволяє виділити ряд ризиків, які з великою ймовірністю будуть виникати в процесі широкомасштабного впровадження новітнього покоління мобільного зв'язку та низки сервісів, що базуються на ньому.

Значно зростає точність визначення місцезнаходження користувача (абонента). 5G передбачає використання більш високих частот, які мають значно меншу довжину хвилі. Менша довжина хвилі призводить до меншого

радіусу розповсюдження радіосигналу, що у свою чергу призводить до необхідності використовувати набагато більшої кількості базових станцій з меншою відстанню між ними та розміщення їх усередині приміщень або на дахах будівель, що в свою чергу призведе до ще більш точного визначення місцезнаходження абонентського пристрою (телефона чи іншого обладнання).

Підвищена точність геолокації, збільшення кількості та категорій даних, що збираються та передаються у мережі, поєднані із зростаючою кількістю пристроїв, які кожен користувач підключатиме через 5G (зокрема використовуючи технологію IoT – Інтернету речей), дозволить здійснювати більш точне розподілення користувачів на групи за певними ознаками, тобто, точне профілювання. Це призведе до зростання кількості та розвитку сервісів автоматизованого прийняття рішень, зокрема на базі технологій штучного інтелекту.

У цьому контексті викликає занепокоєння можливість забезпечення права на захист від автоматизованого рішення, яке полягає у тому, що кожен, стосовно кого було прийнято автоматизоване рішення, яке має юридичні наслідки, має безумовне право вимагати його перегляду. І такий перегляд повинен здійснюватися за участю людини (не програми).

Розвиток нових сервісів поєднаний з можливістю поділу мережі на необмежену кількість логічно-ізолюваних мереж (Network Slicing) під різні потреби та задачі, призведе до зростання кількості осіб, які надають послуги і контролюють кожну з таких мереж, та фактично набувають статусу контролерів, спільних контролерів, та операторів (володільців, співволодільців і розпорядників) персональних даних.

Це може призвести до невизначеності хто саме несе відповідальність за обробку персональних даних та/або за той чи інший інцидент із даними. Також, може бути складно визначити до кого користувач (суб'єкт персональних даних) повинен звертатися за захистом чи реалізацією своїх прав. Тобто, виникає ризик зниження рівня відповідальності як з боку контролерів, так і з боку операторів.

Збільшення кількості послуг та осіб, які обробляють персональні дані може призвести до значного ускладнення реалізації принципу прозорості обробки персональних даних. Навіть якщо кожен з осіб, які обробляють персональні дані (контролерів та операторів), буде сумлінно надавати всю інформацію про обробку, яка вимагається законодавством, виникають обґрунтовані сумніви, що користувач (суб'єкт персональних даних) буде здатним її сприйняти та усвідомити. Що породжує наступний ризик у сфері захисту персональних даних.

З урахуванням зростаючої кількості персональних даних, що збираються різними учасниками мережі 5G, передаються та обробляються у різних точках планети (завдяки великій швидкості роботи мережі та низькій затримці),

користувач втрачає можливість відслідкувати та проконтролювати використання своїх даних.

Збільшення кількості послуг, можливостей підключення, взаємодії, залучених осіб, точок входу та точок управління в мережі, кількості осіб, які впливають на роботу мережі (виробники обладнання, віртуальні оператори тощо) призводить до збільшення так званої “поверхні кібератак” (cyber-attacks surface), тобто загальної кількості потенційно вразливих місць якими можна скористатися для створення загроз конфіденційності.

У мережах 5G буде використовуватися більше компонентів ніж у бездротових мережах попередніх поколінь, зокрема, частин мереж попередніх поколінь, що разом може надати зловмисникам різноманітні можливості для незаконного втручання у роботу мережі та трафік даних. Хоча виробники обладнання 5G та постачальники послуг підвищують безпеку за рахунок удосконалення технологій, зловмисники можуть використовувати як застарілі, так і нові вразливості.

Крім того, розвиток технології Інтернету речей призводить до підключення до мережі 5G численних та потенційно менш безпечних пристроїв.

Технології програмно-визначеної мережі (SDN) та віртуалізації мережевих функцій (NFV) також породжують додаткові ризики та вразливості. В ситуації коли мережею керує програмне забезпечення, ключовим питанням постає досконалість та безпека такого програмного забезпечення. Швидкий розвиток потреб та зростаючі запити ринку можуть спровокувати квапливе розгортання нових мережевих функцій без належної перевірки відповідного програмного забезпечення.

Висновки. Загально прийнято виділяти 7 ключових принципів захисту персональних даних. Коротко розкриємо їх зміст. Фізичні особи повинні бути обізнані про ризики, правила, засоби захисту та права щодо обробки персональних даних, про те, як реалізувати свої права під час такої обробки. Персональні дані повинні оброблятися лише з тією метою, з якою вони були зібрані. Для обробки з новою метою повинна бути окрема підстава обробки. Дозволяється збирати та обробляти мінімальну кількість та обсяг персональних даних, які є достатніми для досягнення мети. Якщо можна досягти цілей без обробки персональних даних – слід утриматися від обробки. Захист від несанкціонованої або незаконної обробки (в тому числі захист від витоку даних), від випадкових або зловмисних втрат даних, їх знищення або пошкодження. Володілець зобов'язаний вжити заходів, які забезпечують можливість підтвердження дотримання ним принципів обробки персональних даних.

