НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ

Серія «Інформаційні стратегії». Випуск 3

ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СУЧАСНОМУ КІБЕРПРОСТОРІ: ПРАВОВІ ТА ТЕХНІКО-ТЕХНОЛОГІЧНІ АСПЕКТИ

Аналітична доповідь

Київ 2014

УДК 342.7:004 [55+056.53]
Г 56

Серію засновано
у 2013 році

Автор:
С. Л. Гнатюк, к. і. н.

Електронна версія: http://www.niss.gov.ua

Гнатюк С. Л.

Г 56 Особливості захисту персональних даних у сучасному кіберпросторі: правові та техніко-технологічні аспекти: аналіт. доп. / С. Л. Гнатюк. – К. : НІСД, 2014. – 92 с. – (Сер. «Інформаційні стратегії», вип. 3).

ISBN 978-966-554-236-0

Розглянуто актуальні питання захисту персональних даних у кіберпросторі. Проаналізовано теоретико-правовий зміст понять «персональні дані» та «*прайвесі*» в сучасному європейському праві. Визначено основні риси та тренди еволюції кіберпростору, а також причини, завдяки яким він сьогодні перетворився на найбільш проблемну сферу захисту персональних даних. Вивчено ініціативи Європейської Комісії, спрямовані на оптимізацію правових механізмів захисту персональних даних в інтернет-середовищі. Розглянуто основні напрями розвитку технікотехнологічного й програмного забезпечення безпеки персональних даних у кіберпросторі. Окрему увагу приділено розвитку системи захисту персональних даних у сучасній Україні.

Для спеціалістів у сфері інформаційної безпеки.

ISBN 978-966-554-236-0

ВСТУП[1]

Нині в країнах Європейського співтовариства склалася досить однозначна і стереотипна юридично-правова дефініція самого поняття «персональні дані» (ПД), а також консенсус щодо основних принципів і процедур їх оброблення та захисту. Для країн Центральної та Східної Європи, що запроваджують або модернізують власну систему захисту ПД (до них належить і Україна), саме ця модель слугує певним стандартом і зразком[2]. Насамперед модернізація стосується національних профільних законодавств держав регіону ЦСЄ, які адаптуються до відповідних базових актів Ради Європи та ЄС.

Для порівняння наводимо декілька визначень з відповідних законодавчих актів різного походження. *Європейська Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних,* підписана в Страсбурзі 28 січня 1981 р.: «Персональні дані – це інформація, що стосується конкретної або такої, що може бути ідентифікованою, особи». Класична для європейського галузевого права *Директива Європейського Союзу 95/46/ЄС «Про захист осіб у зв'язку з обробкою персональних даних і вільним обігом цих даних»* від 24 жовтня 1995 р.: «Персональні дані – будь-яка інформація, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити». *Закон Литовської Республіки «Про правовий захист особистих даних»* від 11 червня 1996 р.: «Особисті дані – будь-яка інформація, пов'язана з фізичною особою – суб'єктом даних, ідентичність особи якого встановлена або може бути встановлена безпосередньо або непрямим шляхом з використанням таких даних, як особистий код, одна або декілька фізичних, фізіологічних, психологічних, економічних, культурних або соціальних ознак, характерних для особи». *Закон Російської Федерації «Про персональні дані»* від 27 червня 2006 р.: «Персональні дані – це будь-яка інформація, що належить до визначеної або визначуваної на підставі такої інформації фізичної особи (суб'єктові персональних

---

[1] Усі фактичні дані, надані в аналітичній доповіді, є актуальними на дату проведення «круглого столу» 10 жовтня 2013 р.

[2] Специфічна модель захисту персональної інформації, що збереглася в деяких державах англосаксонського права (США, країни Тихоокеанського регіону) відрізняється від сучасної європейської особливостями законодавчого забезпечення та адміністрування, але жодним чином не суперечить їй на рівні основних правових трактувань, духу закону. Навпаки, саме у США наприкінці XIX ст. вперше отримали науково-правове розроблення ідеї «прайвесі» (*privacy*), сприйняті й у континентальній Європі.

даних), у т.ч. його прізвище, ім'я, по батькові, рік, місяць, дата і місце народження, адреса, сімейний, соціальний, майновий стан, освіта, професія, доходи, інша інформація». *Закон України «Про захист персональних даних»* від 1 червня 2010 р.: «Персональні дані – відомості або сукупність відомостей про фізичну особу, яку ідентифіковано або може бути конкретно ідентифіковано».

Таким чином, в українському законодавстві закріплено типово європейське правове розуміння ПД і присутня відповідна дефініція, більше того, триває його адаптація до європейських норм (докладніше про це – нижче). Разом з тим треба усвідомлювати, що справді ефективний захист персональних даних неможливо налагодити, розглядаючи його тільки як окрему, самодостатню мету і не беручи до уваги той факт, що *в підсумку вся система захисту ПД – це невід'ємний складник загальної системи забезпечення фундаментальних прав людини і громадянина*. І в цьому випадку йдеться про одну з найважливіших ліберально-демократичних свобод – право на недоторканність приватного життя.

Саме на цю обставину звертає увагу Марі Жорж, експерт з питань захисту даних Національної комісії Франції з інформаційних технологій та свобод, аналізуючи одну з редакцій Закону України про захист персональних даних: «Назва Закону говорить про те, що у ньому йдеться про «захист персональних даних». Ця цитата дещо заплутує, адже здається, що йдеться тільки про питання безпеки даних, тоді як ані Конституція України, ані Конвенція № 108 чи Директива ЄС[3] не використовують такий термін. Європейські тексти визначають мету/предмет, використовуючи набагато ширше та чіткіше формулювання: «забезпечення захисту основних прав громадян, зокрема, на їх особисте життя, у зв'язку з обробкою персональних даних»[4].

Ці слова наочно ілюструють сучасне європейське розуміння кореляції між захистом ПД і правами людини, а також ту чималу увагу, що приділяють у Раді Європи і особливо в ЄС їх дотриманню. Логіка тут досить прозора: сучасна демократія з її приматом поваги до прав і гідності людини є немислимою без повноцінного забезпечення недоторканності її особистого життя, приватності, а це, своєю чергою, неможливо без ефективного захисту персональних даних.

---

[3] Маються на увазі Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Страсбург, 28.01.1981 р., № 108) та Директива Європейського Союзу 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 р.

[4] *Аналіз* Закону України «Про захист персональних даних» / Європейський Союз; Рада Європи. – Страсбург. – 2012. – 19 січня [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/dszpd/doccatalog/document?id=51482

Довідково. *В європейській правовій традиції захист приватного життя як норма законодавства має досить глибокі корені. Відповідні правочини трапляються у практиці англійських мирових суддів вже у XIV ст.: визнавалося за провину підглядання та підслуховування. Законодавство Швеції вже у XVIII ст. зобов'язувало державні органи використовувати особисту інформацію тільки у спеціально обумовлених законом цілях*[5]*. Остаточне оформлення й поширення права на недоторканність приватного життя відбулося в Європі в епоху буржуазних революцій. Наприкінці XIX ст., у 1890 р., у США вперше було сформульовано науково-правове обґрунтування категорії «прайвесі» і запропоновано відповідний концепт, що зводився до формули про право особи «бути залишеною у спокої» (right to be left alone). Один з авторів цього визначення, суддя Верховного суду США Луїс Брандайс (Louis Brandeis) вважав прайвесі найбільш цінною з демократичних свобод і виступав за те, щоб її особливий статус був відображений у Конституції*[6]*. У 1990 р. британський Calcutt Committee, провівши якнайретельніше дослідження трактувань «прайвесі» в межах різних епох, культур і політичних систем, констатував, що «ніде не було знайдено абсолютно прийнятного правового визначення» цього поняття. Разом з цим Комітет запропонував власне сучасне визначення терміна: «Право особи чи її родини бути захищеною від втручання в її особисте життя та стосунки безпосередньо фізичним шляхом або через публікацію інформації»*[7]*.*

Укотре інтерес до права на приватність зріс у 60–70-ті роки XX ст. з появою перших ІКТ (у їх сучасному розумінні) і активізацією інформаційних обмінів. Потенційні можливості стеження та збору за допомогою комп'ютерних систем вимагали встановлення спеціальних правил щодо збору та обігу інформації особистого характеру. Основи сучасного законодавства в цій сфері було закладено першим у світі законом про захист даних, який було введено в дію на федеральній землі Гессен у Німеччині в 1970 р. Наступними були національні законодавчі акти Швеції (1973), Сполучених Штатів (1974), Німеччини (1977) та Франції (1978)[8]*.*

Нині ця позиція є загальновизнаною: **недоторканність приватного життя, в т.ч. особистої інформації людини, як одне з її фундаментальних прав закріплено в засадничих міжнародних актах сучасності** – Загальній декларації прав людини ООН, Міжнародному

[5] *Право* на приватність: conditio sine qua non / Харківська правозахисна група. – Харків : Фоліо, 2004. – С. 12. – (Свобода інформації та право на приватність в Україні: в 2 т. / Харківська правозахисна група; т. 2).

[6] Там само. – С. 5.

[7] *Calcutt D.* Report of the Committee on Privacy and Related Matters. – London : H.M.S.O, 1990. – P. 7. – (ser. «Great Britain. Parlament», Issue 1102).

[8] *Право* на приватність: conditio sine qua non / Харківська правозахисна група. – Харків : Фоліо, 2004. – С. 13. – (Свобода інформації та право на приватність в Україні: в 2 т. / Харківська правозахисна група; т. 2).

пакті про громадянські й політичні права, Конвенції ООН про права дитини, багатьох інших міжнародних і регіональних угодах. Право на приватність тією чи іншою мірою визнається також у більшості національних законодавств світу, причому зазвичай на рівні конституцій[9].

У статті 8 Європейської Конвенції з прав людини це право сформульовано таким чином:

• кожна людина має право на повагу до її особистого і сімейного життя, житла і таємниці листування;

• держава не може втручатися у здійснення цього права інакше ніж згідно із законом та у випадках, необхідних у демократичному суспільстві в інтересах національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням і злочинам, для захисту здоров'я або моралі чи з метою захисту прав і свобод інших людей[10].

Як бачимо, у цій правовій нормі присутній складник *інформаційної приватності*, що встановлює правила збору та обігу персональних даних.

Основи ідеології захисту ПД у правовій практиці сучасних демократичних держав можна звести до таких положень: 1) пріоритетним є право особи розпоряджатися своїми персональними даними; їх використання без дозволу суб'єкта ПД карається згідно із законодавством; 2) для будь-кого, хто здійснює користування персональними даними фізичних осіб з їх дозволу, встановлено відповідальність за умисне розголошування цих даних третім особам (якщо тільки фізична особа не дала дозвіл на таке розголошування)[11].

Таким чином, окреслюються основні права суб'єкта персональних даних. Він має право знати:

• *хто і де обробляє* його ПД;

• *кому передаються* його ПД;

• *де зберігаються* його ПД;

• *як реалізувати право на доступ* до своїх ПД (право на доступ також належить до основних);

• *механізми оброблення* його ПД (у разі їх автоматичного оброблення).

---

[9] *Право* на приватність: conditio sine qua non / Харківська правозахисна група. – Харків : Фоліо, 2004. – С. 5. – (Свобода інформації та право на приватність в Україні: в 2 т. / Харківська правозахисна група; т. 2).

[10] *Конвенція* про захист прав людини і основоположних свобод / Рада Європи [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/995_004

[11] У рамках національних законодавств, однак, зазвичай є спеціально прописані випадки винятків з цих двох фундаментальних правил.

Крім того, до основних прав особи належить право *вимагати знищення чи виправлення* своїх ПД, якщо вони обробляються незаконно чи є недостовірними[12].

З означеними пріоритетами й правами безпосередньо корелюють **вісім основних принципів оброблення персональних даних**, сформульованих ще у 1981 р. Конвенцією Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ст.ст. 5–8). Згідно з ними ПД мають:

• оброблятися сумлінно і законно, причому тільки за наявності підстав та з дотриманням вимог (*принцип законності*);

• отримуватися з конкретними законними цілями та не оброблятися у способи, несумісні з цими цілями (*принцип конкретності цілей*);

• бути адекватними, не надлишковими, відповідати цілям оброблення (*принцип пропорційності*);

• бути точними та своєчасно оновлюватися (*принцип якості даних*);

• не зберігатися довше, ніж це необхідно (*принцип обмеження терміну оброблення*);

• оброблятися з дотриманням прав фізичної особи, включаючи право на доступ до даних та заперечення щодо їх обробки (*принцип прозорості та опозиції*);

• оброблятися з дотриманням технічних вимог щодо захисту даних (*принцип захисту даних*);

• не передаватися поза межі країни без відповідного захисту (*принцип обмеження передачі іноземним суб'єктам*)[13].

Цих норм, принципів і процедур вдавалося дотримуватися у «доцифрову» епоху, коли повсякденні інформаційні обміни відбувалися безпосередньо у фізичному середовищі або за допомогою пристроїв і мереж, які можна було відносно легко ідентифікувати та відстежити (наприклад, телефон чи радіо). Але **технологічний прогрес і глобалізація значно змінили процес збору персональних даних, здійснення доступу до них та способи їх використання (оброблення)**.

Майже в усіх країнах і міждержавних об'єднаннях **найбільш проблемною сферою захисту ПД сьогодні є *IT* і кіберпростір** як нове специфічне інформаційно-комунікаційне середовище, що стрімко розвивається і збільшується. У цій сфері нормативно-правове регулювання хронічно відстає від якісного (технології) та кількісного (пропускна

[12] *Козак В.* Захист персональних даних: право, практика, нагляд / В. Козак [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/dszpd/doccatalog/document?id=51760

[13] *Конвенція* про захист осіб у зв'язку з автоматизованою обробкою персональних даних / Рада Європи. – Страсбург. – 1981. – 28 січня [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_326

здатність і поширеність інфраструктур) розвитку. Це відставання окреслилося ще у 80–90-х роках XX ст., але **стало дійсно системною проблемою протягом 2000-х років** разом із появою революційних винаходів та змінами в інформаційно-комунікаційних технологіях (ІКТ), лавиноподібним розширенням Всесвітньої мережі і міграцією цілих сфер людської діяльності в онлайн-сектор. Виникло й продовжує швидко зростати цілком нове, унікальне середовище, в якому традиційні нормативно-правові механізми, практики та підходи щодо захисту персональних даних стають здебільшого неефективними.

РОЗДІЛ І.
ПРОБЛЕМАТИКА ТА СПЕЦИФІКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У КІБЕРПРОСТОРІ

У наш час інтернет остаточно став глобальною – не лише за принципами організації, а й за кількісними показниками – мережею, кількість його користувачів уже наблизилася до трьох мільярдів і продовжує швидко зростати. Нині приблизно третина населення Землі користується інтернетом, а у 2015 р., за підрахунками, ним буде користуватися половина людства[14]. Так само швидко вдосконалюються *IT*, їх виробничі потужності, масового розповсюдження набула багатофункціональна й високопродуктивна мобільна електроніка. Уже сьогодні інтернет і асоційовані з ним інформаційні технології, сервіси та комунікативні середовища є дійсно всеохоплюючою, загальнодоступною і абсолютно необхідною для нормальної життєдіяльності людства структурою.

Визнання права людини на анонімність в он-лайні завжди було одним із стовпів архітектури та філософії інтернету. Водночас за логікою цієї ж архітектури **без розміщення особою персональних даних на віддалених серверах (а отже, у мережі) повноцінне послуговування всіма її вигодами є неможливим**. У більшості випадків користувач не

[14] У 2008 р. кількість унікальних користувачів інтернету нарешті досягла 1 млрд, на початку 2013 р. – 2,75 млрд (майже 40 % населення Землі), а до 2017 р., за прогнозами компанії *Cisco Systems*, онлайн-аудиторія зросте до 3,6 млрд осіб, склавши близько половини (48 %) людства. Згідно з тими самими прогнозами у 2016 р. глобальний трафік Всесвітньої мережі сягне 1,3 зеттабайт (1 зеттабайт дорівнює 1 млрд терабайт), що перевищить сумарний трафік інтернету з моменту його створення до 2012 р. включно (Див.: *ICT Facts* and Figures – The World in 2013: International Telecommunication Union (ITU) report [Електронний ресурс]. – Режим доступу: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf; *Cisco* Visual Networking Index: Forecast and Methodology, 2012–2017 [Електронний ресурс]. – Режим доступу: http://clck.ru/8paTe).

може здійснити найпростіших речей (встановити програмне забезпечення, завантажити контент, здійснити покупку), не залишивши натомість хоча б мінімальних відомостей про себе. Зрештою **навіть ті дані (здавалося б, суто технічні і необхідні системі для нормальної роботи он-лайн), що ними пристрій користувача в автоматичному режимі обмінюється з віддаленими серверами, є такими, за якими «особа може бути конкретно ідентифікованою», тобто з нормативно-правового погляду – персональними.**

Так, кожного разу, підключаючись до мережі, пристрій користувача автоматично реєструється в ній, вказуючи унікальний ідентифікатор – *IP*-адресу, телефонний номер комутованого з'єднання, абонентський номер договору з оператором доступу та інші, необхідні для реєстрації в мережі, дані. Далі, мандруючи інтернетом, особа залишає за собою інформаційний «шлейф», що складається з іще більшої кількості відомостей. Нижче наведено мінімальний перелік даних, які автоматично передаються і залишаються в мережі при кожному відвіданні будь-якого веб-ресурсу:

• веб-адреса сторінки, що переглядається (*URL*);

• веб-адреса сторінки, що посилається на першу;

• унікальна *IP*-адреса, найменування провайдера, країна реєстрації, місцезнаходження пристрою;

• параметри браузера (тип, версія, мова, налаштування, підтримка додатків) та комп'ютера (основні апаратні можливості, операційна система, роздільна здатність екрану тощо);

• дані проксі-сервера;

• дані про підтримку *cookies*[15] і *Java*;

• часовий пояс.

Нагадаємо, йдеться не про цілеспрямований пошук ПД, а лише про той мінімум даних, що в режимі он-лайн передається комп'ютером користувача *у штатному режимі, постійно і автоматично*.

В умовах нинішньої **тотальної «інтернетизації» інфраструктур** – телекомунікацій, систем транспортування, фінансів, обліку населення, медичного обслуговування, численних баз даних багаторазово збільшує кількість та якість інформації, що опрацьовується щодо кожної особи в кіберпросторі, причому часто без її відома. Стрімко розвива-

[15] *HTTP-cookies, «Кукі, кукіз»* (англ. *cookies* – тістечка, печиво) – у комп'ютерній термінології – невеликі фрагменти текстових або бінарних даних, що відправляються веб-сервером і зберігаються на комп'ютері користувача. При кожній спробі відкрити сторінку відповідного сайту веб-клієнт (браузер) користувача пересилає такий фрагмент даних веб-серверу у вигляді *HTTP*-запиту. Заявлене призначення і сфера застосування є такими: а) збереження даних на стороні користувача; б) аутентифікація користувача; в) зберігання персональних переваг і налаштувань користувача; г) відстеження стану сесії доступу.

ються також **публічні онлайн-сектори**, де населення масово та усвідомлено залишає свої персональні дані: електронний бізнес, банкінг і шопінг, цілий спектр онлайн-послуг, електронна пошта, середовище *Web* 2.0.[16], хмарові сервіси, онлайн-аутсорсинг і багато іншого. Ідеться про заповнення відвідувачами різноманітних анкет, реєстрацію та отримання логіна і пароля, реєстрацію з використанням облікового запису соціальної мережі, надання електронної адреси відвідувача для зворотного зв'язку тощо.

Можливість надійного захисту своєї анонімності та персональних даних у такому середовищі стає для користувача майже нульовою, навіть якщо він дотримується рекомендованих вимог безпеки. Апаратні можливості *IT*-обладнання вже досить давно дозволяють не видаляти дані, що обертаються у вебі, і автоматично зберігати їх. Тому незалежно від обраного особою режиму доступу до ПД **всі приватні відомості**, що розміщуються нею в он-лайні, або з певних причин потрапляють до мережі з її локальних сховищ, **зберігаються у віддалених сховищах і базах даних** інтернету. Таким чином, вони залишаються відкритими для несанкціонованого доступу, причому **пересічний користувач-суб'єкт цих персональних даних зазвичай не має технологічної можливості проконтролювати їх подальшу міграцію та оброблення**. Тому з технічного погляду не є особливою проблемою **створення детального досьє на будь-яку особу** та/або систематичний збір інформації про неї. Уже не перший рік такі маніпуляції здійснюються та аналізуються комп'ютерними системами в автоматичному режимі. **Для зацікавленої людини чи організації питання полягає лише в доступі (законному чи ні) до потрібних інформаційних ресурсів.**

При цьому можуть оброблятися персональні дані дуже широкого діапазону: від анкетних даних (відомості про ідентифіковану особу) до відомостей, які можуть стосуватися особи опосередковано або які можуть використовуватися у процесі ідентифікації особи (інформація про оплату послуг з використанням платіжних карт, логіни та паролі, записи в соціальній мережі, номери телефонів, електронні адреси тощо).

Відповідно, існує і постійно вдосконалюється **ціле сімейство технологій для створення баз персональних даних, індивідуальних і групових «профілів»** на основі збору та аналізу всіх відомостей, що мають будь-який (у т.ч. непрямий) стосунок до користувачів. Наприклад, для відстеження особливостей поведінки відвідувачів веб-ресурсів традиційно використовуються такі – вже класичні – методики, як:

---

[16] *Web* 2.0., за визначенням одного з головних його ідеологів Тіма О'Рейлі, є «методикою проектування систем, які шляхом обліку мережевих взаємодій стають тим краще, чим більше людей ними користуються». Власне, терміном «*Web* 2.0.» прийнято називати сукупність онлайн-проектів і сервісів, що розвиваються і вдосконалюються самими користувачами: блоги, *wiki*, соціальні мережі та ін.

• надсилання до пристрою користувача файлів *cookies* першої та *cookies* третьої сторони (при транзиті через посередницькі проксі-сервери);

• збирання протягом тривалого часу в базах веб-ресурсів детальної інформації про відвідані сторінки, обрані режими, натиснуті клавіші тощо та її подальше оброблення;

• збирання в базах веб-ресурсів інформації про апаратні та програмні засоби, які встановлено в користувача, тощо.

> ***Довідково.*** *Розслідування, проведене газетою The Wall Street Journal ще у 2010 р., свідчить, що в окремих випадках до встановлення імені та особи користувача за його «інтернет-портретом», зібраним автоматичними сервісами поведінкового таргетинга[17], лишається кілька кроків. У зв'язку з цим розслідуванням експерти Electronic Frontier Foundation, американської неурядової організації із захисту приватного життя в онлайн-просторі, наводять такі дані: «з теорії мереж відомо, що для повної деанонімізації особи достатньо 33 біти інформації. Такі біти, як поштовий індекс або дата народження, мають більшу вагу (апроксимуючу цінність), ніж інші. При цьому [x+1] Inc., логістичний сервіс Capital One Financial Company, за єдиний клік збирає на одного з восьми відвідувачів 26,5 біта. Це означає, що особу вдається встановити з точністю 1 до 64, тобто у всьому світі не знайдеться більше 64 осіб з аналогічною сукупністю параметрів профілю. Однозначна деанонімізація цієї людини потребувала б лише ще одного важкого біта – наприклад, даних про точний вік[18].*

Прикладом ефективності **сучасних методик аналізу метаданих**[19] є моніторинг статистики телефонних з'єднань або електронного листування, який нині широко використовується для визначення й відстеження контактів між людьми. Цей метод, зокрема, **дає змогу створювати точні й докладні зрізи соціальних зв'язків**. Видання *CHIP.ua*,

---

[17] Поведінковий таргетинг (англ. *target* – ціль) – технологія збору та оброблення інформації, суть якої зводиться до впровадження механізму збору даних про дії користувача в інтернеті за допомогою *cookie*-файлів. Інформація збирається в спеціальних «профілях» і містить дані про проглянуті сайти, пошукові запити, покупки в інтернет-магазинах тощо. Сформувавши такий профіль, можна не лише стати власником контактних даних об'єкта, а й досить чітко уявити собі його соціопсихологічний портрет (звички, смаки, пристрасті, суспільно-політичні преференції, коло контактів, рівень доходів тощо).

[18] *Эпоха* анонимности в сети заканчивается [Електронний ресурс]. – Режим доступу: http://mmr.net.ua/news/id/20861/

[19] Метадані – дані, що характеризують або пояснюють інші дані, інформація про дані. В аспекті проблематики, що висвітлюється це зазвичай технічна статистика мережі – історія онлайн-відвідувань з певної *IP*-адреси, обрані налаштування та режими роботи, натиснуті клавіші, кліки, «неприв'язані» номери телефонів, банківських карт тощо. Самі собою ці дані можуть не бути персональними даними суб'єкта, проте їх співставлення та аналіз дають змогу, приміром, ідентифікувати особу, налагодити збір інформації про неї тощо.

посилаючись на заяви заступника директора Агентства національної безпеки США Джона Інгліса (*John Inglis*), стверджує, що таким чином можна контролювати до трьох рівнів контактів однієї особи. Іншими словами, якщо в людини в середньому є 100 прямих онлайн-кореспондентів, то в контактах третього рівня теоретично може бути задіяно до мільйона осіб (100×100×100). Усі ці дані можна видобути і проаналізувати, приміром, задля знаходження жертви (зловмисника) або перевірки когось з підозрюваних (у діяльності спецслужб)[20].

Навіть у країнах найбільш демократичних і з більш суворим законодавством щодо захисту ПД **завжди було поширеним незаконне зняття інформації з електронних каналів зв'язку**. Свідченням тому є **численні скандали, шлейф яких тягнеться у 80–90-ті роки XX ст.**, в часи, коли з'явилися перші великі електронні бази даних і поштові сервіси[21]. Але значно більших масштабів ця проблема набула після 2000 р., особливо у зв'язку з бурхливим розвитком середовища *Web* 2.0. та його найпопулярнішого складника – **соціальних медіа**. **Уже наприкінці 2012 р. 6 із 10 користувачів інтернету (майже 1,5 млрд осіб) хоча б раз на день відвідували свої аккаунти** у тих чи інших соціальних мережах, залишаючи власні та/чи обробляючи чужі дані. Оскільки сегмент соціальних медіа нині стабільно зростає, то немає жодного сумніву, що протягом 2013–2014 рр. їхня аудиторія стала ще більшою. Середньостатистичний користувач цих сервісів зареєстрований в 1–3 мережах, але приблизно кожний десятий – у 5 і більше[22]. Таким чином, **ідеться про обіг у віртуальному середовищі гігантської кількості актуальних персональних даних значної частини населення земної кулі**.

У цьому контексті досить закономірними є **пов'язані з несанкціонованим витоком персональних даних численні скандали і судові конфлікти між провідними соціальними мережами (*Facebook*, *Twitter*, *Google+* та інші) з глобальним охопленням і обмежені окремими країнами, з пересічними фізичними чи юридичними особами**. Причому нерідко йдеться про незаконний «злам» сотень тисяч аккаунтів.

Кількість подібних інцидентів є занадто великою, а самі вони надто стереотипними для того, щоб наводити про них докладну інформацію. Останній гучний скандал (або, скоріше, низка скандалів)

---

[20] *Большой* брат следит за тобой [Електронний ресурс]. – Режим доступу: http://www.chip.ua/stati/bolshoy-brat-sledit-za-toboy/

[21] Згідно з останніми даними ця історія має ще більш глибоке коріння. Зокрема, у вересні 2013 р. АНБ США (підрозділ радіотехнічної та електронної розвідки Міністерства оборони США) визнало, що стежило в 1970-х роках за правозахисниками та журналістами.

[22] *Social* Media Around the World 2012 [Електронний ресурс]. – Режим доступу: http://www.slideshare.net/slideshow/embed_code/14426292?rel=0#

пов'язаний з ім'ям Едварда Сноудена (*Edward Snowden*). На початку червня 2013 р. газета *The Guardian* отримала й опублікувала текст секретного судового вироку, згідно з яким американській телекомунікаційній компанії *Verizon* належало упродовж трьох місяців щодня передавати державним структурам США дані про дзвінки своїх клієнтів. Газета *The Washington Post*, своєю чергою, повідомила про існування секретної програми *PRISM*, за допомогою якої спецслужби отримують доступ до даних найбільших світових *IT*-корпорацій. Також повідомлялося, що спецслужби США мають прямий доступ до серверів провідних інтернет-компаній і сервісів – *Microsoft*, *Yahoo*!, *Google*, *Facebook*, *PalTalk*, *AOL*, *Skype*, *YouTube*, *Apple*[23]. Компанії спростували ці повідомлення. Колишній співробітник ЦРУ Едвард Сноуден мав доступ до системи збору даних про користувачів цих сервісів. За його власною версією, він вирішив розкрити інформацію про порушення прав громадян з боку спецслужб, зібрав усі можливі підтвердження цих порушень і, переїхавши до Гонконгу, почав звідти передавати ці відомості для медіа.

Скандал навколо *PRISM* продемонстрував й інше: ступінь співпраці таких корпорацій та спеціальних служб державних органів. Рівень такого співробітництва, його динаміка та глибина, а також обсяги та характер відомостей про особу, що надаються приватними компаніями спецслужбам, мимоволі наштовхують на думку про те, що захист персональних даних людини в тому вигляді, як вони розуміються зараз, є якщо не безнадійною, то дуже складною справою.

Додаткові й дуже серйозні ступені ризику щодо безпеки даних мають елементи новітньої третьої *IT*-платформи, яка принципово орієнтована на: а) зберігання основної частини інформації користувачів не на особистих фізичних носіях, а у віртуальному середовищі; б) швидкий доступ до інтернету, а також автоматизацію і підключення до нього всієї виробничої, транспортної, адміністративної, бізнесово-фінансової, побутової (аж до помешкань і пральних машин) інфраструктури[24]. Зрозуміло, що модель розгортання веб-середовища з по-

---

[23] Крім агрегації значної кількості даних, сучасні комунікаційні онлайн-сервіси у принципі надають можливість автоматичної ідентифікації будь-якої особи в мережі, перманентного збору та довічного збереження даних про неї, включаючи стеження за її переміщеннями в режимі реального часу.

[24] Див., зокрема: *IDC* Predictions 2013 – Competing on the 3rd Platform [Електронний ресурс]. – Режим доступу: http://www.idc.com/research/Predictions13/downloadable/238044.pdf; *2013-й* – год конкуренции вокруг «третьей» платформы [Електронний ресурс]. – Режим доступу: http://www.pcweek.ru/idea/article/detail.php?ID=146072; *Третья* платформа ИТ: «большая семерка» ОС, версия 2012 [Електронний ресурс]. – Режим доступу: http://www.osp.ru/os/2011/10/13012228/; «*Третья* платформа»: что нам ждать в 2013-м [Електронний ресурс]. – Режим доступу: http://www.pcweek.ru/idea/blog/idea/4695.php

дібними характеристиками передбачає формування масової (аж до стовідсоткового охоплення) онлайн-аудиторії, оснащеної такими пристроями доступу, які завжди можуть бути під рукою. Сьогодні це вже стає реальністю: при дуже високих темпах зростання кількості користувачів і підключень до Всесвітньої мережі найвища динаміка все-таки спостерігається у тих її сегментах, які пов'язані з виходом в інтернет за допомогою сучасних **мобільних пристроїв** і безпроводових мереж.

На сьогодні більшість населення Землі користується стільниковими телефонами: у I кв. 2013 р. кількість таких користувачів становила 7,1 млрд осіб, а діючих передплат на послуги мобільного зв'язку тоді ж було зафіксовано 6,8 млрд[25]. Це охоплює **96,2 % людства**.

У будь-якому сучасному «мобільнику» обов'язково присутня функція виходу в інтернет, але глобальні ринки впевнено завойовує наступне покоління телефонів – орієнтовані на постійне перебування в онлайн-режимі смартфони-мінікомп'ютери, в яких можливості веб-серфінгу максимально оптимізовані та урізноманітнені. Сьогодні апаратних та софтверних потужностей навіть середнього за класом смартфону цілком достатньо для перегляду будь-якого контенту та обміну ним, спілкування через аккаунти користувача в поштових сервісах, соціальних мережах і *Skype*, завантаження додатків, користування *GPS*-навігатором тощо.

Але **зворотним боком високої технологічності й багатофункціональності сучасних смартфонів є їхні унікальні «шпигунські» можливості**, які активно використовуються зловмисниками. Значна частина штатного програмного забезпечення для смартфонів у принципі дає змогу для ідентифікації будь-якої особи в мережі, ознайомлення з контентом її пристрою, перманентного збору даних про неї, стеження за її переміщеннями в режимі реального часу тощо[26]. Часто такий функціонал уже активований у налаштуваннях програм «за замовчуванням», і більшість користувачів просто не знає про саму можливість та/або необхідність зміни цих налаштувань.

Крім того, існують додатки та утиліти, за допомогою яких, наприклад, можна непомітно для користувача (а) у фоновому режимі задіяти мікрофон пристрою, прослуховуючи все, що відбувається навколо нього, (б) «змусити» камеру смартфону робити серії фотознімків,

---

[25] *ICT Facts* and Figures – The World in 2013: International Telecommunication Union (ITU) report [Електронний ресурс]. – Режим доступу: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf; *Клепов А.* Stealthphone: мобильность меняет вектор развития ИБ: мат. конф. «Безопасность бизнеса. Технологии 2013», Москва, 19 сентября 2012 г. / А. Клепов [Електронний ресурс]. – Режим доступу: http://bc.rbc.ru/msk/security2013/stuff.shtml

[26] Див., наприклад: *Android*-приложение «фонарик» способно следить за пользователями [Електронний ресурс]. – Режим доступу: http://internetua.com/Android-prilojenie--fonarik – sposobno-sledit-za-polzovatelyami

з яких потім можна створити детальну панораму робочого місця або житла користувача, (в) за допомогою штатних вбудованих сенсорів руху смартфона – з точністю до 80 % розпізнавати текст, що набирається на клавіатурі, поряд з якою він знаходиться, тощо[27]. Зрозуміло, що всі ці технологічні можливості масово використовуються як правоохоронними та спеціальними органами (у межах легальних програм), так і злочинними суб'єктами – з протиправною метою.

Крім подібного «спеціалізованого» шпигунського ПЗ, власники сучасних мобільних пристроїв потерпають і від більш традиційних загроз: комп'ютерних вірусів, «черв'яків», троянських програм, що спричиняють витік даних, недобросовісних платіжних та/чи кредитних сервісів, онлайн-крадіжок тощо. Причому **найбільше негативних показників та загрозливу динаміку зареєстровано саме в сегменті програмного забезпечення для мобільних пристроїв**. Так, лише за 2012 р. і I кв. 2013 р. кількість програм-шкідників для однієї тільки платформи *Android* збільшилася аж на 614 %. Для порівняння: у 2011 р. цей показник становив 155 %[28].

Отже, навіть без урахування суто «стільникового» складника комунікацій (розмови й повідомлення в мережах *GSM*) **сучасний смартфон є пристроєм, що за необхідності постійно, у т.ч. без відома абонента, передає безпроводовими інтернет-каналами його персональні дані** (включаючи навіть дані про поточне місцезнаходження користувача – якщо згадати про вбудовані функції *GPS*-навігації і геотегінгу фотознімків, зроблених камерою смартфону). При цьому, за деякими даними, на 80 % мобільних телефонів, що використовуються нині у світі, не встановлено жодних засобів захисту.

Уже **наприкінці 2012 р. у світі використовувалося 1,3 млрд смартфонів** і було оформлено 1,1 млрд передплат на спеціальні онлайн-послуги для них[29]. І все ж очікується, що до 2015 р. ці показники збільшаться майже втричі[30].

Ще швидше зростають продажі інших мобільних пристроїв з можливістю виходу в інтернет. Їх вартість, функціональність та форм-фактор постійно вдосконалюються, стають різноманітнішими – від звичайних

---

[27] *Шпифон*: наблюдение за личной жизнью владельца [Електронний ресурс]. – Режим доступу: http://www.chip.ua/stati/shpifon-nablyudenie-za-lichnoi-zhiznyu-vladelca/

[28] *Android* Malware Climbs 614 Percent in 2012: Study [Електронний ресурс]. – Режим доступу: http://www.eweek.com/security/android-malware-climbs-614-percent-in-2012-study/

[29] *Internet* 2012 in numbers [Електронний ресурс]. – Режим доступу: http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/

[30] *Mashable* – Ожидается, что глобальный Интернет-трафик к 2015 возрастет в четыре раза [Електронний ресурс]. – Режим доступу: http://www.denwer.ru/ls/blog/mashable/324.html

«електронних книжок» і міні-планшетів до потужних ультрабуків. І вже зараз ці «девайси» здатні задовольнити інформаційно-комунікаційні потреби будь-якого споживача. Вражаючими темпами цей сегмент *IT* зростає й кількісно: за прогнозами, **протягом подальших чотирьох років кількість продажів планшетних комп'ютерів збільшиться на 750 %, а електронних рідерів – на 550 %**[31].

Таким чином, цілком закономірними є цифри, що віддзеркалюють динаміку технологічної модернізації Всесвітньої мережі. Станом на липень 2013 р. на мобільні пристрої припало 17,4 % світового інтернет-трафіку, при тому, що роком раніше цей показник становив приблизно 11,1 %[32]. Передбачається, що до 2016 р. обсяг глобального мобільного трафіку перевищить обсяг проводового, а у 2017 р. їх співвідношення становитиме від 55 до 45 %[33]. Таким чином, **домінуючим трендом розвитку інтернету є його перетворення на всюдисущу, загальнодоступну і абсолютно необхідну для нормальної життєдіяльності людства структуру**.

У тісній інтеграції з мобільними пристроями, безпровідними широкосмуговими інтернет-мережами, соціальними сервісами (*Web* 2.0.) і обробленням «великих даних» (*Big Data*) розвиваються **сервіси т.зв. «хмарового оброблення» даних** (*cloud computing services*)[34] – одна з основ інфраструктури третього покоління.

Останніми роками ця технологія активно пропагується і масово впроваджується провідними світовими *IT*-корпораціями, про-

---

[31] *Mashable* – Ожидается, что глобальный Интернет-трафик к 2015 возрастет в четыре раза [Електронний ресурс]. – Режим доступу: http://www.denwer.ru/ls/blog/mashable/324.html.

[32] *17,4 % глобального* интернет-трафика приходится на мобильные устройства [Електронний ресурс]. – Режим доступу: http://internetua.com/17-4--globalnogo-internet-trafika-prihoditsya-na-mobilnie-ustroistva

[33] *Cisc*o Visual Networking Index: Forecast and Methodology, 2012–2017 [Електронний ресурс]. – Режим доступу: http://clck.ru/8paTe

[34] «Хмарові» обчислення (*cloud computing*, також використовується поняття «хмарове» оброблення даних) – технологія оброблення даних, у якій комп'ютерні ресурси надаються користувачеві як інтернет-сервіс. Користувач не повинен піклуватися про інфраструктуру, операційну систему, купівлю та оновлення програмного забезпечення, має доступ до власних даних он-лайн, але, відповідно, не може повною мірою контролювати їх оброблення і захист. Поняття «хмара» використовується як метафора, що ґрунтується на уявленні інтернету як «хмари» мережних зв'язків або складної інфраструктури, за якою ховаються усі технічні деталі. Згідно з визначенням *Institute of Electrical and Electronics Engineers (IEEE)*, запропонованим у 2008 р., «хмарове оброблення даних – це парадигма, в межах якої інформація клієнта постійно зберігається на серверах в інтернеті та тимчасово кешується на клієнтській стороні, наприклад на персональних комп'ютерах, ігрових приставках, ноутбуках, смартфонах та ін.» (Див.: *Behl A.* Security Paradigms for Cloud Computing / A. Behl, K. Behl // CICSyN 2012: Fourth International Conference on Computational Intelligence, Communication Systems & Networks [Електронний ресурс]. – Режим доступу: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6273236).

те справжній бум зростання «хмарових» ринків прогнозується у 2013 –2015 рр. Достатньо сказати, що за підрахунками авторитетної *International Data Corporation* (*IDC*), вже у 2015 р. до 60 % усіх даних людства зберігатимуться в «хмарах»[35]. Понад те, за одностайними прогнозами провідних консалтингових компаній світу, **швидке вдосконалення та поширення «хмарових» технологій зараз є одним із тих головних трендів, що в найближчі 5–8 років помітно вплинуть на глобальний розвиток** не лише *IT*-індустрії, а й бізнесу, фінансів, державного управління, медицини, освіти і багатьох інших сфер людської діяльності[36]. У найбільш розвинених регіонах світу вже прийнято стратегічні рішення та плани дій щодо системного та комплексного розвитку «хмарових» сервісів, розгорнуто відповідну роботу. Значне й стрімке зростання ринку «хмарових» послуг очікується найближчими роками і в Україні[37]. У контексті даної доповіді все це спонукає детальніше зупинитися на безпекових аспектах «хмарових» технологій.

Підкреслимо, що навіть порівняно з грід-системами, не говорячи вже про «проводово-апаратні» мережі попереднього покоління, сучасний «хмаровий» сервіс та його архітектура є більш лаконічним, продуктивним, універсальним і, що суттєво, – дешевим рішенням. Без сумніву, значні переваги «хмар» (див. Розділ ІІ) стали однією з основних причин їх популярності й феноменально швидкого поширення.

Разом з цим **фундаментальним недоліком «хмарових» сервісів є високі ризики за їх використання**. У квітні 2012 р. т.зв. Берлінська група – авторитетна міжнародна команда експертів із захисту персональних даних у телекомунікаційних мережах[38] – опублікувала результати спеціального профільного дослідження, яке отримало назву «Сопотський меморандум». У документі фіксуються, зокрема, такі проблеми та ризики використання «хмар»:

• технологія все ще знаходиться на стадії розроблення і не апробована остаточно;

---

[35] *IDC Predictions* 2013. Competing on the 3rd Platform: Opportunities at the Intersection of Mobile, Cloud, Social, and Big Data [Електронний ресурс]. – Режим доступу: http://clck.ru/8aXZM

[36] Див., зокрема: *Symantec* : Protecting a Cloudier Future: Market Report, 2012, November [Електронний ресурс]. – Режим доступу: http://www.symantec.com/content/en/us/enterprise/white_papers/esg-protecting-a-cloudier-future.en-us.pdf; *Symantec*. Avoiding the Hidden Costs of the Cloud [Електронний ресурс]. – Режим доступу: http://www.symantec.com/connect/blogs/avoiding-hidden-costs-cloud; *IDC Predictions* 2013. Competing on the 3rd Platform: Opportunities at the Intersection of Mobile, Cloud, Social, and Big Data [Електронний ресурс]. – Режим доступу: http://clck.ru/8aXZM

[37] Докладніше про розвиток «хмарових» технологій та ринків в Україні та світі – у наступних розділах.

[38] *International* Working Group on Data Protection in Telecommunications (IWGDPT) [Електронний ресурс]. – Режим доступу: http://clck.ru/8aXVe

• досі немає міжнародної угоди про єдину термінологію, хоча технологія є транскордонною, а оброблення даних фактично стало глобальним процесом;

• діяльність провайдерів є недостатньо прозорою і не може бути повністю відстежена. Це значно ускладнює оцінку ризиків і створення єдиних правил гри;

• дотримання конфіденційності, недоторканності інформації та режиму доступу до неї не може бути проконтрольоване у «хмарах»;

• під час передачі ПД потрапляють під юрисдикції, в яких не передбачено їх адекватного захисту;

• провайдери та їх партнери використовують приватні дані у своїх інтересах без повідомлення про це суб'єкта та його згоди;

• локальні (національні) контролюючі інститути із захисту ПД фактично не мають можливості нагляду за процесом оброблення даних провайдерами «хмарових» послуг[39].

Висновки експертів цілком підтверджуються наявними цифрами та фактами. Результати глобального дослідження *Avoiding the Hidden Costs of the Cloud*, здійсненого компанією *Symantec* на початку 2013 р., дають змогу дійти висновку про значний відсоток недоброчесних «гравців» на ринку «хмарових» послуг. Так, 77 % опитаних у рамках дослідження організацій щонайменше один раз стикалися з шахрайськими сервісами, а 40 % з цієї кількості стали жертвами викрадення конфіденційних даних[40].

У контексті прогнозів щодо значного збільшення обсягів і масштабів використання віртуальної інформації (освоєння «великих даних») «хмари» стають критично важливим ресурсом завдяки можливості зберігання в них практично необмежених обсягів даних, доступних он-лайн для особистого та/чи корпоративного користування. Понад те, тренди *IT*-індустрії вже сьогодні роблять такі «мегасховища» актуальними для користувачів.

Водночас проведений у 2012 р. глобальний моніторинг британської компанії *Icomm Technologies* засвідчив, що сьогодні «хмарові» сервіси здебільшого не відповідають ані елементарним вимогам безпеки, ані нормам законодавства. На запити користувачів щодо фізичного місцезнаходження їхніх даних (країна, точне розташування) та, відповідно, щодо їх поточної юрисдикції 70 % провайдерів не змогли дати відповіді або намагалися її уникнути будь-яким чином. У матеріалах моні-

---

[39] *Working* Paper on Cloud Computing – Privacy and data protection issues (Sopot Memorandum) / International Working Group on Data Protection in Telecommunications 51st meeting, 23-24 April 2012, Sopot (Poland) [Електронний ресурс]. – Режим доступу: http://clck.ru/8aJ9c

[40] *Мошеннические* облачные сервисы – бич 77 % компаний [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/436587.php

торингу підкреслюється, що, прагнучи знайти найбільш вигідні умови для фізичного розміщення даних, більшість провайдерів практикують оренду площ і потужностей у віддалених країнах, нерідко з недосконалим законодавством у сфері кіберзахисту та захисту персональних даних. Зрозуміло, що в безпековому аспекті таке становище створює серйозні ризики щонайменше за двома напрямами: 1) нормативно-правовим (конфлікт юрисдикцій у частині регулювання транскордонної передачі даних і обмежень щодо їх захисту); 2) технологічним (ситуації, коли (а) надмірна віддаленість сервера може призвести до зволікань із транспортуванням даних і критичних помилок у роботі програм і (б) один потужний дата-центр обслуговує значну кількість споживачів по всьому світу[41])[42].

Красномовним підтвердженням недостатньої надійності сучасних «хмар» для розміщення і зберігання приватних даних є обережне ставлення до них самих розробників. За даними дослідження, здійсненого компанією *Lieberman Software*, понад половину (51 %) *IT*-спеціалістів, безпосередньо причетних до розроблення та обслуговування «хмарових» сервісів, відмовляються зберігати в них свої особисті дані, а 86 % – критично важливу корпоративну інформацію[43]. У листопаді 2012 р. компанія провела опитування учасників світового конгресу *Cloud Security Alliance* (*CSA*), за підсумками якого з'ясувалося, що 88 % з них вважають небезпечним зберігання даних у «хмарі» через високий ризик їх втрати та/або викрадення[44].

Зважаючи на деякі відомості, свою роль тут відіграє певна парадоксальність сприйняття масовим інтернет-користувачем плюсів та мінусів «хмарових» технологій. Так, згідно з дослідженням, проведеним у середині 2012 р. в США та Канаді компанією *CA Technologies*, у 2013 р. понад половина американських організацій планує використовувати «хмарові» сервіси для реалізації своїх бізнес-стратегій. Основний відсоток опитаних, які використовують для цього приватні «хмари» (84 %), і більшість тих, хто послуговується сервісами публічними (73 %), переконані, що саме ці технології достатньо надійно

---

[41] Тут доречно згадати про випадок, коли ураган «Сенді» у 2012 р. пошкодив декілька «хмарових» дата-центрів у Нью-Йорку, що призвело до «падіння» численних веб-ресурсів у різних кінцях світу.

[42] *Firms* Run Data Protection Risk by Not Checking Where Information is Held in the Cloud [Електронний ресурс]. – Режим доступу: http://www.icomm.co.uk/Thought-Leadership/Press-Releases/Firms-Run-Data-Protection-Risk.aspx; *Облачные* провайдеры прячут данные от заказчиков [Електронний ресурс]. – Режим доступу: http://www.cnews.ru/news/top/index.shtml?2012/11/21/510449

[43] *IT-специалисты* не спешат доверить свои данные «облаку» [Електронний ресурс]. – Режим доступу: http://hitech.newsru.com/article/14dec2012/cloudrisk

[44] *Lieberman* Software: *IT*-специалисты не доверяют облачным сервисам [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/435160.php

захищають їхні дані. При цьому всі без винятку респонденти заявили, що стикалися з втратою та/або витоком корпоративних й особистих даних і в 76 % випадків це було пов'язано з відмовою *IT*-систем (у більшості випадків тих самих «хмарових» сервісів)[45]. Більшість учасників (91 %) згаданого світового конгресу *Cloud Security Alliance*, критикуючи «хмарові» сервіси, все ж визнали, що на сьогодні вони є одним із найбільш ефективних, зручних та економних бізнес-рішень[46].

Загалом нині весь комплекс проблем, пов'язаних із дотриманням безпеки персональних даних у «хмарах», можна умовно поділити на дві групи:

• *системні*, тобто такі, що випливають із самої архітектури «хмари» як техніко-технологічного рішення. Невирішеними залишаються питання щодо: а) **безпеки** ПД як такої, тобто принципової здатності сервісів гарантувати зберігання та оброблення даних згідно із законом; б) фізичного **розміщення** ПД та їх **транскордонної передачі**, оскільки утримання дата-центру в будь-якій вигідній провайдеру точці Землі повністю відповідає самій ідеї «хмари», але може бути небезпечним для користувача (див. вище); в) **доступу** користувача до своїх ПД, оскільки об'єктивно не він контролює цей доступ;

• *ситуативні*, тобто зумовлені поточними обставинами (фінансовим та економічним становищем, кон'юнктурою ринків, недосконалістю законодавств, стихійними лихами, доступом до обладнання тощо). З наведених фактів видно, що в умовах формування ринку і бурхливого зростання «хмарової» індустрії значна кількість «гравців» (через свідому недоброчесність або з інших причин) не забезпечують достатнього рівня захищеності споживачів та їх ПД. Ці проблеми здебільшого не мають системного характеру, і можна очікувати, що з подальшим розвитком *IT* і встановленням єдиних «правил гри» на відповідному ринку вони значною мірою будуть розв'язані.