Технологію мобільного зв'язку прийнято поділяти на покоління. Кожне покоління відкривало нові можливості та новий функціонал. Особливими відмінностями мереж 5G є висока швидкість та низька затримка передачі

інформації, що призведе до запровадження цілого ряду нових сервісів; пропускна здатність дає можливість підтримувати підключення набагато більшої кількості пристроїв одночасно, що необхідно для розвитку технології Інтернету речей; зменшений радіус покриття базових станцій призведе до безпрецедентно точного визначення місцезнаходження користувача та появи нових сервісів, заснованих на цьому. Крім того, зв'язок буде забезпечуватися не специфічним обладнанням, яке зазвичай використовується для розгортання мережі Інтернет.

Впровадження нових технологій зазвичай породжує специфічні ризики. Більшість з них можна спрогнозувати та вжити попереджувальних заходів. Проте, деякі ризики можна буде виявити лише на практиці. Відтак, мінімізація ризиків та належне реагування на нововиявлені ризики є нагальною потребою сьогодення.

Слід сконцентрувати зусилля на розвитку таких напрямків як:

- ✓ сертифікація та стандартизація обладнання і програмного забезпечення, що відповідає принципам прозорості та технологічної нейтральності і виступає гарантією функціональної сумлінності;

- ✓ законодавче регулювання, яке гарантує дотримання прав та свобод людини та, зокрема, права на приватність;

- ✓ державний контроль за дотриманням вимог щодо захисту персональних даних та стандартів електрозв'язку усіма гравцями ринку із дотриманням принципів технологічної нейтральності та забезпеченням конкурентного середовища;

- ✓ підвищення правової культури як надавачів послуг (контролерів і операторів персональних даних) так і користувачів послуг (суб'єктів персональних даних), що сприяє усвідомленню та підвищенню рівня відповідальності кожної із сторін правовідносин.

В Україні потрібно:

запровадити нові і ефективні правила регулювання сфери електрозв'язку та не допускати надмірної зарегульованості цього ринку щоб не стримувати його розвиток;

прийняти нову редакцію Закону України “Про захист персональних даних” яка встановить вимоги до рівня захисту персональних даних не нижчі ніж це передбачено у Загальному регламенті ЄС про захист даних;

прийняти закон про створення незалежного наглядового органу у сфері захисту персональних даних, який буде інституційно спроможний забезпечити високий рівень контролю за дотриманням галузевого законодавства.

Література:

1. Законі України «Про захист персональних даних» - Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

2. Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних - Режим доступу: https://zakon.rada.gov.ua/laws/show/994_326#Text

3. Регламенті Європейського парламенту та Ради (ЄС) 2016/679 від 27 квітня 2016 року - Режим доступу: офіційний переклад: https://zakon.rada.gov.ua/laws/show/984_008-16#Text; оригінал, англійською мовою: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

4. GDPR: новый уровень защиты персональных данных - Режим доступу: https://interlegal.com.ua/ru/publikacii/gdpr_novyj_uroven_zashhity_personalnyh_dannyh/

5. Гнатюк, С. Л. Особливості захисту персональних даних у сучасному кіберпросторі: правові та техніко-технологічні аспекти [Електронний ресурс] : аналітична доповідь / С. Л. Гнатюк ; Національний інститут стратегічних досліджень. – Київ : [б. в.], 2014. – 92 с. – (Серія «Інформаційні стратегії» ; випуск 3)

6. Становлення і розвиток правових основ та системи захисту персональних даних в Україні Монографія / [В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник] ; за ред. В.М. Брижко, В.Г. Пилипчука. – К. : ТОВ «Видавничий дім «АртЕк», 2017. – 226 с.

References:

1. Zakoni Ukraïni «Pro zahist personal'nih danih» [The Law of Ukraine "On Personal Data Protection"]. (n.d.). zakon.rada.gov.ua. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text> [in Ukrainian].

2. Konvenciï pro zahist osib u zv'jazku z avtomatizovanoju obrobkoju personal'nih danih [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/994_326#Text [in Ukrainian].

3. Reglamenti Evropejs'kogo parlamentu ta Radi (ES) 2016/679 vid 27 kvitnja 2016 roku [Regulation of the European Parliament and of the Council (EU) 2016/679]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/994_326#Text [in Ukrainian].

4. GDPR: novyj uroven' zashhity personal'nyh dannyh [GDPR: a new level of personal data protection]. (n.d.). interlegal.com.ua. Retrieved from https://interlegal.com.ua/ru/publikacii/gdpr_novyj_uroven_zashhity_personalnyh_dannyh/ [in Ukrainian].

5. Gnatjuk, S. L. (2014). *Osoblivosti zahistu personal'nih danih u suchasnomu kiberprostorі: pravovi ta tehniko-tehnologichni aspekti* [Features of protection of personal data in modern cyberspace: legal and technical-technological aspects]. Kіiv: Nacional'nij institut strategichnih doslidzhen' [in Ukrainian].

6. Pilipchuk, V.G., Brizhko, V.M., Baranov, O.A., Mel'nik, K.S. *Stanovlennja i rozvitok pravovih osnov ta sistemi zahistu personal'nih danih v Ukraïni* [Formation and development of legal bases and systems of personal data protection in Ukraine]. K. : TOV «Vidavnichij dim «ArtEk» [in Ukrainian].