Проте незаперечні та значущі переваги «хмар» навіть при недостатньому рівні їх безпеки стають нині вирішальним чинником швидкого зростання їх популярності і роблять їх актуальним трендом глобального розвитку *IT*. Власне, над розвитком та оптимізацією «хмарових» технологій інтенсивно працюють найкращі фахівці глобальної *IT*-індустрії. Також постійно вдосконалюються системи захисту «хмар», проте з викладеного зрозуміло, що **на цей час, застосовуючи «хмарову» модель зберігання та оброблення інформації, все ж досить проблематично гарантувати особі (а) постійний і стабільний доступ до її персональних даних, (б) недоторканність цих даних, (в) контроль за**

[45] *U.S. Companies* View Cloud Computing as Key to Improved Data Protection [Електронний ресурс]. – Режим доступу: http://investor.ca.com/releasedetail.cfm?releaseid=674043

[46] Там само.

їх обробленням, (г) точні відомості про їх місцезнаходження. Іншими словами, проблематично гарантувати його фундаментальне право на «прайвесі».

Завершуючи цей огляд основних загроз недоторканності приватного життя людини в кіберпросторі, доречно хоча б коротко згадати про ще одну небезпеку, яка поки що не є цілком очевидною, проте може стати актуальною у найближчому майбутньому. В умовах швидко прогресуючої «інтернетизації» технічних засобів та інфраструктур (насамперед побутових) дедалі важливішим джерелом пов'язаної з особою інформації стають **віртуальні пошукові машини, що працюють з т.зв. тіньовим інтернетом** – веб-адресами серверів, веб-камер, принтерів, роутерів та іншої підключеної до мережі *IT*-периферії, а також світлофорів, камер безпеки, домашніх систем автоматизації та опалення[47]. Усі ці відомості також можуть групуватися навколо «віртуального образу особи», у контексті інших даних надаючи додаткові подробиці про її приватне життя.

Підкреслимо, що саме завдяки тому, що описані проблеми дотримання безпеки ПД стосуються кіберпростору, у найближчому майбутньому вони й стануть ключовими і першочерговими у справі захисту. Справді, зважаючи хоча б на такі факти, що (а) існування і подальший розвиток всіх основних інфраструктур та видів діяльності людства уже майже неможливі без інтернету, (б) зараз понад третина населення Землі користується інтернетом, а у 2015 р., за прогнозами, ним користуватиметься половина людства і (в) більшість користувачів буде спілкуватися в соціальних та інших комунікативних веб-сервісах, причому здебільшого з мобільних пристроїв, можна говорити про те, що **на цю мить у мережі інтернет обертається та обробляється основний масив персональних даних населення Землі. При цьому спостерігається різке збільшення і стале зростання обсягів цього масиву**.

Безумовно, у цій ситуації для потенційних зловмисників постає питання пошуку й оброблення потрібної інформації, і нерідко це стає значною проблемою, оскільки може йтися про буквально астрономічні обсяги різноманітних, довільно структурованих і часто «нечитабельних» даних. Проте апаратна продуктивність і сучасне програмне забезпечення зазвичай дозволяють вирішити цю проблему.

Сьогодні вже існують ***IT*-платформи глибокого датамайнінгу**[48], орієнтовані якраз на тонке «просіювання» великих невпорядкованих

[47] Однією з таких пошукових систем є, наприклад, *Shodan* (http://www.shodanhq.com/). Див.: *Shodan* – самый страшный поисковик Интернета [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/post/178501/

[48] Датамайнінг (*Data Mining*) – термін приблизно можна перекласти на українську як «видобуток даних», «глибинний аналіз даних», «інтелектуальний пошук даних».

масивів даних та/або на паралельне оброблення всіх доступних баз даних для знаходження та аналізу пов'язаних між собою (в контексті відповідного запиту оператора платформи) фрагментів інформації. У цих надпотужних системах застосовуються алгоритми та методи аналізу, базовані на апроксимованій моделі людського мислення, що дає змогу їм адекватно та гнучко реагувати на семантично складні запити і їх динамічні зміни. Яскравим прикладом таких апаратно-програмних рішень є продукція американської фірми *Palantir*, серед замовників якої – ЦРУ, ФБР, Міністерство оборони США, аналітичні служби американської армії, морської піхоти і військово-повітряних сил, а також низка фінансових інститутів[49]. Нині подібні системи є одиничними і досить дорогими, але це жодним чином не означає, що закладені в них інноваційні технології залишаться без перспектив подальшого розвитку і поширення. Вся історія розвитку сучасної *IT*-індустрії свідчить, що, найшвидше, буде навпаки. Поява ж таких технологій у загальному доступі означатиме формування низки нових загроз для безпеки персональних даних[50].

Загалом, **дедалі ширша прірва між безпрецедентними «шпигунськими» можливостями сучасних онлайн-сервісів та *IT* і традиційними, «доцифровими» юридичними практиками, базованими на традиційному уявленні про межі й засоби забезпечення «прайвесі»**, є, мабуть, найбільш складним випробуванням для сучасної демократії. У Мадридській декларації про захист особистих даних «Глобальні стандарти по захисту особистих даних для глобального світу» від 3 листопада 2009 р. прямо визнається, що законодавство у сфері захисту ПД, а також інститути, які цим опікуються, сьогодні вже не в змозі повною мірою враховувати нові методи спостереження, включаючи «поведінковий таргетинг», бази даних ДНК й інших біометричних показників, об'єднання даних державного і приватних секторів, а також особливі ризики, до яких схильні вразливі групи населення (діти, мігранти, представники меншин)[51].

Однак будь-яка дієва демократія – це завжди баланс інтересів. І знаходження такого балансу задля **забезпечення інформаційних прав особи є досить складним завданням навіть у фізичному (невір-**

---

[49] *Palantir*, или Говорящие камни на службе ЦРУ / 3D news [Електронний ресурс]. – Режим доступу: http://www.3dnews.ru/621533

[50] У цьому контексті показовим є приклад *Hadoop* – програмної платформи, що вільно поширюється в мережі і призначена для організації розподіленого оброблення великих обсягів даних (Див.: http://hadoop.apache.org/; http://developer.yahoo.com/hadoop/)

[51] *Мадридская* декларация о защите личных данных «Глобальные стандарты по защите личных данных для глобального мира». – 2009. – 3 ноября [Електронний ресурс]. – Режим доступу: http://online.zakon.kz/Document/?doc_id=31067849721260

туальному) середовищі: тут треба досягти певної динамічної рівноваги між фундаментальними правами людини (де поєднуються право на доступ до інформації, право на свободу слова і право на «прайвесі»), національними інтересами, вимогами міжнародного права. Проте з викладеного вище очевидно, що **ця складність зростає на порядки і набуває нового сенсу та якості в кіберпросторі. Якщо найближчим часом не буде знайдено ефективного і при цьому демократичного рішення проблеми захисту персональних даних у веб-середовищі, в перспективі це може призвести до непередбачуваних і небезпечних переосмислень загальноприйнятих уявлень про приватність, її сенс та межі, а отже, до перегляду правового змісту самого поняття «персональні дані»**.

На цей час світ загалом і Європейське співтовариство зокрема перебувають у пошуку ефективних рішень цієї проблеми.

РОЗДІЛ ІІ.
ЄВРОПЕЙСЬКИЙ ДОСВІД ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У КІБЕРПРОСТОРІ

1. Правове регулювання

Традиційно законодавство країн ЄС та право ЄС не передбачають спеціальних нормативних механізмів регулювання захисту ПД у кіберпросторі. На це середовище поширюються загальні принципи та вимоги, передбачені законодавством про захист персональних даних, але з урахуванням специфіки оброблення ПД з використанням інформаційно-комунікаційних систем. Для оперативного реагування на нові виклики досить широко використовуються інструменти «непрямого права» (*soft law*): рекомендації, стратегії, меморандуми, «точки зору» (*opinions*) авторитетних експертних чи політичних організацій щодо нових об'єктів регулювання тощо.

Європейське право включає майже два десятки загальноєвропейських конвенцій, директив та рекомендацій з питань захисту персональних даних, хоча кожна країна ЄС має також свої базові нормативно-законодавчі акти, локальні закони щодо оброблення персональних даних у медичній, статистичній, державній, журналістській, поліцейській та інших сферах. При цьому існує низка міждержавних актів, обов'язкових для всіх країн-членів ЄС та/чи Ради Європи. Основними з них є:

• Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних;

• Додатковий протокол до Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних 2001 р.;

• Директива 95/46/ЄС Європейського парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» (принципи Директиви підтримано Україною);

• Постанова Ради ЄС 2008/977/*JHA* «Про захист персональних даних в рамках поліцейського та судового співробітництва у кримінальних справах»*;

• Регламент Європейського парламенту та Ради № 45/2001 щодо захисту осіб у зв'язку з обробленням персональних даних інституціями та органами спільноти та про вільне переміщення таких даних**;

• Директива 2002/58/ЄС Європейського парламенту та Ради ЄС щодо оброблення персональних даних і захисту приватності у секторі електронних засобів зв'язку***;

• Директива 2009/136/ЄС Європейського парламенту та Ради ЄС, яка доповнює Директиву 2002/22/ЄС про універсальну послугу та права користувачів стосовно мереж та послуг електронних комунікацій»****, Директиву 2002/58/ЄС Європейського парламенту та Ради ЄС і Регламент № 2006/2004 Європейського парламенту та Ради про співробітництво між національними органами влади, відповідальними за використання положень у сфері захисту прав споживачів.

Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р. (Конвенція № 108) – перший обов'язковий для виконання і відкритий для підписання міжнародний документ, що був спрямований не лише на захист фізичних осіб від зловживань, пов'язаних з обробленням даних, а й на регулювання транскордонної передачі ПД.

По суті, Конвенція встановлює певний баланс між свободою переміщення даних і захистом/забороною на їх оброблення в разі незабезпечення належних гарантій їх нерозголошення національним законодавством країни-отримувача даних. Документом спеціально обумовлені права суб'єкта ПД, встановлено обмеження оброблення «чутливих» даних стосовно расової належності, релігійних і політичних поглядів, сексуального життя.

---

* Неофіційний переклад.
** Неофіційний переклад.
*** Неофіційний переклад.
**** Неофіційний переклад.

Основна мета *Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних* (*ETS* № 181) – вдосконалити застосування принципів, що містяться в Конвенції, у спосіб впровадження двох нових діючих положень: про створення одного чи більше органів нагляду кожною Стороною та про транскордонне переміщення персональних даних у країни або організації, яка не є Стороною Конвенції.

Додатковий протокол до Конвенції № 108 супроводжується пояснювальним звітом (від 23 травня 2001 р.), який не є інструментом для офіційної інтерпретації Протоколу, втім, може мати такий характер для сприяння застосуванню положень Протоколу. Протокол відкрито для підпису в Страсбурзі 8 листопада 2001 р.

Стаття 1 Протоколу продовжує термін дії органів нагляду, визначених ст. 13 Конвенції № 108, які відповідають за забезпечення дотримання положень національного законодавства, що втілюють принципи, викладені в Конвенції та Протоколі.

Стаття 2 передбачає, що передача персональних даних користувачам, які підпадають під юрисдикцію держави або організації, яка не є Стороною Конвенції, може відбуватися за умови, що ця держава або організація забезпечить адекватний рівень захисту відповідної передачі даних. Відхилення від цього положення дозволяється при передачі даних у разі: (а) якщо внутрішньодержавне право забезпечує це у зв'язку зі специфічними інтересами суб'єкта даних або перевагою законних інтересів, зокрема важливих суспільних інтересів; (б) якщо гарантії, що, зокрема, можуть випливати з договірних положень, надаються контролером, відповідальним за передачу, та визнаються як достатні компетентними органами відповідно до внутрішньодержавного права.

Директива 95/46/ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 р. розвиває, уточнює і подекуди посилює принципи, закладені в Конвенції № 108.

Директива була прийнята на основі статті 100а Договору про Європейський Союз (на сьогодні, після внесення поправок, – ст. 95 ЄС) з метою сприяння вільному переміщенню персональних даних у спосіб гармонізації законодавчих актів, розпоряджень та адміністративних положень держав-членів стосовно захисту окремих осіб при обробленні таких даних.

Директива стосується захисту основних прав і свобод у внутрішньодержавних законодавствах щодо оброблення персональних даних, передусім права на приватне життя, яке визнається ст. 8 Європейської конвенції про захист прав людини та основоположних свобод та загальними принципами законодавства Європейського Співтовариства. Директива також уточнює принципи, викладені в Конвенції № 108.

Уточнює положення Директиви 95/46/ЄС в телекомунікаційному секторі Директива 97/66/ЄС Європейського парламенту і Ради. Обидві Директиви стосуються оброблення персональних даних, включаючи переміщення даних щодо абонентів та користувачів мережею інтернет. Статті 6, 7, 13, пункти 1 і 2 ст. 17 Директиви 95/46/ЄС та ст.ст. 4, 5, 6 та 14 Директиви 97/66/ЄС стосуються законності такого оброблення телекомунікаційними операторами та постачальниками послуг. Ці положення дозволяють операторам і постачальникам послуг обробляти ПД за досить обмеженими умовами. Пункт 1 ст. 6 передбачає, що персональні дані можуть збиратися лише для встановлених, чітких і законних цілей і надалі не можуть оброблятися у спосіб, несумісний з цими цілями, а також що персональні дані можуть зберігатися у формі, що дозволяє встановлювати особу суб'єктів даних, не довше, ніж це необхідно для цілей, заради яких дані були зібрані чи заради яких вони надалі обробляються. Стаття 5 гарантує конфіденційність передачі даних через державні телекомунікаційні мережі. Держави-члени повинні ввести заборону на прослуховування, запис, зберігання та інші види перехоплення даних іншими (крім користувачів) особами без згоди користувача цих даних, за винятком випадків, визначених відповідно до пункту 1 ст. 14. Існує загальне правило, згідно з яким дані, що передаються телекомунікаційними каналами, мають бути стерті або перетворюватися на анонімні після закінчення їх передачі (пункт 1 ст. 6 Директиви 97/66/ЄС). Національні правила стосовно того, скільки мають зберігатися дані, варіюють від 14 днів (у Норвегії) до 18 місяців (у Сполученому Королівстві)[52].

Директива Європейського парламенту та Ради Європейського Союзу 2002/58/ЄС щодо оброблення персональних даних і захисту конфіденційності у сфері електронних засобів зв'язку від 12 липня 2002 р. (у редакції Директиви 2006/24/ЄС Європейського парламенту і Ради від 15 березня 2006 р., Директиви 2009/136/ЄС Європейського парламенту і Ради від 25 листопада 2009 р.) забезпечує гармонізацію національних положень, необхідних для гарантування відповідного рівня захисту основних прав і свобод і, зокрема, права на приватне життя і конфіденційність інформації про приватне життя у зв'язку з обробленням персональних даних у сфері електронних комунікацій, а також для забезпечення вільного переміщення таких даних, пересування устаткування для електронного зв'язку і послуг електронного зв'язку у Спільноті. Документ репрезентує третє покоління законодавства

[52] *Додатковий* протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних (ETS № 181) [Електронний ресурс]. – Режим доступу: http://pidruchniki.ws/13331222/pravo/dodatkoviy_protokol_konventsiyi_pro_zahist_osib_zvyazku_avtomatizovanoyu_obrobkoyu_personalnih_danih

про персональні дані, спрямоване на забезпечення права самовизначення людини при автоматизованому обробленні його персональних даних в умовах прогресуючої відкритості та універсальності онлайнкомунікацій. Як один із засобів захисту ПД у такому середовищі пропонується мінімізація їх кількості в призначених для користувача мережах і їх анонімність скрізь, де це можливо.

На рівні інституційного оформлення системи захисту ПД **значну увагу в європейському праві приділено організації органів державного нагляду за обробленням даних** (контролерів).

У зв'язку з цим Додатковий протокол до Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних закріплює таке.

1. Кожна Сторона передбачає один чи більше органів нагляду, відповідальних за забезпечення дотримання заходів, які передбачено її внутрішньодержавним правом і які втілюють принципи, викладені в главах II і III Конвенції (994_326) та в цьому Протоколі (пункт 1 ст. 1)

2. Для цього зазначений вище орган нагляду має, зокрема, повноваження стосовно розслідування та втручання, а також право брати участь у судовому розгляді або повідомляти компетентним судовим органам про порушення положень внутрішньодержавного права, що втілюють принципи, викладені в пункті 1 статті 1 цього Протоколу (пункт 2a, ст. 1).

3. Кожний орган нагляду в межах своєї компетенції після розгляду приймає рішення у зв'язку із заявами будь-якої особи стосовно захисту її прав та основоположних свобод стосовно обробки персональних даних пункт 2b, ст. 1).

4. Органи нагляду виконують свої функції в повній незалежності (пункт 3, ст. 1)[53] .

Директивою 95/46/ЄС також передбачено вимоги щодо наглядових органів держав-членів ЄС, відповідальних за захист персональних даних на національному рівні. Зазначені вимоги розвивають положення Конвенції Ради Європи, зокрема:

1) «Кожна держава-член передбачає, що один чи більше державних органів відповідають за моніторинг застосування в межах її території положень, прийнятих державами-членами відповідно до даної Директиви.

Ці органи діють у повній незалежності при здійсненні функцій, якими вони наділені» (пункт 1, ст. 28);

---

[53] *Додатковий* протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_363

2. «Кожна держава-член передбачає, що при розробці адміністративних заходів чи положень, що стосуються захисту прав і свобод фізичних осіб при обробці персональних даних, проводяться консультації з наглядовими органами.

Кожен орган, зокрема, наділений:

– такими слідчими повноваженнями, як право доступу до даних, що є предметом операцій із обробки, і право збирати всю інформацію, необхідну для виконання його обов'язків із здійснення нагляду;

– ефективними повноваженнями на втручання, як-от надання висновків до здійснення операцій із обробки відповідно до статті 20 і забезпечення відповідного опублікування таких висновків, видання розпоряджень про блокування, стирання чи знищення даних, накладення тимчасової чи остаточної заборони на обробку даних, попередження чи винесення догани контролеру, або повноваження звертатися до національних парламентів чи інших політичних інститутів;

– право брати участь у судочинстві, якщо були порушені національні положення, прийняті відповідно до даної Директиви, чи довести ці порушення до відома судових органів.

Рішення наглядового органу, що викликали скарги, можуть бути оскаржені в суді» (пункт 2, ст. 28);

3) «Кожен наглядовий орган розглядає запити, зроблені будь-якою особою чи об'єднанням, що представляє інтереси цієї особи, про захист її прав і свобод при обробці персональних даних. Особа, якої це стосується, повинна бути поінформована про результати розгляду запиту.

Кожен наглядовий орган, зокрема, розглядає запити про перевірки законності обробки даних, зроблені будь-якою особою, у випадках, коли застосовуються національні положення, прийняті у відповідності до статті 13 даної Директиви. Така особа повинна в будь-якому випадку бути поінформована про те, що перевірка мала місце» (пункт 4, ст. 28);

4) «Кожен наглядовий орган регулярно складає звіт про свою діяльність. Звіт повинен оприлюднюватись» (пункт 5, ст. 28);

5) «Кожен наглядовий орган має право, незалежно від того, яке національне законодавство застосовується до відповідної обробки, виконувати на території власної держави-члена повноваження, якими він наділений відповідно до пункту 3. Кожен орган може отримати прохання про виконання його повноважень від органу іншої держави-члена.

Наглядові органи співпрацюють один з одним у тій мірі, наскільки це необхідно для виконання їхніх обов'язків, зокрема, шляхом обміну всією корисною інформацією» (пункт 6, ст. 28);

6) «Держави-члени передбачають, що навіть після звільнення на посадових осіб і персонал наглядового органу поширюється обов'язок

зберігати професійну таємницю відносно конфіденційної інформації, до якої вони мають доступ» (пункт 7, ст. 28)[54].

Загалом усі ці норми спрямовані на досягнення двоєдиної мети: **максимальна незалежність національного контролера захисту та оброблення ПД від політичних, адміністративних, фінансових впливів при збереженні максимальної прозорості діяльності та звітності перед суспільством**.

Разом з цим саме керівництво ЄС визнає, що в частині регулювання захисту персональних даних у віртуальному середовищі **класичне законодавство Євросоюзу є застарілим і малоефективним**. При цьому в кожній державі ЄС є і своє національне законодавство про захист персональних даних, і свій контролюючий орган. У сучасних умовах це, швидше, перешкоджає гармонізації відносин у сфері.

За офіційно оприлюдненими даними спеціального дослідження Єврокомісії в країнах ЄС, 74 % європейців сприймають дедалі меншу захищеність персональної інформації як характерну ознаку сучасності, причому пов'язують це передусім з участю у соціальних мережах (61 %) та з онлайн-шопінгом (79 %)[55]; 72 % опитаних стурбовані обсягом персональної інформації, викладеної в інтернет, і відсутністю повноти контролю над власними даними[56]. Характерно, що при цьому понад половина опитаних (54 %) знайомляться з оголошеними на онлайн-сервісах умовами збору та подальшого використання наданих ними даних[57].

Нині ведеться інтенсивна робота з модернізації відповідної правової бази. 25 січня 2013 року було опубліковано пропозиції Єврокомісії щодо реформування законодавства про захист персональних даних у Європі – єдині для всіх країн ЄС **Стандарти захисту персональних даних Євросоюзу (*European Data Protection Regulation*)**[58], які мають

---

[54] Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_242

[55] *How will the data* protection reform affect social networks? [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf

[56] *Why* do we need an EU data protection reform? [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

[57] *How will the data* protection reform affect social networks? [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf

[58] *Commission* proposes a comprehensive reform of the data protection rules [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

замінити Директиву 95/46/ЄС та визначити основні вимоги законодавства ЄС у сфері захисту персональних даних. В основу проекту було покладено результати широких консультацій з громадськістю, національними органами захисту персональних даних, Європейським контролером з питань захисту персональних даних та іншими агенціями ЄС.

Стандарти спрямовані передусім на гармонізацію режиму захисту ПД в Європі і надання споживачам можливості контролювати, яким чином їхні персональні дані обробляються компаніями. Особливий *акцент у Стандартах робиться на наданні громадянам більшого обсягу можливостей контролю їх ПД і на питаннях використання інтернету дітьми*. Пропонується, наприклад, встановити, що доступ до веб-сайтів, реєстрація на них, а також отримання розсилок цільового маркетингу особами молодшими від 18 років може здійснюватися тільки зі згоди їхніх батьків[59].

У Стандартах передбачено низку заходів щодо спрощення процедур захисту персональних даних та послаблення бюрократичного тиску на здійснення таких процедур:

• створюються єдині правила із захисту персональних даних, дійсні в усьому ЄС. Виключаються зайві адміністративні вимоги, такі як відправлення компаніями-операторами персональних даних повідомлень про оброблення персональних даних у контролюючі органи;

• знижуються вимоги щодо повідомлення операторами персональних даних контролюючих органів про вжиті заходи із захисту персональних даних;

• встановлюється час, що дорівнює 24 год., впродовж якого оператору персональних даних бажано повідомити національний контролюючий орган про інциденти з даними;

• оператори персональних даних матимуть справу тільки з одним національним контролюючим профільним органом. Крім того, громадяни можуть звернутися в такий орган у країні свого перебування, навіть якщо їхні дані обробляє компанія, що базується поза межами ЄС або в інших країнах ЄС;

• для використання і передачі персональних даних третім особам операторам персональних даних буде необхідно отримати однозначну згоду громадян на здійснення таких операцій з персональними даними.

---

[59] Показово, що основною причиною даної ініціативи представники Європейської Комісії назвали систематичні інциденти та судові процеси між державами, що входять до ЄС, і великими компаніями, які реалізують свої сервіси в мережі інтернет. Наприклад, скандал, пов'язаний із сервісом *Google Street View*, проти діяльності якого з-поміж низки інших країн виступили Франція і Бельгія.

Стандарти передбачають також розширення прав осіб-суб'єктів персональних даних при одночасному посиленні контрольованості та відповідальності операторів ПД:

• гарантування вільного доступу до власних персональних даних у будь-яких базах даних;

• «право на вільне перенесення персональних даних». Згідно з новим законодавством громадяни повинні отримати спрощену процедуру передачі своїх персональних даних від одного постачальника послуг до іншого (мобільність даних). Передбачається, що це підвищить конкуренцію між постачальниками послуг;

• «право бути забутим», тобто спрощення для громадян процедур знищення своїх персональних даних у базах даних із забороною подальшого використання, якщо немає законних підстав для їх збереження;

• «право на добровільне і відкрите волевиявлення володільця персональних даних» щодо певних типів їх оброблення;

• розширення повноважень національних контролюючих органів із захисту персональних даних. Зокрема, передбачено посилення дисциплінарних заходів щодо компаній, які порушують відповідні правила ЄС. Так, недобросовісному операторові персональних даних може бути виписане попередження за перше порушення, накладений штраф у розмірі від 250 тис. євро або 0,5 % від обороту за незначні порушення і штраф у розмірі до 1 млн євро або до 2 % від загальносвітового річного обігу компанії у разі завдання збитку суб'єктам персональних даних;

• запроваджуються загальні принципи і правила щодо захисту персональних даних задля оптимізації міждержавної співпраці поліції і правоохоронних органів, у т.ч. у кримінальних справах;

• нові правила ЄС мають прийматися також і нерезидентами ЄС, якщо вони активно працюють на ринку ЄС і надають свої послуги громадянам ЄС[60].

Передбачається, що стандарти буде введено в дію в найближчому майбутньому.

---

[60] *European* Commission. Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf; *How will the data* protection reform affect social networks? [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf; *Евросоюз* предлагает реформирование законодательства в сфере защиты персональных данных [Електронний ресурс]. – Режим доступу: http://club.cnews.ru/blogs/entry/import_evrosoyuz_predlagaet_reformirovanie_zakonodatelstva_v_sfere_zashchity_personalnyh_dannyh_0de4

У вересні 2012 р. Європейська Комісія виступила зі стратегічним документом **Вивільнення потенціалу хмарових обчислень в Європі** (*Unleashing the potential of cloud computing in Europe*)[61], спрямованим на прискорення імплементації та значне розширення використання «хмар» в економіці ЄС. Передбачається, що реалізація цих завдань забезпечить створення 2,5 млн робочих місць і отримання 160 млрд євро чистого прибутку щороку. Основними цілями Стратегії є:

• запровадження вже у 2013 р. єдиних технічних та інших стандартів задля забезпечення належної мобільності, функціональної сумісності й оборотності даних;

• співробітництво з достойними довіри провайдерами «хмарових» послуг у масштабах ЄС;

• розвиток та підтримання моделі «безпечно і справедливо» (*safe and fair*) при укладенні угод на ринку «хмарових» послуг;

• запровадження спеціального інституту – Європейського «хмарового» партнерства (*European Cloud Partnership, ECP*) – за участю країн-членів та представників індустрії задля залучення потенціалу приватного сектору, оформлення європейського галузевого ринку, стимулювання європейських провайдерів з метою підвищення їх конкурентоспроможності і запровадження оптимальної системи *e*-урядування[62].

Спеціальну увагу у Стратегії приділено питанням безпеки користувачів і, зокрема, захисту персональних даних. Як розробник документа Європейська Комісія офіційно оголосила, що:

• сьогодні саме проблеми захисту персональних даних на ринку «хмарових послуг» є найбільш серйозним бар'єром для його подальшого розвитку;

• одним з головних завдань, заявлених у Стратегії, є розроблення особливої моделі «положень та умов» (*terms and conditions*) контрактів для сфер, які не регулюються Європейським Законом про купівлю та продаж (*Common European Sales Law*). До таких належить і весь комплекс питань, пов'язаних із захистом персональних даних. Розроблення адекватних юридичних рішень у цій сфері розглядається як «шлях до широкої популярності «хмарових» сервісів завдяки зростанню довіри користувачів»;

• положення та завдання Стратегії «дбайливо узгоджені» із Стандартами захисту персональних даних Євросоюзу. Заявлено, що в

---

[61] *Unleashing* the Potential of Cloud Computing in Europe // European Commission. – Brussels. – 2012. – 27 October – COM(2012) 529 final [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf

[62] *Digital* Agenda: New strategy to drive European business and government productivity via cloud computing [Електронний ресурс]. – Режим доступу: http://europa.eu/rapid/press-release_IP-12-1025_en.htm?locale=en

Стандартах закладений «добрий загальний базис» для майбутнього розвитку європейського ринку «хмарових» послуг. У зв'язку з цим констатується важливість ухвалення цього документа Радою Міністрів ЄС та Європейським парламентом вже у 2013 р.[63]

У перспективі Європейська Комісія планує за участі *ENISA (European Union Agency for Network and Information Security)*, та інших профільних організацій підтримувати постійні діалоги та консультації на міжнародних майданчиках, проводити дослідження задля відпрацювання оптимальних механізмів безпечного та ефективного використання «хмарових» технологій[64].

В основу зазначених пропозицій було покладено результати широких консультацій із громадськістю, національними органами захисту персональних даних, Європейським контролером з питань захисту персональних даних та іншими агенціями ЄС.

Основними напрямами ініційованої ЄК реформи законодавства ЄС щодо захисту персональних даних у кіберпросторі є такі:

- забезпечення прав осіб на захист персональних даних;
- економічний вимір захисту персональних даних;
- захист персональних даних у діяльності правоохоронних органів;
- міжнародний вимір захисту персональних даних.

Наведені законодавчі пропозиції Європейської Комісії викликали значний резонанс у пресі та у середовищі європейських політиків, лунають думки про надмірність, навіть нездійсненність запропонованих заходів.

Нині **ці законодавчі пропозиції оцінюються як найбільш складні проекти, які коли-небудь опрацьовувалися Європейським парламентом – євродепутатами було запропоновано близько 4 тис. поправок і пропозицій**. З-поміж держав-членів ЄС відсутня одностайність не тільки щодо остаточного тексту, а й щодо форми та правового статусу майбутніх законодавчих актів (зокрема, чи матимуть вони форму регламентів, які містять норми прямої дії, чи директив, які передбачають лише напрями та цілі, проте імплементацію залишають на розсуд національних урядів). Окремі експерти, наближені до переговорного процесу, навіть побоюються, що остаточні тексти міститимуть нижчі, ніж у чинних документах, стандарти захисту персональних даних[65].

Попри це, один з ініціаторів даних ініціатив – Єврокомісар з питань юстиції Вівіан Редінг (*Viviane Reding*) – незмінно наполягає на

---

[63] *Unleashing* the Potential of Cloud Computing in Europe – What is it and what does it mean for me? [Електронний ресурс]. – Режим доступу: http://www.abbl.lu/sites/abbl.lu/files/FAQ_Cloud_Computing.pdf

[64] Там само.

[65] *Щодо* актуальних питань захисту персональних даних : лист від 11.06.2013 р., вх. № 3111/16-600-1513 / Представництво України при Європейському Союзі.

необхідності їх якнайшвидшого прийняття та імплементації у законодавство ЄС. У вересні 2013 р. вона закликала завершити цей процес до травня 2014 р., тобто до чергових виборів до Європейського Парламенту[66].

Але в будь-якому разі немає сумніву, що **ці дискусії і робота в євроінституціях визначать передові світові стандарти захисту персональних даних**. Водночас, зважаючи на наявні контраверсійні позиції, **питання остаточної транспозиції нових європейських підходів у національне законодавство України доцільно було б опрацювати після завершення зазначених дискусій**.

2. Техніко-технологічні рішення

Неоднорідність кіберпростору як віртуального і технологічного середовища дає змогу умовно виділити в його межах кілька зон, що відрізняються за критеріями: а) особливостей оброблення/збереження ПД; б) режиму доступу до ПД третьої сторони. Такими зонами є:

1) *автоматизована* – рівень мережевого протоколу і локатора вебресурсів *URL*, куди дані про комп'ютер, місцезнаходження та історію відвідувань користувача потрапляють «за замовчуванням», що зумовлено суто технічними потребами роботи мережі;

2) *відкрита,* де особа добровільно розміщує в публічному доступі свої дані (сайти, блоги, чати);

3) *частково відкрита* – передусім комунікативні сервіси (*e-mail*, соціальні мережі, *Skype*, *ICQ*), де особа сама обирає режим доступу третьої сторони до своїх ПД;

4) *закрита* – локальні сховища підключених до інтернету персональних пристроїв користувача, до контенту яких технічно можливим є несанкціонований доступ (ПК, планшет, мобільний телефон тощо).

Зазвичай захист персональних даних у третій та четвертій зонах інтернет-середовища регулюється узгодженими між собою міжнародними правовими актами та законодавствами держав, де перебувають суб'єкт, володілець і розпорядник ПД. В ідеалі такого адміністративно-правового регулювання має бути достатньо для забезпечення повноцінного і повсюдного захисту персональних даних. У фізичному середовищі, можливо, так воно і є, але у віртуальному для того, щоб досягти хоча б базового рівня захисту ПД (контроль їх місцезнаходження, транзиту, режиму доступності тощо), необхідні додаткові суто технічні інструменти.

---

[66] *Єврокомісар* закликала Євросоюз ввести загальні правила захисту даних [Електронний ресурс]. – Режим доступу: http://www.unian.ua/news/593894-evrokomisar-zaklikala-evrosoyuz-vvesti-zagalni-pravila-zahistu-danih-zmi.html

Як свідчить практика, найчастіше персональні дані з використанням веб-ресурсів обробляються (санкціоновано чи ні) під час таких цілком добровільних з боку користувачів процесів:

• заповнення відвідувачами веб-ресурсів анкет;

• реєстрація та отримання логіна та пароля;

• реєстрація з використанням облікового запису соціальної мережі;

• надання електронної адреси відвідувача для зворотного зв'язку.

При цьому можуть оброблятися ПД широкого діапазону: від анкетних, які явно є відомостями про особу, яка ідентифікована, до відомостей, які можуть стосуватися особи опосередковано або які можуть використовуватися в процесі ідентифікації особи (інформація про оплату послуг із використанням платіжних карт, логіни та паролі, записи в соціальній мережі, номери телефонів, електронні адреси тощо).

Разом з тим існує дуже широкий спектр **прихованих способів онлайн-доступу до персональних даних**, які користувач під час онлайн-сесії просто не в змозі зафіксувати, а отже, проконтролювати – від класичного надсилання на пристрій *cookies* до використання для доступу нібито цілком респектабельних ліцензійних програм, або «підселення» у пристрій спеціальних вірусів, ім'я яким – легіон.

Протиборство тих, хто бажає отримати доступ до чужих даних, з тими, хто не бажає ними ділитися і взагалі воліє зберігати анонімність в он-лайні, ніколи не припиняється. І хоча прийнято вважати, що в цій «гонці озброєнь» хакери завжди будуть на крок попереду, уже давно утворилося і продовжує поповнюватися не менш репрезентативне, ефективне та різноманітне **сімейство *PET(s)* – «технологій захисту приватності»** (приблизний переклад на українську усталеної англійської назви *Privacy Enhancing Technologies, PET*). Грамотне і комплексне застосування цих технологій зазвичай дозволяє досягти безпечного перебування в режимі он-лайн[67]. Щоправда, це передбачає наявність у користувача таких спеціальних знань і кваліфікації, які просто відсутні в сучасного пересічного користувача мережі. Але в будь-якому разі використання *PETs* схвалено і навіть рекомендовано спеціальним меморандумом Європейської Комісії[68].

---

[67] Див., наприклад: *Способы* идентификации в интернете [Електронний ресурс]. – Режим доступу: http://javascript.ru/unsorted/id#primer; *Советы* по безопасной работе в интернете [Електронний ресурс]. – Режим доступу: http://www.windxp.com.ru/articles56.htm; *Защита* конфиденциальных данных и анонимность в интернете [Електронний ресурс]. – Режим доступу: http://clck.ru/8rWPJ; *Как* не оставлять следов в Сети [Електронний ресурс]. – Режим доступу: http://www.chip.ua/stati/kak-ne-ostavlyat-sledov-v-seti/

[68] *Privacy* Enhancing Technologies (PETs). The existing legal framework [Електронний ресурс]. – Режим доступу: http://europa.eu/rapid/press-release_MEMO-07-159_en.htm

Свою специфіку має дотримання безпеки даних у новітніх онлайн-середовищах, про які уже згадувалося. Зважаючи на тенденції та прогнози розвитку сучасної *IT*-сфери, на спеціальну увагу заслуговує питання підвищення безпеки даних у хмарових сервісах.

Як вже зазначалося, архітектура «хмарового» сервісу є значно лаконічнішим, продуктивнішим і дешевшим рішенням порівняно з мережами попереднього покоління.

По-перше, хмари дають змогу істотно знизити капітальні витрати на побудову центрів оброблення даних, закупівлю серверного та мережевого обладнання, апаратних і програмних рішень тощо. Левова частка цих видатків поглинається провайдером «хмарових» послуг[69]. Додатково клієнт економить на утриманні *IT*-персоналу, адмініструванні тощо.

По-друге, «хмарові» технології забезпечують можливість досить оперативно змінювати конфігурацію корпоративної *IT*-інфраструктури залежно від поточних потреб, споживаючи (і купуючи) стільки ресурсів, скільки потрібно на конкретний момент. Ресурсів «хмари» зазвичай цілком достатньо для замовлення віртуального «суперкомп'ютера» або інфраструктури для великої корпорації, і при цьому не виникає проблем з оновленням програмного забезпечення (завжди доступні його останні версії), сумісністю різних операційних систем тощо.

По-третє, «хмарові» сервіси надають можливість у буквальному розумінні носити своє робоче місце із собою: за наявності мобільного термінального пристрою і доступу до інтернету користувач незалежно від свого місцезнаходження завжди має доступ до власного віртуального комп'ютера, зконфігурованого у «хмарі», корпоративних мереж, баз даних тощо.

По-четверте, постійно розширюється спектр послуг, пропонованих виробниками та провайдерами «хмарових» рішень. Зазвичай їх «асортимент» цілком відповідає постійно зростаючим можливостям сучасної комп'ютерної техніки[70].

Усе це лише найсуттєвіші технологічні переваги «хмарових» сервісів, перелік яких можна продовжити. Понад те, виробникам і про-

---

[69] Наприклад, *De Novo*, один з великих українських «хмарових» провайдерів, гарантує скорочення витрат на *IT*-інфраструктуру до 50 % у разі користування їх сервісами (Див.: Облачные сервисы [Електронний ресурс]. – Режим доступу: http://www.de-novo.biz/arenda-servernoj-infrastruktury). Це досить типовий показник на сучасних галузевих ринках.

[70] Див., наприклад: *Решения* Fujitsu в области облачных вычислений [Електронний ресурс]. – Режим доступу: http://www.fujitsu.com/ua/cloud/; *Explore* SAP Products [Електронний ресурс]. – Режим доступу: http://www.sap.com/cis/solutions/technology/cloud/index.epx; *Symantec*. The Sign of a Safe Cloud [Електронний ресурс]. – Режим доступу: http://www.symantec.com/cloud-computing-software

вайдерам «хмар» вдалося сформувати досить гнучку та адекватну потребам сучасного ринку систему надання послуг[71].

У найбільш розвинених регіонах світу вже ухвалено стратегічні рішення та плани дій щодо системного та комплексного розвитку «хмарових» сервісів, розгорнуто відповідну роботу. У глобальному вимірі ринок «хмарових» обчислень стає полем дедалі жорсткішої конкуренції між провідними світовими *IT*-корпораціями (*Google*, *Yahoo*, *Amazon*, *Microsoft*, *Zoho*, *Cisco*, *Symantec*, *Fujitsu* та інші). Великі бізнес-гравці, які ще не мають своєї «частки» на цьому ринку, готуються завойовувати її в найближчому майбутньому. Така ситуація додатково інтенсифікує техніко-технологічну гонку, тому нові апаратні рішення, стартапи, програмне забезпечення розробляються і просуваються у «хмаровому» секторі справді випереджальними темпами.

Здійснюється активна робота з міжнародної стандартизації «хмарових» обчислень. У двох технічних підкомітетах Об'єднаного технічного комітету № 1 «Інформаційні технології» (*Joint Technical Committee* 1) Міжнародної організації зі стандартизації (*International Organization for Standardization, ISO*) триває робота над групою стандартів і технічних звітів стосовно «хмарових» технологій. Її результати передбачається оприлюднити наприкінці 2014 р.[72]

«Хмарові» технології вже зараз є одним із суттєвих чинників міжнародного розвитку, вплив якого найближчими роками значно зросте. Варто підкреслити, що цей глобальний тренд і проблеми, пов'язані з його розвитком, **є актуальними і для України**. За результатами опитування, проведеного у вересні 2012 р. партнерами компанії «Майкрософт Україна» – «Софтлайн-*IT*» та *Intecracy Group*, уже за рік «хмарові» технології використовуватимуть 30 % українських компаній. До 2015 р. частка таких компаній зросте в Україні до 40 % і більше[73].

---

[71] Див., зокрема: *Гнатюк С.* Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики : аналіт. зап. / С. Гнатюк [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1191/

[72] Див.: *Міжнародний* досвід: проводиться робота над групою стандартів, що стосуються хмарових обчислень [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/dszpd/uk/publish/article/53913;jsessionid=ABF5CECAF86F57E8E8E4B04651C56EDB; *ИСО*: Идет работа над группой стандартов, касающихся облачных вычислений [Електронний ресурс]. – Режим доступу: http://rusrim.blogspot.com/2013/03/blog-post_14.html; *ISO/IEC* CD 27040 Information technology – Security techniques – Storage security [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44404

[73] *Прогноз*: к 2015 году треть украинских компаний будут использовать облачные технологии [Електронний ресурс]. – Режим доступу: http://www.marrero.com.ua/oblachnye-tekhnologii/149-prognoz-k-2015-godu-tret-ukrainskikh-kompanij-budut-ispolzovat-oblachnye-tekhnologii

Разом з цим фундаментальним недоліком «хмарових» сервісів є високі ризики за їх використання (див. Розділ І). Це зумовлено як особливостями самої технології, так і тим фактом, що вона все ще недостатньо апробована для масового використання. Разом з тим в організації та архітектурі «хмарового» сервісу існують ланки, здатні стати потенційною основою потужної та ефективної системи захисту даних. Понад те, їх цілком можна розглядати як безпекові переваги порівняно з технологічним веб-середовищем попереднього покоління.

По-перше, в сучасних «хмарових» сервісах усі дані і трафік обов'язково шифруються (зазвичай з використанням протоколу *SSL – Secure Sockets Layer*). Отже, персонал «хмарових» дата-центрів, як і будь-які інші треті особи, не мають прямого доступу до персональних даних користувача – без введення унікального пароля вони є просто набором символів. До того ж споживачеві завжди доступний додатковий ступінь захисту – шифрування інформації за допомогою електронного цифрового підпису, що, крім пароля, передбачає введення особливого електронного ключа, розміщеного на фізичному носії – спеціальній флешці, яка є тільки в суб'єкта ПД. Усе це робить прямий несанкціонований доступ до даних користувача, розміщених у віддалених сховищах, досить проблематичним.

По-друге, професійному хакеру набагато простіше отримати доступ до інформації на локальному комп'ютері (наприклад, відправивши електронною поштою програму-троян), ніж намагатися «зламати» системи захисту «хмарового» дата-центру, де він, зокрема, зіткнеться з протидією фахівців – системних адміністраторів.

По-третє, на випадок втрати даних унаслідок надзвичайної ситуації у сучасних дата-центрах зазвичай робиться резервне копіювання інформації на інші сервери.

По-четверте, сьогодні на рівні глобальних *IT*-підприємств здійснюється постійна й масштабна робота з удосконалення апаратно-програмних комплексів захисту даних у «хмарах». Менеджер *Cisco* з маркетингу мережевих обчислень і віртуалізації Джеймс Уркхарт (*James Urquhart*) констатує: «Великі постачальники «хмарових» послуг, такі як *Amazon, CSC, HP, IBM, Salesforce.com, Verizon Business* та ін., створили потужні механізми безпеки. Вони працюють не лише на прикладному, а й на інфраструктурному рівні і включають до свого складу такі інфраструктурні засоби, як міжмережеві екрани і системи шифрування»[74]. Експерт *Cisco* твердить, що нині вже існують рішення для досить ефективного захисту будь-яких «хмарових» послуг.

---

[74] *CEBIT-2013*. Безопасность в «облаках» [Електронний ресурс]. – Режим доступу: http://www.softline.kiev.ua/ru/blog/blog-kompanii/cebit-2013/729-cebit-2013-bezopasnost-v-oblakakh.html

Довідково. *З-поміж сучасних високоефективних систем захисту даних можна назвати низку спеціалізованих апаратно-програмних рішень CloudSpan від компанії Layer 7 (CloudConnect, CloudProtect та CloudControl), а також JaxView for Cloud Management компанії Managed Methods. Такі компанії, як Altor Networks, Catbird Networks і Reflex Systems, також адаптували свої продукти для безпеки центрів оброблення даних до роботи у «хмаровому» середовищі, яке гарантує компаніям безпечне використання «хмарових» сервісів. Платформа Symantec O_3 Cloud Identity and Access Control створює єдину точку доступу до будь-яких «хмарових» рішень і сервісів, застосовуючи при цьому трирівневий захист: контроль доступу, інформаційну безпеку, управління інформацією*[75]*. Узагалі системи безпеки стають дедалі більш диверсифікованими й гнучкими. Так, архітектура Cisco для «хмарової» безпеки дозволяє організаціям задавати системі складні індивідуалізовані налаштування. У документах компанії наводиться приклад такого налаштування: «віце-президент з продажів має право на доступ до глобальних прогнозів продажів, але якщо він спробує отримати такі дані через смартфон з території країни ім'ярек за допомогою невідомого протоколу і при цьому двома годинами раніше він виходив у мережу з повною аутентифікацією з Каліфорнії, запит має бути відхилено»*[76]*. Цікаво, що нині й самі «хмарові» технології використовуються для створення надпотужних і надшвидкісних антивірусних мереж, наприклад розподіленої мережі Kaspersky Security Network*[77]*.*

Іншими словами, якщо основою підходу перших систем захисту даних у «хмарах» була ідея захисту корпоративних мереж за допомогою брандмауерів, то більшість сучасних рішень у цій сфері зорієнтовані передусім на захист точок доступу за рахунок поєднання міжмережевих екранів і засобів шифрування даних на рівні користувача. Як результат – яким би пристроєм не користувався абонент для доступу в «хмару», дані будуть захищені на всіх стадіях оброблення.

Усе щойно викладене – типовий набір аргументів, що зазвичай висувається виробниками й вендорами «хмарових» рішень на користь безпеки їх використання. Вони одностайно запевняють, що вже на такій фазі розвитку технології імовірність втрати персональних даних, розміщених у «хмарових» дата-центрах, набагато нижча, ніж у разі їх традиційного збереження на персональному комп'ютері.

У жодному разі немає сумнівів, що засоби захисту даних у «хмарах» швидко еволюціонують і вдосконалюються. Цей факт помітно підвищує рівень оптимізму поміж експертів. Наприклад, один з відо-

---

[75] *Symantec* создает новую систему безопасности для облаков [Електронний ресурс]. – Режим доступу: http://www.symantec.com/ru/ru/about/news/release/article.jsp?prid=20120314_01

[76] *Безопасность* в облаке [Електронний ресурс]. – Режим доступу: http://www.cisco.com/web/UA/about/news/2011/11152011b.html

[77] *Защита* из облака – что такое Kaspersky Security Network [Електронний ресурс]. – Режим доступу: http://blog.kaspersky.ru/ksn/

мих *IT*-фахівців, член наглядової ради консорціуму *Intecracy Group* Антон Марреро упевнений, що «новітні розробки у сфері безпеки «хмар» мають повністю розвіяти побоювання клієнтів». За словами експерта, сьогодні провідні постачальники «хмарових» послуг зберігають у себе на серверах петабайти конфіденційних даних, і за весь час не сталося жодної вагомої втрати/витоку даних[78]. З іншого боку, важко не погодитися і з Річардом Стинноном (*Richard Stiennon*), аналітиком компанії *GigaOM Pro* і засновником фірми *IT-Harvest*, що здійснює дослідження у сфері інформаційної безпеки: «Досі ми не бачили жодного серйозного «зламу» систем безпеки в хмарі, але рано чи пізно це обов'язково станеться. Це лише питання часу»[79].

Техніко-технологічна й інфраструктурна специфіка «хмар» зумовлює і специфічність ризиків, пов'язаних з їх використанням, – вони значно відрізняються від інформаційних небезпек, типових для систем попереднього покоління, і сьогодні є більш критичними. Але не варто забувати, що «хмарові» технології постійно та інтенсивно вдосконалюються, причому чи не найшвидше саме той їх сегмент, що пов'язаний із безпекою персональних і корпоративних даних.

Крім того, суттєво підвищити рівень захисту даних у «хмарі» можливо, ретельно дотримуючись, сказати б, певних «правил виробничої гігієни». Резюмуючи міркування експертів стосовно цього питання, можна виділити низку умов, необхідних для досягнення задовільного (хоча й не стовідсоткового) рівня безпеки сучасного «хмарового» сервісу для персональних даних користувача. Сьогодні це можливо за наявності таких обов'язкових складників:

• *апаратний (фізичний, хардверний) складник*: а) обладнання, на якому реалізована «хмарова» *IT*-інфраструктура, має розміщуватися в захищеному приміщенні, з клімат-контролем, безперебійним живленням, ефективним протипожежним захистом; б) має бути забезпечене цілодобове обслуговування усієї інфраструктури; в) необхідним є фізичне розділення ресурсів, наприклад, інфраструктура, в якій обробляються критично важливі та конфіденційні дані, фізично має розташовуватися окремо від загальної інфраструктури, посилена безпека якої не передбачається;

• *програмний (софтверний) складник*: а) повномасштабний антивірусний захист, особливо в разі користування такими сервісами, як *SaaS* (програмне забезпечення як послуга) і *PaaS* (платформа як послуга); б) наявність спеціальних налагоджених мережевих екранів (брандмауерів, фаєрволів) для віртуальних машин, а також для всіх

[78] *Защита* из облака – что такое *Kaspersky Security Network* [Електронний ресурс]. – Режим доступу: http://blog.kaspersky.ru/ksn/.

[79] *Безопасность* в облаке [Електронний ресурс]. – Режим доступу: http://www.cisco.com/web/UA/about/news/2011/11152011b.html

операційних систем, задіяних в інфраструктурі; в) захист систем і програм хоча б у частині найбільш уразливих місць; г) обов'язкове шифрування принаймні важливої і конфіденційної інформації, розташованої у «хмарі»;

• *адміністративно-нормативний складник*: а) пропускний режим у приміщеннях дата-центру (аж до біометричного контролю доступу), максимальна обмеженість, регламентування та облік доступу до інформації, що зберігається в спеціалізованих сховищах і базах даних; б) аутентифікація користувачів за логіном і паролем з обов'язковим шифруванням цього процесу; в) запровадження системи статусів користувачів з відповідною диверсифікацією прав і рівнів доступу до ресурсів інфраструктури; г) чітке дотримання провайдером норм чинного законодавства (для безпеки українського користувача насамперед Закону України «Про захист персональних даних»).

Як бачимо, дотримання безпеки даних «хмарового» сервісу вимагає від провайдера, крім високого рівня уваги, відповідальності та професіоналізму, ще й постійних додаткових зусиль. Але в сучасному кіберпросторі (немає значення, «хмаровий» це чи «традиційний» апаратно-провідний його сегмент) це твердження справедливе й щодо пересічного користувача – суб'єкта ПД. **У сучасному інтернеті ефективний захист власних персональних даних залежить від користувача не менше, ніж від національного контролера чи провайдера онлайн-послуг.** Для цього користувач також повинен бути відповідальним, уважним, мати певні спеціальні знання для грамотного використання та комбінування доступних йому інструментів дотримання безпеки, дотримуватись певної «гігієни» використання мережевих ресурсів тощо. Іншими словами, **йдеться про своєрідну культуру онлайн-безпеки користувача та необхідність її популяризації в глобальному масштабі**.

РОЗДІЛ ІІІ.
ТЕНДЕНЦІЇ ТА ПРОБЛЕМИ РОЗВИТКУ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

Стаття 32 *Конституції* України забороняє втручатися в особисте і сімейне життя людини, у т.ч. збирати, зберігати, використовувати та поширювати конфіденційну інформацію про особу без її згоди, крім випадків, передбачених Конституцією України та/чи визначених законом[80]. Разом з цим треба визнати, що як саме поняття «персональні

[80] *Конституція* України : закон від 28.06.1996 р. № 254к/96-ВР [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

дані», так і правові практики, пов'язані з їх захистом та обробленням, є відносно новими, а отже, малознайомими для українського суспільства. Системна робота над створенням національних наглядових інституцій та законодавства у сфері захисту ПД започаткована в Україні лише у 2010 р.[81] Таким чином, наша держава перебуває у початковій фазі цього процесу, і тому, щоб оцінити для неї перспективи захисту ПД у кіберпросторі, потрібно розглянути стан і тенденції розвитку системи загалом.

6 липня 2010 р. Україна ратифікувала базові європейські стандарти у сфері захисту персональних даних, зокрема *Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних* (Страсбург, 28 січня 1981 р., № 108) та *Додатковий протокол* до неї щодо органів нагляду та транскордонних потоків даних (*ETS* № 181). Крім того, Україна офіційно підтримала принципи *Директиви 95/46/ ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних»* від 24 жовтня 1995 р. Таким чином, **Україна взяла на себе зобов'язання адаптувати національне законодавство та систему захисту персональних даних до положень цих актів**, наблизивши його таким чином до європейських стандартів.

Отже, зокрема, **від створення дієвої, гармонізованої з європейським законодавством вітчизняної системи захисту персональних даних залежить успішність інтеграції України в ЄС**.

По-перше, наявність такої системи є **підставою для успіху т.зв. безвізового діалогу між Україною і ЄС**, що був офіційно започаткований на самітах Україна–ЄС 9 вересня 2008 р. у Парижі та 29 жовтня 2008 р. у Брюсселі. Така умова безпосередньо передбачена *Планом дій щодо лібералізації Європейським Союзом візового режиму для України*, прийнятого 22 листопада 2010 р. у Брюсселі.

По-друге, імплементація європейських норм і принципів щодо захисту ПД є також передумовою для подальшого **розширення участі України в низці європейських і міжнародних профільних організацій**.

По-третє, створення єдиних для України та ЄС нормативно-правових «правил гри» у сфері захисту ПД абсолютно необхідне для повноцінного розгортання обмінів, контактів і співробітництва в політичній, бізнесово-фінансовій і багатьох інших сферах.

---

[81] Власне, першу редакцію Закону України «Про захист персональних даних» було прийнято 9.01.2007 р., однак уже 30.01.2007 р. тодішній Президент України наклав вето на цей акт. 22.02.2007 р. було ухвалено Постанову Верховної Ради України про доопрацювання Закону України «Про захист персональних даних». Редакція Закону за № 2297-VI, що згодом стала основою українського профільного законодавства, вперше була подана на розгляд ВР України 1.06.2010 р. (Див.: http://zakon4.rada.gov.ua/laws/card/2297-17).

З 2010 р. Україна здійснила значну законотворчу й адміністративно-організаційну роботу зі створення національної системи захисту ПД. Подальшій імплементації європейських положень і норм багато в чому сприяло ухвалення *Закону України «Про захист персональних даних»* від 1 червня 2010 р., який набув чинності 1 січня 2011 р. Закон базується на основних принципах Директиви 95/46/ЄС. Деякі з пропозицій Єврокомісії вже тоді знайшли своє відображення в українському законодавстві, зокрема вимоги щодо згоди суб'єкта на оброблення даних, зобов'язання призначити окрему особу або інститут, відповідальний за захист персональних даних, право особи вимагати знищення даних.

Однією з вимог ЄС до України згідно із зазначеним вище Планом дій є прийняття відповідного законодавства про захист персональних даних і створення політично та фінансово незалежного наглядового органу у сфері захисту персональних даних, а також імплементація Закону України «Про захист персональних даних» та забезпечення ефективного функціонування незалежного наглядового органу з питань захисту персональних даних, у т.ч. у спосіб передбачення необхідних фінансових і людських ресурсів.

9 грудня 2010 р. *Указом Президента України № 1085/2010* «Про оптимізацію системи центральних органів виконавчої влади» утворено *Державну службу України з питань захисту персональних даних (ДСЗПД)* як центрального органу виконавчої влади України, діяльність якого спрямовується і координується Кабінетом Міністрів України через міністра юстиції України. 6 квітня 2011 р. Указом Президента України № 390 затверджено Положення про Державну службу України з питань захисту персональних даних.

У жовтні-листопаді 2011 р. у межах процесів імплементації зазначеного Плану дій відбулися експертні місії Європейської Комісії та Європейського підрозділу співпраці у сфері юстиції (Євроюст) в Україну. Їх метою була перевірка поточного функціонування уповноваженого органу України з питань захисту персональних даних (ДСЗПД) щодо відповідності встановленим для Європейського співтовариства стандартам незалежності. За результатами експертних місій було надано звіти, в яких рекомендовано звернути увагу, зокрема, на таке:

• внесення змін до Закону України «Про захист персональних даних» на основі рекомендацій європейських експертів;

• забезпечення незалежності уповноваженого органу України з питань захисту персональних даних[82].

[82] *Щодо актуальних* питань захисту персональних даних : лист від 11.06.2013 р., вх. № 3111/16-600-1513 / Представництво України при Європейському Союзі.

Таким чином, **саме інституційна організація системи захисту ПД в Україні стала предметом найбільш інтенсивних консультацій з ЄК та Євроюстом**. Експерти місії зазначили, що перебування Державної служби України з питань захисту персональних даних у системі органів виконавчої влади не надає достатніх гарантій інституційної незалежності цього органу, оскільки за такої моделі зберігається високий ризик зовнішнього тиску та політичного впливу[83]. За результатами зазначеної місії було висунуто такі **вимоги щодо незалежності державного органу України із захисту персональних даних**: «законодавство повинно забезпечувати інституційну, організаційну та повну функціональну незалежність органу із захисту персональних даних. Це означає, що при виконанні своїх функцій зазначений наглядовий орган повинен бути захищений від будь-якого зовнішнього впливу та мати необхідні повноваження та ресурси»[84].

Цікаво, що, обґрунтовуючи ці положення, місія посилалася на власний досвід. Так, у жовтні 2012 р. у Суді ЄС розглядалася справа з наглядовим органом із захисту ПД Австрії, подібним до українського. Суд визнав цю інституцію як таку, що не відповідає вимогам Директиви ЄС через відсутність достатньої функціональної незалежності цього органу від уряду, оскільки він належав до структури відомства федерального канцлера Австрії, його працівники були службовцями Канцелярії тощо[85]. Подібний судовий розгляд мав місце у 2010 р. – рішення Суду ЄС від 9 березня 2010 р. у справі C-518/07 «Європейська Комісія проти Федеральної Республіки Німеччини» (пп. 36 та 37)[86].

На користь ефективності моделі, у якій контрольний орган із захисту ПД підзвітний саме парламенту, але при цьому зберігає особливий статус і повноваження, свідчить також досвід Бельгії, Сполученого Королівства, Угорщини[87].

І хоча *організаційна* незалежність Державної служби України з питань захисту персональних даних була визнана експертами адекват-

---

[83] Щодо *актуальних* питань захисту персональних даних : лист від 11.06.2013 р., вх. № 3111/16-600-1513 / Представництво України при Європейському Союзі.

[84] Там само.

[85] *Action* under Article 258 TFEU for failure to fulfil obligations, brought on 22 December 2010 : judgment of the court in case C-614/10, 16 Oct. 2012 [Електронний ресурс]. – Режим доступу: http://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=EN

[86] *Щодо актуальних* питань захисту персональних даних : лист від 11.06.2013 р., вх. № 3111/16-600-1513 / Представництво України при Європейському Союзі.

[87] *Різак М.* Правовий статус уповноваженого органу з питань захисту персональних даних в Україні: сучасний стан та перспективи розвитку / М. Різак // Наукові записки Інституту законодавства Верховної Ради України. – 2013. – № 2. – С. 48 [Електронний ресурс]. – Режим доступу: http://instzak.rada.gov.ua/instzak/doccatalog/document?id=62276

ною, експертна місія запропонувала передати ДСЗПД під юрисдикцію Верховної Ради України[88].

З огляду на висновки з боку ЄС, а також ґрунтуючись на відповідних положеннях Конституції України, *Міністерство юстиції як головний розробник законодавства України у сфері захисту персональних даних внесло пропозиції щодо передачі функцій захисту персональних даних Уповноваженому Верховної Ради України з прав людини*[89].

Черговим кроком у модернізації вітчизняного профільного законодавства став *Проект закону України «Про внесення змін до Закону України «Про захист персональних даних»* (щодо удосконалення правового регулювання у цій сфері)» від 28 травня 2012 р. № 10472-1, який було ухвалено Верховною Радою України 2 жовтня того ж року. Формально цей нормативний акт був зорієнтований на європейські норми, у т.ч. на розглянуті Стандарти захисту персональних даних Євросоюзу. Зокрема, змінено сферу дії Закону України «Про захист персональних даних», у т.ч. визначено, що він поширюється на будь-які дії, що стосуються оброблення персональних даних, і не обмежується лише базами персональних даних. Також розширено права суб'єктів персональних даних, зокрема щодо заперечення оброблення ПД, внесення застережень стосовно їх оброблення, оскарження оброблення персональних даних і відкликання згоди на їх оброблення.

При цьому нову редакцію Закону неодноразово критикували вітчизняні експерти, спеціалісти Ради Європи, громадські організації та деякі українські посадовці[90]. 8 листопада 2013 року Президент України застосував до Закону право вето. У його пропозиціях, офіційно направлених до Верховної Ради України, зокрема, зазначається, що введення в дію цього акта «призведе до дублювання повноважень органів виконавчої влади, не відповідає засадам утворення, ліквідації та реорганізації центральних органів влади, визначеним ст. 5 Закону України «Про центральні органи виконавчої влади»[91].

---

[88] *Щодо актуальних* питань захисту персональних даних : лист від 11 червня 2013 р., вх. № 3111/16-600-1513 / Представництво України при Європейському Союзі.

[89] Там само.

[90] Див.: *Эксперты* просят Януковича ветировать закон о защите персональных данных [Електронний ресурс]. – Режим доступу: http://www.unian.net/news/529743-ekspertyi-prosyat-yanukovicha-vetirovat-zakon-o-zaschite-personalnyih-dannyih.html; *Лутковская* призывает Януковича ветировать закон о защите персональных данных [Електронний ресурс]. – Режим доступу: http://www.unian.net/news/530011-lutkovskaya-prizyivaet-yanukovicha-vetirovat-zakon-o-zaschite-personalnyih-dannyih.html

[91] *Пропозиції* Президента України до Закону «Про внесення змін до Закону України «Про захист персональних даних» [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=43550

На інституційну неврегульованість української системи захисту ПД вкотре вказали і європейські експерти: «істотним недоліком» Закону, прийнятого 2 жовтня 2012 р., вони знову назвали «відсутність чіткої норми про організаційну та функціональну незалежність уповноваженого державного органу з питань захисту персональних даних»[92].

12 лютого 2013 р. відбулися чергові багатосторонні консультації за участю експертів генеральних директоратів Європейської Комісії «Юстиція, свобода та безпека», «Внутрішні справи», Європейської служби зовнішньої діяльності, Представництва ЄС в Україні, Ради Європи, а також Національної комісії Франції з питань інформаційних технологій та свобод. Під час консультацій експерти погодилися, що запропоноване українською стороною вирішення проблеми відповідатиме європейським стандартам незалежності органів захисту персональних даних[93].

14 травня 2013 року Верховна Рада України ухвалила *Проект закону «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних»* від 17 квітня 2013 р. № 2836, яким передбачено низку змін у законодавстві в контексті модернізації галузевої нормативно-правової бази[94].

Так, цим актом внесено зміни до Кодексу України про адміністративні правопорушення, Закону України «Про захист персональних даних» та Закону України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних, **що стосуються визначення Уповноваженого Верховної Ради України з прав людини уповноваженим органом у сфері захисту персональних даних**. 6 червня 2013 р. Президент України повернув Закон до Верховної Ради України, а 3 липня український парламент прийняв його з урахуванням пропозицій Президента[95]. Зокрема, пропозиції стосувалися виключення з Розділу ІІ «Прикінцеві та перехідні положення» підпункту 3 п. 3 та доповнення його приписом щодо передачі Державного реєстру баз персональних даних і заяв

---

[92] *Коментарі* експертів Ради Європи до змін до Закону України про захист персональних даних [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/dszpd/doccatalog/document?id=51483

[93] *Щодо актуальних* питань захисту персональних даних : лист від 11.06.2013 р., вх. № 3111/16-600-1513 / Представництво України при Європейському Союзі.

[94] *Пропозиції* Президента до Закону «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=46647

[95] Там само.

про реєстрацію баз персональних даних, поданих у встановленому порядку, до набуття чинності цим Законом. Кабінету Міністрів України було доручено протягом трьох місяців з дня набуття чинності Законом (1.01.2014 р.) забезпечити у встановленому законодавством порядку передачу реєстру Уповноваженому Верховної Ради України з прав людини. Відповідно, до настання зазначеного терміну спеціально уповноваженим державним органом у сфері захисту персональних даних є Державна служба України з питань захисту персональних даних (ДСЗПД України)[96].

Таку реструктуризацію повноважень підтримали всі дотичні до реформування системи захисту ПД державні відомства та інститути (у т.ч. Президента України і Верховної Ради України), крім ДСЗПД України. Жодним чином не заперечуючи доцільність розформування ДСЗПД і подальшого вдосконалення механізмів захисту ПД в Україні, експерти Служби разом із цим вважають запропонований у Законі шлях хибним. На їхню думку, «запропоновані зміни не повною мірою узгоджуються з природою конституційно-правового статусу Уповноваженого Верховної Ради України з прав людини, який відповідно до ст. 101 Конституції України здійснює парламентський контроль за додержанням конституційних прав і свобод людини і громадянина», тоді як «...переважна більшість повноважень з питань здійснення державного контролю за додержанням законодавства про захист персональних даних <...> за своєю природою є повноваженнями саме органів виконавчої влади»[97]. Отже, вони вважають цю зміну *«концептуально вразливою і такою, що не повною мірою узгоджується з відповідними положеннями Конституції та Закону України «Про Уповноваженого Верховної Ради України з прав людини»* (курсив мій – *С. Г.*)[98].

ДСЗПД запропонувала власну модель модернізації: «...Серед існуючих моделей побудови органів державної влади в Україні *найбільш оптимальним варіантом є створення уповноваженого органу як державного органу зі спеціальним статусом* (курсив мій – *С. Г.*). Державні органи зі спеціальним статусом мають визначені законодавством України особливі завдання й повноваження, щодо них може встановлюватися спеціальний порядок утворення, реорганізації, підконтроль-

[96] *Верховна* Рада України 14 травня 2013 року ухвалила Закон «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/dszpd/uk/publish/article/56523

[97] *Щодо актуальних* питань захисту персональних даних : лист від 20.06.2013 р., вх. № 09/1675-13 / Державна служба України з питань захисту персональних даних.

[98] Там само.

ності, підзвітності, а також призначення і звільнення керівників та вирішення інших питань». В якості модельного прикладу такого органу згадується Антимонопольний комітет України[99].

Загалом експерти ДСЗПД України, посилаючись на власні висновки та оцінки європейських спеціалістів, констатують, що вимоги поточної редакції Закону України «Про захист персональних даних» та застосування його положень при обробленні персональних даних із використанням веб-ресурсів «повністю кореспондуються з рекомендаціями Комітету міністрів Ради Європи щодо захисту недоторканності приватного життя в інтернеті, рекомендаціями Робочої групи, що функціонує відповідно до статті Директиви 95/46/ЄС, та рекомендаціями Міжнародної робочої групи (Берлінська група) з питань захисту персональних даних у телекомунікаціях»[100]. Тут можна додати, що **з чинної редакції Закону було вилучено деякі архаїчні норми**, які не лише не регулювали оброблення ПД у кіберпросторі, а і в низці положень, по суті, унеможливлювали її. З-поміж іншого, переглянуто сферу застосування процедури реєстрації баз даних, яка є майже неможливою в режимі он-лайн, надто – у «хмарах». Якщо раніше передбачалася безумовна та обов'язкова реєстрація таких баз, то тепер необхідно буде лише попереджати Уповноваженого про факт збору/оброблення персональних даних і лише в тому випадку, якщо вони є «особливим ризиком для прав і свобод суб'єктів персональних даних» (відповідний перелік встановлюється Уповноваженим)[101].

Підсумовуючи, треба зазначити, що з 2010 р., коли фактично розпочалася робота зі створення української системи державного нагляду за обробленням та захистом персональних даних, Україні загалом вдалося сформувати сучасну, відповідну європейським стандартам нормативно-правову базу для подальшого формування вітчизняної системи захисту ПД, що є значним досягненням, зважаючи на безпрецедентні виклики, пов'язані з глобалізацією, революційними змінами в ІКТ, комунікаціях тощо.

---

[99] *Щодо актуальних* питань захисту персональних даних : лист від 20.06.2013 р., вх. № 09/1675-13 / Державна служба України з питань захисту персональних даних.

[100] *Практика* застосування законодавства з питань захисту персональних даних при обробці персональних даних з використанням веб-ресурсів : мат. до відкрит. засід. колегії Держ. служби України з питань захисту персональних даних [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/dszpd/doccatalog/document?id=53900

[101] *Пропозиції* Президента до Закону «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=46647

Показником успішності та фахового рівня роботи українського регулятора захисту персональних даних (ДСЗПД) є його широка міжнародна співпраця з Євроюстом, Європолом, Управлінням з питань запобігання зловживанням та шахрайству*, Групою керівників уповноважених органів з питань захисту персональних даних країн Центральної та Східної Європи, членство в Глобальній мережі усунення порушень у сфері приватності (*Global Privacy Enforcement Network, GPEN*), регулярний експертний обмін з Радою Європи, участь у Міжнародній робочій групі з питань захисту персональних даних у сфері телекомунікацій (*International Working Group on Data Protection in Telecommunications, IWGDPT*)[102].

Проте, якщо на рівні державних органів та експертних кіл ситуація у сфері захисту ПД є задовільною, **пересічні українці поки що демонструють** байдужість до нових для них правових практик і **недостатній рівень розуміння сутності персональних даних, а також значення їх захисту в сучасному світі, надто у мережі інтернет**.

Наприкінці 2012 р. Всеукраїнська громадська організація «Українська асоціація захисту персональних даних» ініціювала та провела перше **дослідження в межах громадського моніторингу відкритості та прозорості оброблення персональних даних в інтернеті**[103]. За результатами дослідження, зокрема, виявилося, що лише близько третини веб-ресурсів національного сегмента інтернету надають користувачам мінімальні відомості про розпорядника їхніх персональних даних – найменування юридичної чи ім'я фізичної особи, яка і є відповідно до законодавства відповідальною за оброблення персональних даних відвідувачів та дотримання прав останніх на невтручання в їх сімейне та приватне життя. Так само приблизно третина веб-ресурсів повідомляють відвідувачів про їхні права.

Автори моніторингу також констатують: «Можна впевнено зробити висновок, що **переважна частина національних веб-ресурсів, можливо більше трьох четвертей, не забезпечують відкритості і прозорості обробки персональних даних**, ігнорують вимоги ратифікованої Україною Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, положень Закону України «Про захист персональних даних», рекомендацій Комітету міністрів

---

[102] *Козак В.* Захист персональних даних: право, практика, нагляд / В. Козак [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/dszpd/doccatalog/document?id=51760

[103] *Проведено* перший громадський моніторинг інтернет-ресурсів [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/dszpd/uk/publish/article/52973;jsessionid=63B651D13E1C92357A4B761F62586F8B

* ОЛАФ (*OLAF, European Anti-Fraud Office)*, скорочення оригінальної назви французькою мовою.

№ R(99)5 від 23 лютого 1999 р. державам-членам Ради Європи «Про захист недоторканності приватного життя в Інтернеті»[104].

Така ситуація є парадоксальною та тривожною, адже **Україна належить до найбільш перспективних держав світу за показниками/прогнозами імплементації *IT* і проникнення інтернету**. За офіційними даними НРКЗІ, на тлі тенденції до стабільного зростання інтернет-аудиторія України у 2012 р. становила 43,5 % жителів, причому 35 % домогосподарств мали широкосмуговий доступ до Всесвітньої мережі (одне з перших місць у Європі). Уже у 2011 р. Україна увійшла до першої десятки країн світу з найшвидшим доступом до інтернету, і тоді ж уперше – до рейтингу абонентів галузевої організації *FTTH Council Europe*. Згідно з останніми показниками цієї організації, проголошеними на Всесвітньому форумі з широкосмугових технологій (Париж, вересень 2012 р.) Україна посідає 16-те місце у світі за розвитком мереж *FTTH*[105].

Понад те, висока динаміка зростання спостерігається й у тих секторах українського кіберпростору, які входять до групи особливого ризику з погляду безпеки персональної інформації. Так, 56 % вітчизняних інтернет-користувачів виходять в он-лайн для спілкування в соціальних мережах, 52 % – для користування електронною поштою[106]. Але найкритичнішим має стати один із новітніх і найбільш неоднозначних у плані безпеки даних онлайн-секторів – ринок «хмарових» послуг.

16 квітня 2013 року один з провідних українських операторів «хмарових» сервісів *De Novo* і *GfK Ukraine* презентували результати дослідження українського ринку «хмарових» обчислень[107]. Дослідження було сфокусоване на середніх і великих підприємствах фінансової, телекомунікаційної, торгівельної, логістичної і виробничої галузей, оскільки саме вони є основними споживачами *IT*-послуг в Україні.

Згідно з отриманою статистикою споживання, «**хмаровий» ринок України**, подібно до сусідніх (Російська Федерація, Угорщина, біль-

---

[104] *Проведено* перший громадський моніторинг інтернет-ресурсів [Електронний ресурс]. – Режим доступу: http://uapdp.org/images/news/doslidzhennya/Research-results-v.2.2.pdf

[105] *Звіт* про роботу Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, 2012 рік [Електронний ресурс]. – Режим доступу: http://www.nkrz.gov.ua/uk/activities_nkrzi/1324727592/1364229681/

FTTH (*Fiber To The Home* – волокно до будинку користувача) – архітектура побудови мережі, за якої волоконно-оптичний кабель використовується для з'єднання центру надання послуг і певного приміщення (квартири) або приватного будинку.

[106] Там само.

[107] *De Novo* и GfK Ukraine измерили облачный потенциал Украины [Електронний ресурс]. – Режим доступу: http://www.de-novo.biz/novosti-i-istorii-uspeha/news/gfk/

шість країн СНД), **є на етапі формування попиту і акумулювання первинного досвіду споживання «хмарових» рішень**. Про це свідчать мінімальний рівень знання кінцевих користувачів про «хмарові» обчислення та невисокий рівень проникнення технології. Так, 47 % опитаних *IT*-служб вважають свою обізнаність у «хмарових» рішеннях поверхневою, а 88 % опитаних керівників зовсім не знайомі з «хмаровими» сервісами[108].

Разом з тим понад третина опитаних *IT*-служб планує користуватися «хмаровими» рішеннями, а 75 % з них збираються це робити вже у 2014 р. «Підігрівають» ринок також *IT*-компанії, що активно опановують технологію та відповідні бізнес-рішення. Згідно з результатами дослідження «хмарові» технології вивчають близько половини опитаних керівників *IT*-компаній, 15 % уже мають експертизу в цій сфері, а 94 % планують працювати на «хмаровому» ринку України. Стрімкому проникненню «хмарових» обчислень на український ринок у 2014–2016 рр. сприятиме і цей чинник, і позитивний досвід первинного використання: «хмарові» сервіси майже або ж повністю виправдали очікування 84 % опитаних українських організацій[109].

Плани українських підприємства щодо використання «хмарових» рішень, а також інтенсивне освоєння технології *IT*-компаніями створюють потенціал ринку, який **«до 2015–2016 рр. демонструватиме експоненціальне зростання, характерне для хмарових ринків розвинених країн»**[110].

Показово, що майже таких самих оцінок і висновків щодо України дійшли також експерти компанії *Parallels*, дослідивши наприкінці 2012 р. динаміку «хмарових» ринків у країнах СНД[111].

*Зрозуміло, що **стрімкий розвиток українського онлайн-середовища** за всієї оптимістичності перспектив додатково **загострює й актуалізує весь комплекс проблем захисту ПД «у віртуалі»**. Для успішного протистояння викликам у цій сфері Україна потребує щонайменше: а) адекватного правового забезпечення та ефективної національної системи регулювання та нагляду; б) розвиненого й диверсифікованого ринку юридичних послуг; в) кваліфікованих і відповідальних контрагентів – провайдерів онлайн-послуг та споживачів, суб'єктів персональних даних, їх володільців і розпорядників. Із цих трьох необ-*

---

[108] *De Novo* и GfK Ukraine измерили облачный потенциал Украины / [Електронний ресурс]. – Режим доступу: http://www.de-novo.biz/novosti-i-istorii-uspeha/news/gfk/

[109] Там само.

[110] Там само.

[111] *Колеров Ю.* Облачный рынок в цифрах и фактах: взгляд Parallels: Доклад на *CLOUD Computing Summit*, 1 марта 2013 г. [Електронний ресурс]. – Режим доступу: http://www.ex.ua/view_storage/271113003934

хідних складників впевнено поки що можна говорити лише про досить успішне формування першого.

Також певна робота здійснюється й на рівні громадських та експертних організацій. Третій Український Форум з управління інтернетом, що відбувся в Києві 28 вересня 2012 р., у своїй Резолюції ухвалив адресувати постачальникам послуг інтернет-звернення щодо доцільності дотримання рекомендацій Комітету міністрів Ради Європи № R(99)5 від 23 січня 1999 р.[112]

З ініціативи згаданої Української асоціації захисту персональних даних 25 жовтня 2012 р. було прийнято Декларацію *«За недоторканність приватного життя в Інтернеті»*, до якої приєдналася низка провідних національних телекомунікаційних компаній.

У вересні 2013 р. було опубліковано посібник «Кібертероризм і захист персональних даних», який став результатом дослідної роботи колективу експертів ТОВ «Консалтингова компанія «СІДКОН», виконаної в інтересах ВГО «Українська асоціація захисту персональних даних». Автори посібника роблять акцент на залученні підвищеної уваги державних органів, а також керівників комерційних компаній до проблеми, пов'язаної з кібертероризмом і захистом державних і корпоративних інформаційних ресурсів, персональних даних громадян, а також демонстрації масштабу поширення та необхідності першочергового вирішення зазначеної проблеми[113].

Подібні акції свідчать про усвідомлення експертною та професійною спільнотою необхідності розгортання в Україні системної роботи щодо підвищення правової культури, поширення адекватного сприйняття «прайвесі» в суспільстві, бізнесі та політиці, встановлення єдиних «правил гри» щодо оброблення і захисту персональних даних як у фізичному, так і у віртуальному середовищі. Водночас дані зазначеного моніторингу оброблення персональних даних у національному сегменті інтернету переконують у тім, що сьогодні всі ці поняття і практики тільки починають засвоюватися українським суспільством.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

I

1. У європейській правовій традиції захист персональних даних трактується як одна з безумовних підстав забезпечення фундаментального права людини на недоторканність її особистого життя, яке, своєю

---

[112] *Резолюція* Форуму, Київ, 28 вересня 2012 р. [Електронний ресурс]. – Режим доступу: http://igf-ua.org/docs/Resolution_IGF-UA_2012.pdf

[113] *Кібертероризм* і захист персональних даних [Електронний ресурс]. – Режим доступу: http://www.uapdp.org./index.php/contact-us/2-uncategorised/57-2014-06-10-17-56-10

чергою, є засадничим для сучасної демократії з її приматом поваги до прав і гідності людини. Нині цей погляд є загальновизнаним у світі: недоторканність приватного життя, у т.ч. особистої інформації людини, як одне з її основних прав закріплена в найважливіших міжнародних актах сучасності, а також у абсолютній більшості національних законодавств світу.

2. Сьогодні не лише в ЄС, а й майже в усіх країнах і міждержавних об'єднаннях **найбільш проблематичною сферою захисту ПД стали *IT* і кіберпростір** як нове специфічне інформаційно-комунікаційне середовище, що стрімко розвивається і збільшується. **У цій сфері нормативно-правове регулювання хронічно відстає від якісного (технології) та кількісного (продуктивність і поширеність інфраструктур) розвитку**. Це відставання окреслилося ще в 90-ті роки XX ст., але **стало дійсно системною проблемою протягом 2000-х років** разом із революційними винаходами та змінами в інформаційно-комунікаційних технологіях (ІКТ), лавиноподібним поширенням Всесвітньої мережі і міграцією цілих сфер людської діяльності до онлайн-сектору.

3. Основним протиріччям зазначених процесів є **дедалі ширша прірва між безпрецедентними можливостями сучасного інтернет-середовища** (разом з асоційованими з ним електронними пристроями неконтрольованого збору, оброблення, зберігання і оприлюднення гігантських обсягів різних ПД) **і традиційними, «доцифровими» юридичними нормами та практиками**, базованими на традиційному уявленні про межі й засоби забезпечення приватного життя людини.

4. Тотальна комп'ютеризація телекомунікацій, систем транспортування, фінансів, обліку населення, медичного обслуговування, численних баз даних **постійно збільшує кількість та якість інформації, що опрацьовується стосовно кожної особи**, причому зазвичай без її відома. Існує та постійно вдосконалюється низка технологій для датамайнінгу та створення індивідуальних «онлайн-портретів» на основі збору та аналізу всіх відомостей, що мають будь-який (хай і непрямий) стосунок до користувачів. **Рівень «деанонімізації» користувачів у сучасному онлайн-середовищі стає майже стовідсотковим, навіть якщо вони дотримуються вимог безпеки**.

5. Додаткові й дуже серйозні ступені ризику щодо безпеки даних несуть у собі елементи новітньої третьої *IT*-платформи, яка нині активно впроваджується у світі і принципово орієнтована на: а) зберігання основної частини інформації користувачів не на особистих фізичних носіях, а у віртуальному середовищі («хмарові» сервіси); б) повсюдний швидкісний безпровідний доступ до інтернету. Практика свідчить, що на цей час така **модель зберігання та оброблення інформації не може гарантувати особі (а) постійний і стабільний доступ до її персональних даних, (б) недоторканність цих даних, (в) контроль за їх**

обробленням (г) точні відомості про їх місцезнаходження. Іншими словами, проблематично гарантувати фундаментальне право особи на «прайвесі» (приватність).

6. Загалом сьогодні **суть проблеми захисту персональних даних у кіберпросторі визначається процесами**, що є тісно пов'язаними та взаємодоповнюваними:

• **перманентне і швидке збільшення кількості персональних даних громадян у публічному та/чи несанкціонованому ними доступі**;

• **перманентне зменшення для пересічного громадянина реальних можливостей контролю збору й оброблення його власних ПД**.

Поки що **ці дві тенденції є прогресуючими і стабільними рівно настільки, наскільки сталим є розвиток самого кіберпростору**, незважаючи на численні скандали, судові позови, суспільні та законодавчі ініціативи, вимоги дотримання права і вдосконалення систем безпеки.

7. У суто соціальному вимірі основний вектор розвитку кіберпростору резюмується у **швидкому перетворенні глобального інтернет-середовища на справді всюдисущу, загальнодоступну й абсолютно необхідну для нормальної життєдіяльності людства структуру**. Отже, **майже вся зафіксована людиною інформація, у т.ч. персональні дані, надалі обертатиметься та зберігатиметься у Всесвітній мережі**.

8. Якщо найближчим часом не буде знайдено ефективного й при цьому демократичного рішення проблеми захисту персональних даних у веб-середовищі, у перспективі **це може призвести до непередбачуваних і небезпечних переосмислень загальноприйнятих уявлень про приватність, її сенс та межі, а отже, до перегляду правового змісту самого поняття «персональні дані»**.

II

9. Нині саме керівництво ЄС визнає, що у сфері регулювання захисту персональних даних у віртуальному середовищі **класичне законодавство Євросоюзу є застарілим і малоефективним**. З 2011 р. триває робота Європейської Комісії над глибокою реформою нормативно-правового поля щодо захисту персональних даних.

10. Єврокомісія здійснює спроби правового врегулювання питань захисту ПД з урахуванням нових викликів і загроз у кіберпросторі з позиції безумовного пріоритету невід'ємного права особи на недоторканність і вільне розпорядження ними. У цьому напрямі формуються і стандарти у сфері розширення прав осіб-суб'єктів персональних даних при одночасному посиленні контрольованості та відповідальності операторів ПД. Нові правила ЄС мають прийматися також і нерезидентами ЄС, якщо вони активно працюють на ринку ЄС і надають свої послуги громадянам ЄС.

11. Попри те, що стандарти ще не ухвалені, вони є чітким індикатором сучасних настроїв у Єврокомісії (а, ймовірно, і загалом у керівництві ЄС) щодо **надання громадянам більших можливостей контролю використання їхніх персональних даних у спосіб вдосконалення адміністративних процедур, розширення відповідних прав і збільшення контрольованості та відповідальності компаній-операторів** стосовно питань захисту і оброблення персональних даних.

12. У вересні 2012 р. Європейська Комісія виступила зі стратегічним документом **«Вивільнення потенціалу «хмарових» обчислень в Європі» (***Unleashing the potential of cloud computing in Europe***)**, спрямованим на прискорення імплементації та значне розширення використання «хмар» в економіці ЄС. Особливу увагу в документі приділено питанням безпеки користувачів, зокрема захисту персональних даних.

13. Нині законодавчі пропозиції Єврокомісії оцінюються як найбільш складні проекти, які коли-небудь розроблялися та опрацьовувалися в межах ЄС. Водночас немає сумніву, що **ці дискусії та робота в євроінституціях визначать провідні світові стандарти захисту персональних даних**.

III

14. Маємо розуміти, що створення дієвої, гармонізованої з європейським законодавством вітчизняної системи захисту персональних даних є одним з чинників подальшої успішності інтеграції України в ЄС.

15. Системна робота над створенням національних наглядових інституцій та законодавства у сфері захисту ПД триває в Україні лише з 2010 р. **Україна взяла на себе зобов'язання адаптувати національне законодавство та систему захисту персональних даних до положень відповідних правових актів та стандартів ЄС**. За цей час **Україні загалом вдалося сформувати сучасну, відповідну європейським стандартам нормативно-правову базу для подальшого формування вітчизняної системи захисту ПД, а профільні державні структури здійснюють масштабну міжнародну співпрацю з цих питань**.

16. 14 травня 2013 року Верховна Рада України прийняла Проект Закону «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» від 17 квітня 2013 р. № 2836, яким передбачено низку змін у законодавстві в контексті модернізації галузевої нормативно-правової бази. Зокрема Уповноважений Верховної Ради України з прав людини визначений **уповноваженим органом у сфері захисту персональних даних**.

17. На сьогодні закладено лише основи вітчизняного профільного законодавства. Необхідними є його подальша **систематизація, розроблення підзаконних актів, відповідних національних стандартів, чітке визначення термінів, понять і категорій**. Безумовно, Україна

має уважно слідкувати за відповідним законотворчим процесом у ЄС, проте **питання остаточної транспозиції нових європейських підходів у національне законодавство України доцільно було б порушувати після результативного завершення** цього процесу в Європейському Союзі.

18. Саме поняття «персональні дані» і правові практики, пов'язані з їх захистом та обробленням, є відносно новими, а отже, малознайомими для українського суспільства. **Пересічні українці демонструють байдужість до них і недостатній рівень розуміння значення захисту персональних даних у сучасному світі, надто у мережі інтернет**.

19. Оскільки в Україні швидкими темпами запроваджуються сучасні *IT*-технології та поширюється інтернет, відповідно актуалізується весь комплекс проблем із захисту ПД «у віртуалі». **Для успішного протистояння викликам у цій сфері Україна потребує щонайменше: а) адекватного правового забезпечення та ефективної національної системи регулювання та нагляду; б) розвиненого й диверсифікованого ринку юридичних послуг; в) кваліфікованих і відповідальних контрагентів – провайдерів онлайн-послуг та споживачів, суб'єктів персональних даних, їх володільців і розпорядників. Із цих трьох необхідних складників впевнено поки що можна говорити лише про досить успішне формування першого**.

Додаток

ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СУЧАСНОМУ КІБЕРПРОСТОРІ: ПРАВОВІ ТА ТЕХНІКО-ТЕХНОЛОГІЧНІ АСПЕКТИ

Матеріали засідання «круглого столу»
10 жовтня 2013 р.

10 жовтня 2013 року в Національному інституті стратегічних досліджень відбувся «круглий стіл» на тему: **«Особливості захисту персональних даних у сучасному кіберпросторі: правові та технікотехнологічні аспекти»**. На заході були присутні представники органів державної влади, зокрема Комітету з питань свободи слова та інформації Верховної Ради України, Комітету з питань інформатизації та інформаційних технологій Верховної Ради України, експерти та науковці. Учасники «круглого столу» визначили ключові проблеми захисту персональних даних у сучасному кіберпросторі, а також запропонували основні напрями їх вирішення.

В обговоренні взяли участь[114]:

БАРАНОВ Олександр Андрійович	директор Департаменту стратегії розвитку зв'язку Адміністрації Державної служби спеціального зв'язку та захисту інформації України
БЄЛЯКОВ Костянтин Іванович	завідувач наукового відділу правових проблем інформаційної діяльності Науково-дослідного інституту інформатики і права Національної академії правових наук України
БРИЖКО Валерій Михайлович	керівник центру проблем методології інформаційного права Науково-дослідного інституту інформатики і права Національної академії правових наук України
ВИСОЦЬКИЙ Сергій Михайлович	старший науковий консультант Департаменту Служби безпеки України
ГНАТЮК Сергій Леонідович	головний консультант відділу досліджень інформаційного суспільства та інформаційних стратегій НІСД
ДУБОВ Дмитро Володимирович	завідувач відділу досліджень інформаційного суспільства та інформаційних стратегій НІСД
ЗАЙЧУК Олег Володимирович	в.о. директора Інституту законодавства Верховної Ради України

[114] Усі посади та назви підрозділів є актуальними на дату проведення «круглого столу» 10 жовтня 2013 р.

ЗОЛОТАРЬОВА Оксана Вадимівна	начальник відділу взаємодії з Державною службою України з питань захисту персональних даних та Державною архівною службою України Міністерства юстиції України
ІСАКОВА Тамара Олегівна	головний спеціаліст відділу досліджень інформаційного суспільства та інформаційних стратегій НІСД
КАСПЕРСЬКИЙ Ігор Петрович	доцент спеціальної кафедри Національної академії Служби безпеки України
КОГУТ Юрій Іванович	голова правління ВГО «Українська асоціація захисту персональних даних»
КОНАХ Вікторія Костянтинівна	головний консультант відділу досліджень інформаційного суспільства та інформаційних стратегій НІСД
КУКАРІН Олександр Борисович	заступник завідувача кафедри інформаційної політики та технологій Національної академії державного управління при Президентові України
ЛАВРИК Вадим Олександрович	помічник-консультант народного депутата України Лук'янчука Руслана Валерійовича
ЛАНДЕ Дмитро Володимирович	завідувач наукового відділу правових проблем інформаційної безпеки Науково-дослідного інституту інформатики і права Національної академії правових наук України
ЛІТВІНОВ Максим Юрійович	начальник управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України
МЕЛЬНИК Костянтин Сергійович	начальник Управління юридичного забезпечення Державної служби України з питань захисту персональних даних
НАУМОВ Вадим Валентинович	заступник начальника Департаменту інформаційно-аналітичного забезпечення МВС України

ОЖЕВАН Микола Андрійович	головний науковий співробітник відділу досліджень інформаційного суспільства та інформаційних стратегій НІСД
ПАНЧЕНКО Валентина Миколаївна	начальник наукової лабораторії Національної академії Служби безпеки України
ПЕТРОВ Валентин Володимирович	представник Служби безпеки України
ПИЛИПЧУК Володимир Григорович	директор Науково-дослідного інституту інформатики і права Національної академії правових наук України
ПОПОВА Наталя Олексіївна	старший науковий консультант Департаменту Служби безпеки України
СЕЛЕЦЬКИЙ Петро Іванович	головний консультант секретаріату Комітету Верховної Ради України з питань свободи слова та інформації
СИТНІЧЕНКО Євген Анатолійович	помічник-консультант народного депутата України, голови Комітету з питань європейської інтеграції
УВАРЕНКО Микола Миколайович	головний спеціаліст відділу телекомунікаційних мереж НКРЗІ
ФАЛЬ Олексій Михайлович	провідний науковий співробітник Інституту кібернетики імені В. М. Глушкова Національної академії наук України
ФУРАШЕВ Володимир Миколайович	перший заступник директора з наукової роботи Науково-дослідного інституту інформатики і права Національної академії правових наук України
ХОМУТ Галина Тарасівна	виконавчий директор ВГО «Українська асоціація захисту персональних даних»
ЦАРУК Олександр Васильович	головний консультант секретаріату Комітету Верховної Ради України з питань інформатизації та інформаційних технологій

ЧЕРНИШУК Сергій Вікторович	співробітник відділу телекомунікаційних мереж Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації
ЧУВИРІН Дмитро Едуардович	головний спеціаліст Департаменту інформаційно-аналітичного забезпечення МВС України
ЯБЛОНСЬКИЙ Василь Миколайович	заступник директора Національного інституту стратегічних досліджень
ЯКОВЕНКО Євген Володимирович	представник Служби безпеки України

ВИСТУПИ УЧАСНИКІВ

ЯБЛОНСЬКИЙ Василь Миколайович,
заступник директора Національного інституту стратегічних досліджень

Доброго дня, шановні учасники нашого «круглого столу»! Радий вас вітати в нашому Інституті!

Сподіваюся, що найближчі півтори-дві години стануть цікавими і дискусійними, тим більше, що питання, яке винесене сьогодні на обговорення – тема персональних даних – стосується кожного з нас. І, очевидно, з кожним роком ця тема ставатиме дедалі більш актуальною. У назву нашого заходу ми винесли лише частину проблеми, тобто проблему захисту ПД в умовах стрімкої інформатизації та глобалізації кіберпростору. Однак я сподіваюся, що заявлена тема спонукатиме нас до більш широкої дискусії і до обговорення ширшого кола питань.

Ми не можемо ігнорувати той факт, що під впливом інформатизації трансформується сама концепція захисту ПД, а ступінь їх поширення (причому часто поза бажанням їх суб'єктів) набуває загрозливого розмаху. У загальносвітовому вимірі точаться дискусії щодо того, яким має бути ефективний захист персональних даних, що уряди, громадяни, бізнес можуть зробити для їх більшого убезпечення, але щоб при цьому не постраждав економічний розвиток держави, який дедалі більше пов'язаний із вільними мережевими комунікаціями. Ще гострішою ця проблема стає внаслідок швидкого розвитку нових *IT*-платформ, які за своєю суттю мало підходять для ефективного застосування традиційних норм і правил захисту ПД. До таких, безумовно, належить і так звана «третя платформа» – бездротові веб-мережі, «хмарові» технології, мобільні пристрої доступу до мережі інтернет, оброблення «великих даних». Також ми не можемо ігнорувати багаторазове збільшення масштабів збору і моніторингу ПД, про що постійно чуємо останніми роками. І в Україні, і у світі все це знову і знову змушує порушувати питання про знаходження певного балансу між безпекою ПД і потребами економічного, технологічного та суспільного розвитку. Причому основна дискусія з цього приводу, очевидно, ще попереду.

Проблема захисту ПД нині є предметом особливої уваги з боку Європейського Союзу, інтеграція до якого залишається ключовим орієнтиром нашої і зовнішньої, і внутрішньої політики. Питанням ПД та їх оброблення присвячено окремі пункти Угоди про Асоціацію. Створення ефективних механізмів захисту ПД та необхідної інституційної основи їх безпеки є однією з умов подальшої поглибленої співпраці

між Україною та Європейським Союзом, у т.ч. з питань безвізового режиму та спрощення міграційних процесів. Україна приділяє значну увагу тематиці ПД, намагається побудувати ефективну правову та інституційну основу забезпечення прав громадян у цій сфері. Про актуальність цієї проблеми свідчить і той резонанс, який викликав нещодавній інцидент з держреєстрами. Україна не лише прагне, а реально вибудовує власну систему захисту ПД, яка відповідатиме найліпшим європейським практикам та інтересам наших громадян. Сподіваюся, сьогоднішнє обговорення надасть додаткового імпульсу цій роботі.

На початку «круглого столу» наші фахівці представлятимуть аналітичну доповідь «Особливості захисту персональних даних у сучасному кіберпросторі: правові та техніко-технологічні аспекти», а потім я запрошую всіх до плідної дискусії.

ГНАТЮК Сергій Леонідович,
головний консультант відділу досліджень інформаційного суспільства та інформаційних стратегій НІСД

Представив доповідь «Особливості захисту персональних даних у сучасному кіберпросторі: правові та техніко-технологічні аспекти».

ДУБОВ Дмитро Володимирович,
завідувач відділу досліджень інформаційного суспільства та інформаційних стратегій НІСД

Як уже говорив сьогодні Василь Миколайович, наша дискусія не має обмежуватися виключно тезами нашої доповіді і може бути ширшою, зачіпати ті питання, які не порушувалися в доповіді. Я гадаю, буде логічним, якщо ми надамо слово передусім представнику тієї структури, яка, власне, і відповідає в державі за захист персональних даних, – Державної служби захисту персональних даних.

МЕЛЬНИК Костянтин Сергійович,
начальник Управління юридичного забезпечення Державної служби України з питань захисту персональних даних

Хотів би сказати кілька слів стосовно порушеного сьогодні питання. Усім відомо, що Україна ратифікувала базові європейські стандарти, створено інституційну систему захисту персональних даних. Щодо їх захисту в кіберпросторі хотілося б звернути увагу на таке. По-перше, діяльність суб'єкта персональних даних у кіберпросторі слід розглядати крізь призму двох складників: з одного боку, це дотримання його прав у мережі інтернет, з іншого – це виконання володільцями персональних даних вимог законодавства та дотримання відповідних міжнародних стандартів. Протягом другого і третього кварталу поточного року наша Служба здійснила низку контрольних заходів щодо

дотримання володільцями персональних даних вимог законодавства. За їх результатами можна констатувати таке: лише у 15 % перевірок не було виявлено порушень, відповідно у 85 % виявлено порушення і видано приписи щодо їх усунення; на сьогодні виконали припис 35 % порушників, поінформували про виконання припису 53 %, термін дії припису ще не сплинув у 12 %. На сьогодні Служба узагальнила типові порушення законодавства у сфері захисту персональних даних під час їх оброблення в мережі інтернет.

Зокрема, на момент збору ПД суб'єктові ПД не повідомляється про володільця ПД, їх склад і зміст, мету їх збору, а також про права самого суб'єкта. У більшості випадків зміст персональних даних був явно надмірним щодо мети їх оброблення. Процедури оброблення ПД були визначені на сайті, але не були встановлені розпорядчими документами володільця, як це передбачено законодавством. Відвідувачі вебресурсу не повідомлялися про порядок доступу до їхніх ПД, не мали змоги висунути мотивовану вимогу щодо зміни або знищення своїх ПД. Відомості про відвідування сайтів надавалися третім сторонам без повідомлення відвідувачів.

У принципі, дотримання законодавства про захист ПД під час їх оброблення з використанням веб-ресурсів не вимагає від володільця ПД значних зусиль. У процесі здійснення перевірок значні порушення неодноразово усувалися протягом короткого часу. Ігнорування ж прийнятих в усьому світі правил оброблення ПД їх володільцями в Україні, на нашу думку, пов'язане насамперед з низькою правовою культурою і нерозумінням певних особливостей, встановлених Законом України «Про захист персональних даних». Тому усунення названих порушень вимагає зусиль як з боку уповноважених органів, так і з боку бізнесу, громадськості та інших суб'єктів.

ДУБОВ Д. В.:

Оскільки, крім уповноважених структур, на нашому заході присутні і представники Міністерства юстиції України, буде логічним також надати їм слово.

ЗОЛОТАРЬОВА Оксана Вадимівна,
начальник відділу взаємодії з Державною службою України з питань захисту персональних даних та Державною архівною службою України Міністерства юстиції України

Передусім хочу звернути вашу увагу на те, що Міністерство юстиції є органом, який формує державну політику у сфері захисту ПД, тобто всі нормотворчі ініціативи останніх двох-трьох років у цій сфері виходили насамперед з Мін'юсту. Дуже непростим був процес ухвалення першого закону 2010 р. (ці процедури були складними не тіль-

ки в Європейському Союзі, а й в Україні). Робота над першими профільними законами розпочалася ще у 2002 році, і в них було закладено хибну ідею про те, що суб'єкт ПД володіє своїми ПД відповідно до права власності, як встановлено Цивільним кодексом. Уже потім був ухвалений рамковий Закон, який є наразі чинним, він був результатом компромісу між усіма політичними силами. Закон був ухвалений заради ЄС, задля ЄС, через ЄС і за допомогою ЄС. Зрештою, ми маємо бути вдячними цьому міждержавному об'єднанню за те, що засадничі права людини нарешті стали захищеними в Україні. Зважаючи на рамковість цього Закону, було вжито заходів щодо його вдосконалення, і зараз ми можемо говорити про два умовні етапи розвитку законодавства щодо захисту ПД після ухвалення зазначеного Закону. Перший етап – це модернізація Закону, яка відбулася минулого року: за ініціативою уряду Верховна Рада прийняла Закон України № 10472-1[115]. Основні його новели стосувалися врегулювання питань транскордонної передачі персональних даних, істотного розширення прав суб'єкта ПД і спроби вирішення питання правових підстав оброблення ПД, із чим раніше виникали значні труднощі.

У доповіді правильно вказано щодо застосування Президентом України права вето[116], хочу лише додати, що це право було використане ним, зважаючи на пропозицію народних депутатів надати Державній службі захисту персональних даних повноважень у сфері їх стандартизації та сертифікації дій з оброблення ПД. З огляду на Закон «Про стандартизацію» і сучасну практику захисту ПД, що склалася у світі, зазначена сфера не може бути технічно врегульована. Ані про стандартизацію, ані про сертифікацію, ані про оцінку відповідності йтися не може, оскільки все це не гарантує дотримання жодних прав інших суб'єктів ПД.

Наступним етапом законодавчого вдосконалення стало ухвалення цього року Закону України № 2836[117] щодо інституційної системи. Експерти ЄС і Ради Європи від самого початку наголошували на низькому рівні незалежності й ефективності інституційної системи, оскільки Державна служба України з питань захисту персональних даних є урядовим органом, який координується Кабінетом Міністрів. З урахуванням практики Євросоюзу, зважаючи на Паризькі критерії, критерії

[115] Мається на увазі Проект закону України від 28.05.2012 р. № 10472-1 «Про внесення змін до Закону України «Про захист персональних даних» (щодо удосконалення правового регулювання у цій сфері)», який було прийнято Верховною Радою України 2 жовтня того ж року.

[116] Розділ III. – *Прим. ред.*

[117] Мається на увазі Проект закону «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» від 17.04.2013 р. № 2836, прийнятий Верховною Радою України та чинний в редакції від 03.07.2013 р. №383–VII. – *Прим. ред.*

Конвенції Ради Європи, а також нещодавньої практики Європейського суду було визначено, що недостатньо досконалими є у нас механізми призначення голови Служби, а також відсутній мандат його дії, тобто не забезпечується те, щоб на період свого головування він був справді незалежним і недоторканним і міг ухвалювати рішення без огляду на будь-що. Коли приймався перший Закон, уряд був свідомий того, що статус ДСЗПД не відповідає закладеним принципам, і було очевидно, що єдиним варіантом є призначення Уповноваженого Верховної Ради з прав людини. Проте у попереднього Уповноваженого не було достатньо бажання, щоб взяти на себе виконання зазначених функцій, але тепер домовленості досягнуто й ухвалено цей Закон.

Хотілося б звернути увагу й на інші важливі питання, вирішені завдяки ухваленню цього Закону. По-перше, скасування процедури державної реєстрації. Тут варто зазначити, що в цьому питанні ми випереджаємо Європу. Такої системи повідомлень жодна європейська країна ще не має, але новим Регламентом ЄС, який буде ухвалено після модернізації Конвенції Ради Європи, таку систему запропоновано. І всі експерти говорять, що вона буде запроваджена і в Європейському Союзі. З 1 січня 2014 р. Уповноважений Верховної Ради з прав людини буде встановлювати перелік процесів оброблення, про які він має бути повідомлений. Цей перелік не визначено Законом для того, щоб він був максимально гнучким і щоб Уповноважений мав змогу швидко реагувати на проблеми, які виникають у суспільстві.

Наступною нашою важливою новелою є розширення переліку вразливих ПД. Так само вони розширені відповідно до нової Конвенції, яка розглядається зараз у Консультативному комітеті Ради Європи, хоча принципові рішення з цих двох питань уже ухвалено. Список вразливих ПД (ст. 7 Конвенції) доповнений генетичними і біометричними персональними даними.

І, напевно, найбільше досягнення цього нового українського Закону – це зміна сфери його дії. Хочу нагадати, що перший Закон про захист ПД поширювався на діяльність з оброблення персональних даних лише в базах ПД, Закон 2012 р. розширив цю сферу дії до будь-якої діяльності з оброблення ПД, а новий Закон уже відповідає всім принципам демократичного суспільства, оскільки він надав право обробляти ПД (наскільки це необхідно в демократичному суспільстві) журналістам, творчим особам і фізичним особам. Також приведено у відповідність до європейських стандартів і випадки незастосування цього Закону: в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

І наостанок я хотіла б закликати розглядати процеси оброблення ПД, особливо в мережі інтернет, як сукупність заходів у сфері захисту

інформації і розглядати її з трьох аспектів – як нормативно-правову систему, як організаційну систему і як технічну систему.

ДУБОВ Д. В.:

У мене, до речі, виникло питання, коли йшлося про невідповідність інституційного положення ДСЗПД і необхідність передання цих повноважень Уповноваженому Верховної Ради з прав людини. Чи розглядалася можливість закладення в нову Конституцію окремого інституту, окремого прописування цієї структури?

ЗОЛОТАРЬОВА О. В.:

Так, така можливість зараз розглядається, ми всі свідомі того, що Уповноважений – це перехідний момент. І всі європейські країни, які йшли нашим шляхом, розглядали це як перехідний момент.

ПИЛИПЧУК Володимир Григорович,
директор Науково-дослідного інституту інформатики і права Національної академії правових наук України

Шановні присутні, моя колега дещо полегшила мій виступ, оскільки розкрила деякі системні моменти і міжнародно-правові аспекти, які я теж планував розглядати.

Я хотів би подякувати організаторам цього «круглого столу», оскільки, дійсно, його тема є досить актуальною на сьогодні й свідчить про те, що Україна переходить до другого (перший був пов'язаний з нарощуванням і розвитком ІКТ) етапу розвитку інформаційного суспільства – формування конкретних суспільних відносин в інформаційній сфері, виникнення потреби в їх регулюванні тощо. Це комплекс нових питань, які вимагають нового рівня обговорення.

Хотів би звернути увагу на те, що фахівці нашого інституту ще на початку 2000-х років брали участь у розробленні теоретико-правових основ захисту ПД і в тому числі пропонували створити спеціалізований державний орган у системі виконавчої влади в цій сфері. На жаль, це рішення було ухвалене лише 2010 р., і ми згаяли час, який могли б використати для вирішення різних інституційних питань, формування необхідної правової бази тощо.

Який стан ми маємо сьогодні? Колеги вже про це говорили... Риторичне запитання до всіх присутніх: чи знайдеться поміж них хоча б одна людина, яка достеменно знає, де саме, які саме, у якому обсязі зберігаються її ПД і як саме вони обробляються? Хто їх використовує, продає тощо? Є відповідь на це питання? Мабуть, ні. Тим часом ідеться про відомості, які безпосередньо стосуються кожного з нас, кожного громадянина України.

Приклади можна наводити до безкінечності, розглянемо лише один. Беремо телефонну компанію, що надає відповідні послуги. І ось ми знаходимо в інтернеті інформацію про користувачів цієї компанії з адресами, прізвищами, номерами телефонів тощо – це правильно чи ні? Мабуть, ні. Далі. Банк чи будь-яка інша комерційна структура, домовляючись з особою про надання послуг, у договірних документах завжди намагаються прописати право цієї структури самостійно, у повному обсязі володіти ПД своїх клієнтів, передавати їх третім особам тощо. Якщо ж особа відмовляється підписати в такій редакції цей договір, то її відразу обмежують у правах на отримання відповідних послуг. Це теж, мабуть, не зовсім правильний підхід, адже два суб'єкти договору як мінімум рівноправні.

Варто звернути увагу на рішення Національного банку України щодо збору персональних відомостей – ксерокопій паспортів у будь-якому обміннику. Наслідки вже відомі – коли ці самі ксерокопії використовуються для злочинних схем, у т.ч. отримання кредитів без відома особи тощо. Ще одна сумна подія – те, що стосується державних реєстраційних баз даних. Це відома тема, не буду її коментувати.

Тобто є комплекс різних питань, які потребують вирішення. З ними пов'язане ще одне системне питання: а чи є правильним наш підхід до розбудови інформаційних систем і баз даних? Більшість з них містить персональні дані. То чи мають вони бути жорстко централізовані, чи, можливо, варто запровадити інший принцип? Є підхід, апробований у державних органах і досить ефективно застосовуваний вже десятки років. Йдеться про автономну систему в регіоні та доступ до цих регіональних систем з центру. За таких умов якщо якась частина зазнає *DDoS*-атак чи здійснюються інші спроби знищити дані або заволодіти ними, загальноукраїнська система залишається «на плаву» незалежно від того, хто й якими силами намагається її знищити. Над цим варто замислитися ще й тому, що прагнення максимальної концентрації призводить до того, що базами даних усіх громадян України володіє декілька осіб. Це теж ненормально, коли немає перешкод впливу на них з метою скоєння тих чи інших правопорушень, порушень правил безпеки.

І ще, шановні колеги, я хотів би з вашого дозволу звернути увагу на деякі правові питання, законодавче регулювання. Наша Державна служба працює досить активно і в досить непростих умовах з моменту її створення – дійсно, тут необхідні й розуміння, й державна підтримка, й фінанси. Водночас Закон про захист персональних даних був прийнятий ще у 2010 році, і я абсолютно погоджуюсь із колегою, що він є результатом певного консенсусу, якого можна було досягти на тому етапі. Та давайте глибше проаналізуємо текст цього Закону: чи створює він необхідні передумови для захисту прав людини? На-

приклад, стаття 5 передбачає, що персональні дані є інформацією з обмеженим доступом. Автоматично постає питання: яким є правовий статус обмеження цієї інформації? Державна таємниця? Конфіденційна інформація? Правовий статус автоматично передбачає правові наслідки. Тоді це – рівень відповідальності, рівень захисту, рівень доступу тощо. А згідно із зазначеним документом це – лише декларація. Задекларовано положення про обмежений доступ, але фактично вільний доступ має досить широке коло осіб.

Друге питання: ст.ст. 6 і 14. Остання надає право обробляти та поширювати ПД без відома громадян в інтересах національної безпеки, економічного добробуту і прав людини. Тут є питання до змістової частини. Зокрема, інтереси національної безпеки сумнівів ні в кого не викликають, тут усе зрозуміло і врегульовано на рівні закону. Однак що таке економічний добробут у транскрипції цих статей? Чий це економічний добробут – держави, суспільства, фінансово-промислової групи, транснаціональної корпорації, якоїсь конкретної особи? Про що йдеться? В інших законах такий термін не використовується.

Ще одне посилання. Право обробляти та поширювати ПД без відома громадян в інтересах прав людини. Дещо колізійно звучить. Тут є предмет для роздумів, тому варто серйозно замислитися над деякими формулюваннями.

Те саме стосується ч. 5 ст. 11. Згідно з нею однією з підстав для оброблення персональних даних є необхідність захисту законних інтересів третіх осіб. І в контексті цієї статті права суб'єкта ПД, тобто права людини, по суті, перебувають на одному рівні з правами третіх осіб.

Стаття 19, по суті, створює мотивацію для продажу ПД. Застосовується поняття «плата за персональні дані». Наскільки це коректно? Адже це пряма підстава для бізнес-операцій у цій сфері.

І, нарешті, ст. 29, яка стосується міжнародних відносин. Я би звернув увагу на частини 3 і 4 цієї статті. Вони передбачають можливість передачі ПД іншим державам, але не встановлено жодних обмежень щодо отримання згоди громадянина на те, що його ПД будуть доступними за кордоном.

Я навів лише деякі приклади, шановні колеги. Ідеться про те, що Закон досить компромісно підготовлений, але якщо розглядати його історію, то за три роки до цього документа тричі вносилися зміни. Це ще раз підтверджує, що було зроблено те, що можна було зробити на тому етапі, але нині постає завдання рухатися далі. Ці зміни засвідчили необхідність подальшого руху. І до цього процесу слід долучатися фахівцям із ДСЗПД. Ми, зі свого боку, теж готові взяти участь у цій роботі задля подальшого законодавчого регулювання у зазначеній сфері.

БАРАНОВ Олександр Андрійович,
директор Департаменту стратегії розвитку зв'язку Адміністрації Державної служби спеціального зв'язку та захисту інформації України

Я хотел бы, во-первых, выразить благодарность Институту за то, что он периодически поднимает очень актуальные проблемы, которые имеют большой резонанс в нашей стране.

Во-вторых, что касается темы сегодняшней. Немного истории, особенно для специалистов из Министерства юстиции. Первая статья, появившаяся у нас в стране по теме ПД, была моей, и вышла она 14 июня 1996 г. 1 июня 2010 г. был принят Закон Украины «О защите персональных данных». Таким образом прошло 14 лет, в течение которых происходил непрерывный процесс осознания необходимости принятия такого закона в Украине. В 1997 г., работая в Национальном агентстве по вопросам информатизации при Президенте Украины, я инициировал создание законопроекта, и в 1999 г. он был подан на рассмотрение в Кабинет Министров как первый законопроект о защите персональных данных. Один из основных разработчиков сидит рядом со мной, это Валерий Михайлович Брыжко.

После первой подачи было получено более 200 замечаний различного характера от разных министерств и ведомств, в т.ч. и от Министерства юстиции, замечаний действительно конкретных, хороших. У нас была дискуссия с Министерством юстиции по поводу основной новеллы, которую мы предлагали: признания ПД каждого гражданина его собственностью. Мы предполагали, что в таком случае гражданско-правовые механизмы защиты прав и интересов граждан будут работать в полной мере. Тем более, что Гражданский кодекс изобилует нормами, которые де-юре это признают. Вы знаете, что по нормам Гражданского кодекса запрещено без согласия гражданина использовать его фотографию в любых целях. И сегодняшняя судебная практика Украины свидетельствует о том, что принят ряд соответствующих решений судов в пользу граждан и возмещен моральный ущерб за использование фотографий без согласия их владельцев.

И в первом законе, и в моей статье предлагалась двухуровневая модель, в которой первый уровень – нормативно-правовой защиты – предлагалось отдать Уполномоченному по правам человека, хотя на примерах других стран можно сделать вывод, что везде существует автономный институт Уполномоченного по защите ПД. Но поскольку было понятно, что в наших реалиях создать ещё один институт будет сложно (тем более учитывая то, что это конституционная норма), было предложено возложить все эти полномочия на Омбудсмена. Второй, очень важный, уровень, связанный с организационными вопросами

(технической защитой информации), предлагалось возложить на специальный орган. К сожалению, в той редакции Закона, которая увидела свет в 2010 г., это предложение о вовлечении в процесс защиты ПД Уполномоченного по правам человека исчезло буквально за два-три месяца до голосования, причём по настоянию именно представителей Уполномоченного в связи с тем, что они не захотели брать на себя эту ответственность.

Законопроект с 2002 г., с первого официального внесения его в парламент, трижды голосовался и трижды был принят. Дважды налагалось вето при непосредственном участии Министерства юстиции. Я беседовал практически со всеми министрами, действующими в то время, с заместителями министров, которые занимались этим вопросом, и с ныне исполняющей обязанности Уполномоченного, которая на последней стадии отвечала за принятие этого Закона.

Процесс принятия этого закона – ещё раз повторяю, 14 лет понадобилось для его осознания и принятия – был долгим, но, к сожалению, для общества он прошёл незамеченным. Многие критики Закона, которые спрашивают, что он дает простому человеку, абсолютно правы по той простой причине, что сам Закон и его принятие не создали действенной и эффективной системы защиты прав и интересов граждан при обработке их ПД. И тут следует говорить о том, что это связано с ущербностью Закона, который многие обязанности и полномочия возложил на орган, который де-юре не мог этого выполнить. И нынешняя новелла, с одной стороны, положительна, а с другой – абсолютно ошибочна. Я глубоко убеждён, что аппарат Омбудсмена не справится с теми задачами, которые на него возлагает Закон, в силу специфики его деятельности и той сферы регулирования, о которой идёт речь.

Что касается доклада, то я хочу отметить, что он достаточно полный, аргументированный, автор постарался сделать его многосторонним, но, по моему мнению, докладчик слишком увлекся «облачными» технологиями и даже ввёл такое понятие – «хмаровий» ринок України». Думаю, с терминотворчеством следует быть аккуратнее. Можно понять так, что кто-то торгует «облаками». На самом деле с точки зрения специфики защиты информации, защиты ПД «облачные» вычисления ничего не дают. Это технико-технологическая часть. Это специфика организации технической защиты информации. В нормативно-правовую область эта новая технология ничего не привносит. Все, что происходит в сфере компьютеров, сетей, для юристов *terra incognita*, в т.ч. «облачные» вычисления.

Но есть другая проблема, о которой мы еще не говорим, но которую уже обсуждает Европа. В 2010 г. была опубликована Рекомендация Комитета министров Совета Европы № 13 о защите частных лиц в связи с автоматизированной обработкой персональных данных в кон-

тексте профилирования[118]. Это одна из главных угроз сегодня – комплексирование данных, которые собираются в разных базах данных, в т.ч. незарегистрированных. Мы не даем согласия на то, чтобы сведения о нас там появлялись, но они там появляются. Это различные системы наблюдения, прохода, пропусков, регистрации в онлайн-магазинах и прочее. Комплексирование этих данных сегодня позволяет узнать о человеке всё, я подчеркиваю это слово – **всё**. Появилось достаточно много исследований, подтверждающих то, что в течение двух-трёх дней можно собрать о человеке абсолютно полную информацию – о его привязанностях, устремлениях, личной жизни и т.д. Более того, в этом году, 11 июня, Комитет министров Совета Европы принял Декларацию о рисках для основных прав человека, связанных с цифровым слежением и другими технологиями наблюдения. То есть пока мы отрабатываем то, о чём в Европе ещё в 1981 году была принята Конвенция[119], угрозы растут, и очень серьёзные, а мы об этом мало говорим.

Что касается в целом проблем в нормативной плоскости этой сферы в Украине, то, конечно, Закон «О защите персональных данных» принимался исходя из того, что он будет рамочным, а впоследствии появится достаточное количество специальных нормативных актов, которые определят и чувствительные данные, и особенности обработки ПД в банковской, правоохранительной сфере, сфере образования, медицины и т.д. Но ничего из этого не сделано. Как следствие, возникает много вопросов, в частности: что значит обработка ПД в интересах прав человека? А когда человек умирает, он ничего не может сказать, однако его данные заносятся в базы без его согласия. Именно это и имелось в виду, и в соответствующей Рекомендации Совета Европы по медицине это прописано.

И о новеллах. Уважаемые коллеги из Минюста! Я очень уважаю ваше ведомство, поскольку это одно из немногих ведомств, которое формирует и нашу правовую политику, и правосознание. Однако реляция о том, что благодаря новелле об отмене регистрации баз данных мы впереди Европы всей, – это неправильно. Надо учесть, что Европа вводит эту новеллу исходя из того, что у них уже сделано, из того, что у них воспитано отношение к защите ПД, из того, что во Франции до сегодняшнего дня ни одно юридическое лицо не имеет права даже начать работу по созданию базы ПД до тех пор, пока соответствующий орган

---

[118] Рекомендація № REC(2010)13 Комітету міністрів державам-членам Ради Європи про захист приватних осіб у зв'язку із застосуванням автоматизованого оброблення персональних даних у контексті профілювання [Електронний ресурс]. – Режим доступу: http://ciberpeace.org.ua/files/iii_6pdf (неофіційний переклад). – *Прим. ред.*

[119] Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, ухвалена 28 січня 1981 р. – *Прим. ред.*

не даст разрешение. То есть там уже есть культура, там сформировалось соответствующее правосознание, и поэтому эта новелла ложится на действительно хорошо проработанную почву. У нас при нашем правовом нигилизме и фактическом отсутствии системы защиты ПД эта новелла, на мой взгляд, только навредит.

В целом же то, что Институт поднял эту проблему, – очень важно и очень нужно. К ней следует подходить всесторонне, но прежде всего в двух плоскостях – нормативной и технической. Мы сегодня, насколько я понимаю, в основном обсуждаем первую.

ДУБОВ Д. В.:

Дякую, за Ваш як завжди ґрунтовний виступ. Ми сьогодні вже стільки разів згадали про безпеку, про загрози ПД, що, мабуть, логічно буде послухати того, хто безпосередньо займається вирішенням цих питань.

ПЕТРОВ Валентин Володимирович,
представник Служби безпеки України

Сергію Леонідовичу, хочу подякувати за ґрунтовну і змістовну доповідь, дійсно дуже цікаву.

Є декілька риторичних запитань. У нашій країні вибудовується відразу декілька систем захисту інформації. Є система захисту ПД, є система технічного захисту інформації... От читаю Закон України «Про захист персональних даних», відкриваю ст. 5: «Персональні дані є інформацією з обмеженим доступом», крапка. Відсилаюсь до Закону України «Про інформацію», згідно з яким інформація з обмеженим доступом є трьох видів: конфіденційна, службова або таємна. А база ПД якоїсь комерційної фірми? Скоріше за все, вона буде або службова, або конфіденційна, під дію зводу відомостей, що становить державну таємницю, вона не підпадає. Далі відкриваю базовий Закон України «Про захист інформації в інформаційних і телекомунікаційних системах», читаю ст. 8, де написано, що «інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації». А Закон України «Про захист персональних даних» і накази Міністерства юстиції, до речі, встановлюють вимоги щодо захисту ПД. І водночас у нашій державі є спеціальний уповноважений орган, який відповідає за організацію спеціального зв'язку та захист інформації, – ДССЗЗІ. Тобто ми вже маємо неузгоджені системи, у кожної з них є свої плюси, мінуси, вони можуть бути більш чи менш прогресивними, є питання і до Держспецзв'язку, і до комплексних систем, які зараз вибудовуються. Але в будь-якому разі ми вже маємо юридичну колізію:

до однієї бази даних одночасно мають застосовуватися дві правові системи. І якою з них керуватися, скажімо, правоохоронним органам у своїй діяльності?

Далі. Хто у нас сьогодні відповідає за захист персональних даних? Давайте порахуємо. Є таке японське прислів'я – у семи капітанів корабель неминуче розіб'ється. Так от, колеги з Мін'юсту нагадали, що саме їх відомство відповідає за формування державної політики у сфері захисту ПД. Це раз. ДСЗПД – два. Омбудсмен з'являється з нового року, теж за щось відповідає – три. Є Міністерство внутрішніх справ, у підзвітності якого зараз перебуває ст. 361-2 – «збут інформації з обмеженим доступом», тобто розповсюдження баз даних, – чотири. П'ять – це Служба безпеки України, на яку покладено завдання з контррозвідувального захисту інтересів держави у сфері інформаційної безпеки і насамперед захист баз даних державних органів. І Державна служба спеціального зв'язку та захисту інформації, яка є в державі спеціальним уповноваженим органом у сфері технічного захисту інформації, – шість. Не вистачає ще сьомого, щоб остаточно посадити на мілину наш корабель.

ЗОЛОТАРЬОВА О. В.:

Є ще Кабінет Міністрів, Верховна Рада і Президент. На практиці саме так і є.

ПЕТРОВ В. В.:

Так, є ще Генеральна прокуратура, яка здійснює загальний нагляд за законодавством. Можемо так і далі піти, на другий десяток, тоді наш корабель уже дуже глибоко сидить на каменях. І от, до речі, питання, яке нещодавно виникло щодо державного підприємства «Держінформ'юст». З повідомлень ЗМІ абсолютно незрозуміло, хто є володільцем баз даних, які оброблялися у цьому підприємстві. Начебто це державне підприємство, тобто мала б бути держава, або Мін'юст, або компанія «Артмастер», або офшор, який за нею стояв. Тобто постає дуже багато питань, але з'ясувати, хто саме володів цими даними і як саме вони оброблялися... Зараз крайніх знайти неможливо. Якщо підходити до баз цих даних як до баз ПД, то це має бути одна система, якщо як до інформації з обмеженим доступом – це вже зовсім інша правова система.

Тобто ми вдосконалюємо наше законодавство і рухаємося в певному напрямку, але при цьому треба узгоджувати різні системи, приводити до одного знаменника. Можливо, варто внести зміни до Закону України «Про інформацію» і визначити, що крім конфіденційної, службової і таємної, є ще персональна інформація, яка теж з обмеженим доступом, але проходить окремо, і виключити її з компетенції

Держспецзв'язку. Або, навпаки, долучити саме Держспецзв'язку до технічного захисту таких даних.

Це, власне, щодо нормативно-правової побудови системи захисту ПД в Україні.

ДУБОВ Д. В.:

Оскільки у нас уже висловилася держава, висловилася наука, я гадаю, саме час надати слово недержавним організаціям.

КОГУТ Юрій Іванович,
голова правління ВГО
«Українська асоціація захисту персональних даних»

Хотів би сказати, що не завжди працював у такій організації, як зараз. Був час, коли ми з паном Барановим створювали державну систему технічного захисту інформації. Це було в 1992 році. Я працював у Раді безпеки, а Олександр Андрійович був першим заступником цієї поважної структури. До появи України як незалежної держави захисту інформації надавалася першочергова увага. У Радянському Союзі ці питання вирішувалися на рівні державної технічної комісії, керівник якої мав ранг і повноваження віце-прем'єра. Коли Україна стала самостійною державою, був створений Апарат РНБО, і перше питання, яке тоді виникло, стосувалося створення державної служби з технічного захисту інформації. Вона була створена. І питання вирішувалося таким чином, що голова цієї служби повинен був за місяць розрахувати її структуру та штат, який би дав змогу захистити інформацію в державі. Було виділено особливо важливі об'єкти і чисельність персоналу було пораховано таким чином, щоб цей орган міг захистити інформацію. Було створено інспекцію, і все працювало.

Однак була одна проблема, про яку ми сьогодні забуваємо. Технічний захист інформації в Україні завжди починався з розроблення моделі загроз. Якщо ви хочете захистити дані, ви маєте точно знати, від кого і яким чином ви будете їх захищати. За відсутності таких відомостей робота із захисту стає неефективною. Ви просто не зможете побудувати ефективну систему захисту. В Україні розробленням моделі загроз займалися спеціальні органи, розвідка. У ній було прописано всі технічні розвідки іноземних держав, які мали своєю метою добування інформації в інших державах.

Що ми маємо сьогодні? Ми говоримо про захист інформації, але не уточнюємо від кого. Тому ми як асоціація спробували розібратися в загрозах безпеці персональних даних і виклали результати в книзі, яку сьогодні вам роздали. Вона називається «Кібертероризм і захист персональних даних». Ми намагалися систематизувати ці загрози

для ПД і, знаючи їх, з'ясувати, яким чином краще було б побудувати систему захисту персональних даних у державі.

Подібно до того, як це роблять колеги, я розділив би цю проблему на частини. А саме: на суто політичну частину, ту, яка стосується захисту прав людини (цим, безумовно, Омбудсмен має займатися), і технологічну частину, якою теж хтось має займатися, і ефективно займатися. Ефективно, оскільки комплексна перевірка різних державних систем здійснюється рідко. І якщо здійснюється, то цим займаються уповноважені державні органи, і тоді це відбувається коректно, спокійно, у межах якоїсь політики, концепцій, програм. А може здійснюватися стихійно. Стихійно, як ви пам'ятаєте, було перевірено систему ПВО Радянського Союзу. Взяв Руст і сів на Красній площі в Москві, і всім стало зрозуміло, що система ПВО в країні не працює.

Так само і система технічного захисту інформації в Україні працювала чудово, доки не прослухали кабінет Президента. Тоді стало всім зрозуміло, що, мабуть, у системі є проблеми. Не все відпрацьовано на рівні нормативних документів, не все гаразд на рівні державних систем і структур, які мали б цим займатися.

Сьогоднішня проблема з реєстрами теж висвітлила низку питань, які в державі не вирішені, і їх, мабуть, треба вирішити. І для того, щоб їх вирішити, необхідно створити систему, яка б ефективно працювала у сфері технологічного захисту ПД.

Разом з цим згідно з новим законом відповідальним за захист ПД визначено Омбудсмена, і там же зазначено, що введення цього закону в дію не потребує ніяких додаткових бюджетних витрат. Але ж це нонсенс. Не може Омбудсмен, не маючи штату, не маючи кваліфікованого персоналу, виконувати покладені на нього функції. Та й сьогоднішня Державна служба із захисту персональних даних розташована тільки в Києві, а ми маємо ще 27 регіонів в Україні. Що з ними робити? Хто це має робити? Незрозуміло.

Відповідна акція була проведена у Верховній Раді влітку, коли обговорювалося питання реєстрів, і вів цей захід народний депутат Вадим Колесниченко. Я його запитав, чи знає він, скільки існує в різних регіонах конфесій, які цікавляться персональними даними. Він відповів, що, мабуть, їх існує декілька, я тоді зауважив, що тільки в Криму є півтори тисячі конфесій. Причому з них православних, таких, які працюють, сказати б, у руслі державної політики, – одиниці. Усі інші – це реакційні структури, які, зокрема, дуже цікавляться збором ПД і які якщо не сьогодні, то завтра працюватимуть *не* в руслі державної політики.

Тому потрібно виділити об'єкти інфраструктури, розділити питання розроблення законів і питання технологічні. А для того, щоб вирішити питання технологічні, необхідно створити відповідну систему і

порахувати, які кошти для неї мають бути виділені. Причому вирішити це питання можна тільки в межах інтересів державних. Інші інтереси сюди закладати не потрібно. Політики нехай конкурують з різними законопроектами, але ті питання, які стосуються національної безпеки, мають бути вирішені коректно і з відповідними розрахунками. А закон, у якому прописано, що ПД будемо захищати, але кошти для цього не потрібні, захищати персональні дані ніколи не буде.

Ще раз хочу подякувати за запрошення і нагадати, що своє бачення всіх цих моментів ми виклали у брошурі, яку вам роздано. Будемо вдячні за коментарі та критику.

ДУБОВ Д. В.:

Ми багато говорили про законодавчі основи, про юридичні нюанси, але все одно це, зрештою, проходить через Верховну Раду. А у нас сьогодні присутні два представники від Верховної Ради, від профільних комітетів, які займаються цими питаннями.

СЕЛЕЦЬКИЙ Петро Іванович,
головний консультант секретаріату Комітету Верховної Ради України з питань свободи слова та інформації

Я відчув, що настав момент сказати кілька слів щодо тих питань, які ми сьогодні обговорюємо. Річ у тім, що, говорячи і про правові, і про технологічні аспекти захисту ПД, ми не маємо права абстрагуватися від положень тих законів, які забезпечують інформаційні права наших громадян. Я маю на увазі закони України «Про інформацію» і «Про доступ до публічної інформації». Тільки в контексті цих двох базових законів ми можемо говорити про захист ПД. Як би ми не хотіли перекрити, заборонити, встановити якісь бар'єри в доступі до ПД, сьогодні це ані технологічно, ані законодавчо неможливо. Основними причинами цього є стрімкий розвиток інтернет-технологій і наше бажання знати, бачити, бути, втручатися. І не можна забувати, що Україна, просуваючись до Європи, зробила багато відкриттів. Відкриваючи світ, вона сама відкривається світові. Принципи прозорості, відкритості є одними із визначальних аспектів того, що відбувається в правовому полі.

Тиждень тому відбувся IV Інтернет-форум, на якому багато говорили на цю тему, але треба виокремити два дуже важливі моменти. Перше. Інтернет в Україні сьогодні розвивається випереджальними темпами, Україна набагато швидше, ніж Європа і більшість країн Азії, крокує до глобального, сказати б, охоплення інтернет-технологіями, до їх присутності в усіх сферах нашого життя. Причому вони зростають як кількісно, так і якісно. Друге. З'являється дедалі більше людей, здатних не лише створювати *IT*-системи, а й «ламати» їх, розкривати. І методом заборон тут нічого не вирішиш. Є низка пропозицій щодо ви-

рішення цього питання: за допомогою саморегулювання, більш активного розвитку законодавчої бази (дійсно, сьогодні наше законодавство відстає, і це всі визнають). Але тут прозвучала і дуже слушна думка про те, що ЄС нині теж констатує недосконалість своєї бази, хоча ще вчора ми сподівалися, що якщо нам вдасться все європейське імплементувати, то ми перекриємо можливості для зловживань. На жаль, на це розраховувати не доводиться.

Як сьогодні законодавець до цього всього підходить? Треба всі свої зусилля спрямувати не на те, щоб обмежити доступ, а на рішучу протидію спробам діяти несанкціоновано, всупереч закону. Так, як борються, наприклад, із порнографією в інтернеті. Певні успіхи в цьому напрямі є. Отже, є і технологічні, і правові підстави говорити про те, що в цьому самому ключі можна буде вирішувати питання захисту ПД, але тільки з урахуванням принципів відкритості і прозорості. Тому що під приводом захисту можна різним чином зловживати, і все виглядатиме так, ніби ми захищаємо права людини. Оскільки в Конституції України записано, що права людини є визначальними щодо політики держави, треба, щоб з цього питання була повна ясність.

Кілька слів про ті тенденції, які існують сьогодні в роботі нашого Комітету. Закон «Про доступ до публічної інформації» нині є на стадії узгодження з рештою законодавчої бази, є низка колізій, які необхідно подолати. Сподіваємося, що законодавець піде на те, щоб якнайшвидше усунути ці колізії, і всі норми, передбачені зазначеним Законом, поширити на все правове поле. На мою думку, в цьому зацікавлене суспільство.

Існує й інша тенденція, яка випливає з інтересів певних груп: під приводом захисту ПД взагалі нейтралізувати дію Закону України «Про доступ до публічної інформації». Гадаю, в історичній перспективі ці спроби приречені на невдачу, але сьогодні свідченням цього процесу є Законопроект № 3301[120], у якому пропонується обмежити доступ до будь-яких ПД. Є й рішення Конституційного Суду, яке певною мірою впливає на це питання.

Вважаю, що не помилюся, якщо скажу, що Україна перебуває на початковому етапі формування інформаційного суспільства, але етап формування громадянського суспільства вже завершився. Сьогодні ми маємо достатню кількість активних експертів із громадськості, які активно впливають на зазначені процеси, і свідченням ефективності цього впливу є історія згаданого Законопроекту № 3301. Відомо, яке широке обговорення відбувається в нашому інформаційному просторі

[120] Мається на увазі Проект закону «Про внесення змін до Закону України «Про доступ до публічної інформації» (щодо удосконалення окремих процедур)», зареєстрований 20.09.2013 р. – *Прим. ред.*

з цього питання. Нині є вагомі підстави говорити про те, що цей Законопроект буде якщо не повністю відхилений, то принаймні перероблений, пом'якшений.

Отже, йдеться про те, що ми не можемо стати на дорозі цього потяга, який називається «інформаційне суспільство», ми повинні просто врахувати, використати, іти далі, розвиватися і вміти протидіяти тим реальним загрозам, які виникатимуть у процесі цього нашого поступу.

ЦАРУК Олександр Васильович,
головний консультант секретаріату
Комітету Верховної Ради України
з питань інформатизації та інформаційних технологій

Продовжуючи обговорення, я хотів би задати питання Державній службі з питань захисту персональних даних. Я знаю, що були спроби розслідування питання збору та передачі ПД однією з великих закордонних пошукових систем. А також я бачу, що серед запрошених є представник однієї з російських пошукових систем, яка за принципом своєї роботи абсолютно нічим не відрізняється. Запитання: чи Служба домоглася якогось успіху в розслідуванні цього питання? Я хотів би подати таку інформацію.

Наш Комітет працює трохи менше ніж рік, і в предметах відання в нього прописаний захист інформації та ПД в інформаційно-телекомунікаційних системах. Тобто якщо порівнювати критику уряду щодо відповідності захисту і регулювання питання ПД, то в українському парламенті ситуація набагато простіша. Відповідно, стратегічними, загальними підходами до цих суспільних відносин займається Комітет Верховної Ради України з питань свободи слова та інформації, а технологічним складником – наш Комітет. Також у нашому Комітеті на розгляді, на стадії до першого читання, перебуває Законопроект № 2207а щодо проблем кібернетичної безпеки України[121]. Наш Комітет визначено як основний щодо його розгляду. Користуючись нагодою, закликаю фахівців здійснити глибоку експертизу цього Законопроекту, тому що він надзвичайно складний і вперше порушує таке важливе для безпеки країни і сфери ІКТ питання. Він поки що існує у формі рамочного законопроекту, але вже звучать численні побоювання, що він може призвести до цензури, надмірного регулювання інтернету, порушення прав особи тощо. Тому було б цікаво, можливо, в рамках експертної ради, яка створена при Комітеті, обговорити це питання.

Що стосується проблематики ПД і «хмарових» технологій, про яку кілька учасників нашого «круглого столу» теж сьогодні говори-

[121] Мається на увазі Проект закону «Про кібернетичну безпеку України», зареєстрований 04.06.2013 р. – *Прим. ред.*

ли. У мене була нагода влітку та восени цього року відвідати два досить цікаві заходи – літню школу з управління інтернетом у Мейсені, Німеччина (це такий європейський оплот «мультистейкхолдеризму» щодо управління інтернетом) і конференцію у Страсбурзі щодо транспарентності інтернету. Яких основних висновків я дійшов, відвідавши ці два заходи? Перше. Зараз у кіберпросторі триває війна між ТНК, які контролюють більшість інтернету і більшість «хмар», а отже, контролюють ПД і оперують відповідною інформацією для рекламних цілей.

Отже, запитання: чи цікавилася ДСЗПД або інші державні органи, які вивчали це питання, скільки було показано контекстної реклами та банерів всіма пошуковими системами, скільки було переходів і скільки перераховано до державного бюджету коштів як плата за надання рекламних послуг на території України? У 2011 році я як незалежний дослідник опублікував на одному з фінансових порталів України дослідження-порівняння економічної природи віртуальної валюти «мавро», яку вигадав Сергій Мавроді у своїй новій «піраміді», з титульними знаками однієї з платіжних онлайн-систем, що контролювала 80 % ринку онлайн-платежів України. Після цього представник цієї платіжної системи в Україні заявив мені, що вони позиватимуть на мене до суду. Я подякував за рекламу, пізніше вони передумали. Але за рік їх закрили. Так от: що робитимуть державні органи з онлайн-сервісами в інтернеті, які мають багатомільярдні обороти, і що вони сплачують до державного бюджету? Чи виконують вони норми Податкового кодексу, згідно з якими представництво іноземної компанії, яке надає відповідні послуги з оборотом понад, здається, 500000 грн, зобов'язане сплачувати податки на загальних підставах?

Тобто є ТНК, які обстоюють свої комерційні інтереси, прибутки, вплив. Інша модель – це модель ООН. Нині існує протистояння між Міжнародним союзом електрозв'язку, який діє під егідою ООН, є міжнародною організацією і який намагається взяти під контроль управління інтернетом і корпорацією *ICANN*, яка обстоює ідеї «мультистейкхолдеризького» підходу щодо управління інтернетом, у якому голос держави – дорадчий.

По суті, різні стейкхолдери – асоціації, корпорації, наука та інші організації – зараз керують доменною індустрією у світі, видають відповідні ліцензії на домени верхнього рівня. Тож зрозумілим є занепокоєння Європейської Комісії тим, що, наприклад, ліцензії на домени видає американська корпорація, зареєстрована в Каліфорнії, яка має імперативний контракт з Державним департаментом торгівлі США і Рада директорів якої формується навіть не з представників держав, а з мультистейкхолдер-ком'юніті. І у Страсбурзі це питання обговорюється дуже активно.

Тепер. Як стейкхолдери трактують питання «хмарових» технологій. Адепти «мультистейкхолдеризького» підходу обстоюють неможливість т.зв. балканізації інтернету, за якої кожна країна намагатиметься створити власну національну чи регіональну «хмару» і дані електронної пошти, реклами, *cookies* тощо зберігатимуться виключно на цій території. У результаті глобальна компанія не зможе отримати доступ до них, проте його зможе отримати локальна служба, яка відповідає за пошук даних. І саме в цьому руслі відбувається дискусія, оскільки невеликим країнам такі «хмари» абсолютно недоступні, тому що це високотехнологічне рішення, і керувати переданням і обробленням великих обсягів даних для бідних корпорацій чи країн абсолютно недоступно.

Однак велике об'єднання країн зацікавлене у своїй кібернетичній безпеці і занепокоєне тим, що представники однієї з найбільших країн світу можуть отримувати доступ не лише до їхніх ПД, а й до корпоративних даних їхніх підприємств, можливо, з метою корпоративної розвідки. У цьому аспекті можна зрозуміти, чому ж у Європі так стурбовані «хмаровими» обчисленнями: по-перше, це багатомільярдний ринок інформаційних і рекламних послуг, по-друге, це безпека країни.

І тут постає запитання: яку модель Україна обере для себе, зважаючи на свої реалії, обмеження і дійсний стан розвитку ІКТ? Які є пропозиції щодо того, як управляти інтернетом, і чи потрібно нам, хоча б виключно для державних органів, зберігати дані електронної пошти, реєстрів тощо в надзвичайно безпечних системах чи можна цей сервіс придбати в *Amazon.com* за копійки і заощадити мільйони бюджетних коштів?

ДУБОВ Д. В.:

Запитання прозвучало, але представника Міндоходів серед присутніх немає, тому, гадаю, на фінансову частину питання навряд чи хтось Вам відповість. Однак відповідь щодо ПД, напевно, буде. Костянтине Сергійовичу, прошу Вас.

МЕЛЬНИК К. С.:

Я хотів тільки уточнити. Ви мали на увазі пошукову систему *Google*?

ЦАРУК О. В.:

Я спеціально не називав імена, тому що вони відразу готові позивати до суду за наклеп.

МЕЛЬНИК К. С.:

Питання щодо перевірок ДСЗПД є відкритою інформацією, яка розміщується на веб-сайті Служби. Це по-перше. По-друге, я хотів

би зробити дуже важливе зауваження: ми не перевіряли пошукову систему. Ми перевіряли ТОВ «*Google*-Україна», яке жодного стосунку до пошукової системи *Google* не має. Щодо того, які результати були досягнуті, скажу так: самі результати є службовою інформацією, але в загальному вимірі можу повідомити, що було видано припис щодо усунення порушень законодавства, в яких ознак адміністративного порушення або ознак злочину встановлено не було. Термін виконання припису – 23 жовтня 2013 р., і, наскільки мені відомо, ТОВ «*Google*-Україна» вже вчора надіслало результати виконання припису.

БРИЖКО Валерій Михайлович,
керівник центру проблем методології інформаційного права Науково-дослідного інституту інформатики і права Національної академії правових наук України

Можно добавить, что фактически Закон разрабатывался с 1996 г., когда Александр Андреевич приехал из Москвы и привез книгу Копылова. В течение всех этих лет, до 2010 г., когда был принят Закон, периодически менялись руководители министерств, а как только происходит смена руководства, начинается и смена низшего звена. И начинается переписывание. Было восемь версий Законопроекта. В 2006 г. за него дважды голосовала Верховная Рада. И мы решили, что с 2007 г. Закон «пойдет в жизнь». Но вдруг ни с того ни с сего он куда-то «исчез». И опять началось переписывание. И если бы не усилия Жиляева, Баранова, других представителей Комитета науки, наверное, мы бы до сих пор были без Закона.

Что касается Минюста, я ничего плохого не хочу сказать, но несколько человек на основании наших работ защитились. Сейчас они говорят, что мы впереди планеты всей (в вопросе регистрации баз ПД). Да вы посмотрите: 40 стран мира регистрируют базы ПД. О чём мы говорим? Вопрос в другом: как и что мы собираемся регистрировать?

Второе. Кто-нибудь знает, что на Западе, где каждая страна имеет закон о защите ПД или о защите данных, введено лицензирование прав на ПД?

И третий момент. В Законе «О защите персональных данных» есть ст. 8 – о правах субъекта ПД. И есть статья Гражданского кодекса, кажется, 200-ая. Там написано: «особисте немайнове право на персональні дані». А что, персональные данные не продаются? Вдумайтесь, какой нонсенс! И он существует многие годы. Поэтому в первой версии мы и предлагали ввести имущественные права на ПД, до конца дрались, но Минюст был категорически против. Он боится трогать этот Гражданский кодекс «прекрасный». Но ведь вовсю идет торговля! На Западе маленькая база ПД стоит полторы-две тысячи, а вообще

до десятков тысяч цена доходит. То есть персональные данные имеют экономическую цену, и надо с этим разбираться.

А теперь вернемся к более высоким категориям. Что такое ЕС? Это конгломерат, в который сейчас Украина энергично движется. И какие же он преследует цели? Цели экономические, больше ничего. Далее. Что такое Совет Европы? Это конгломерат, который пытается поднимать (и поднимает) вопросы основополагающих прав и свобод человека. То есть, с одной стороны, мораль, с другой – экономика. Как соединить слона и трепетную лань? Очень сложно. Таким образом, проблема защиты данных – это дилемма, сопровождающая поиск оптимального варианта.

Есть две составляющие проблемы. Первая – нормативная. Мы всегда говорили, что создавали рамочный закон, и везде писали: давайте разработаем именно рамочный закон, а потом по отраслям будут приняты отдельные законы, в которых будут учтены все нюансы. Так и делается в Европе. Так вот, украинский Закон уже в 2010 г. отвечал европейским правовым стандартам. И хотя законодатели его тогда подрезали, подрубили, убрали, в частности, право собственности человека на его ПД, Закон по-прежнему соответствовал норме, и это необходимо понимать.

А вот вторая составляющая защиты ПД у нас не работала, не работает и работать не будет. Эфемерность защиты ПД... У нас создаются структуры, передаются полномочия, а на самом деле ничего не решается. Вот сейчас передали эти полномочия Омбудсмену, а что это за должность? Это не в её компетенции. Потому что в ЕС есть комиссар по защите данных, а в Совете Европы – Омбудсмен и комиссар по защите персональных данных. Оба защищают ПД. Однако один защищает с точки зрения экономики, а второй – с точки зрения прав и свобод человека. И это перетягивание одеяла у них происходит постоянно, с 1981 г., со времени принятия Конвенции. И в этом документе правильно написано, что уполномоченный по ПД не должен подчиняться никакому государственному органу, тем более Омбудсмену. Так вот, эта административно-организационная составляющая у нас – больной вопрос, с ним надо серьезно разбираться. Но мы тут можем сидеть и разбираться, выдумывать, а на смену тем, кто принимает решения, придут новые люди и начнут принимать новые решения, не зная тех, которые уже принимались ранее. И это может продолжаться бесконечно.

Принимать решение необходимо, но не здесь, в Украине. Надо ехать в Германию, в землю Гессен, где ещё в 1970 г. был принят первый в мире Закон о защите ПД. У них 18 федеральных земель, и в каждой сегодня есть собственный такой закон да ещё общий федеральный Закон сверху. И не начальники, которые впоследствии бу-

дут далеки от этого, должны ехать знакомиться с этим опытом. Необходимо собрать серьезный коллектив порядочных, неглупых людей и дать им возможность ознакомиться с лучшим практическим опытом того, как надо защищать ПД. Хотя мы знаем, что в Европе, в той же Германии, тоже бардака хватает, но у них есть опыт, есть дух подчинения закону.

БЄЛЯКОВ Костянтин Іванович,
завідувач наукового відділу правових проблем інформаційної діяльності Науково-дослідного інституту інформатики і права Національної академії правових наук України

Я тоже очень пессимистически смотрю на проблему защиты ПД в Украине и в этом вопросе согласен с Валерием Михайловичем: у нас не существует ни правового, ни организационного механизма защиты ПД. Какие бы хорошие законы мы не разрабатывали, они реализовываться не могут. Поясню свой тезис. Я более масштабно (и тоже пессимистически) смотрю на проблему информатизации Украины, отдельной составляющей которой является вопрос защиты ПД в киберпространстве. Я коснусь некоторых технологических моментов, поскольку эта проблематика также заявлена в теме «круглого стола».

Этой весной я присутствовал на «круглом столе», организованном ДСЗПД, и там эксперты ЕС делились своим опытом. Я задал вопрос: «А как у вас решается проблема цифровой подписи?» И докладчик, не ответив на мой вопрос, корректно перевёл разговор на другую тему. То есть эта проблема, очевидно, у них тоже не решена. А ведь говоря о персональных данных в киберпространстве, мы не имеем права не говорить о решении проблемы цифровой подписи и электронного документооборота, потому что именно здесь находятся источники утечки информации. Без цифровой подписи говорить всерьез о защите ПД технологически смешно.

Вторая проблема ещё более глобальна – это вопрос создания собственного программного обеспечения, так называемой операционной платформы. Здесь вообще парадокс, в том смысле, что мы всегда говорим, что современная кибернетика родилась в Украине, в институте имени В. М. Глушкова. Это справедливо, и мы считаем, что наряду с США мы здесь основатели. Что же происходит дальше? Говорят, нет денег, а между тем на информатизацию ушло 4 или 5 миллиардов. Это бешеные деньги.

Третий, организационный, аспект: субъекты защиты ПД. Если рассматривать последние события – с ЕДАПСом, с Минюстом, – мы везде видим коммерческие структуры. Почему коммерческие структуры являются владельцами массивов данных государственного назначения? Хотя в тех же коммерческих структурах работают те же одарённые

люди, из института Глушкова в том числе, которые имеют своё ноухау в виде программного обеспечения. И почему бы государству этим не заняться? А потому, что якобы нет денег.

В заключение приведу тезис из одной хорошей статьи, которую сейчас читаю: «Политическая воля к разработке проектов информатизации многократно демонстрировалась. Однако её не нашлось для реализации этих проектов».

ДУБОВ Д. В.:

Касательно нашего доклада – почему там не нашла своего отображения, в частности, проблема электронно-цифровой подписи и прочие вопросы? В первую очередь потому, что мы сосредоточились на отдельно взятой проблеме. Однако в позапрошлом, кажется, году мы специально проводили «круглый стол» по ЭЦП и СЭД – системам электронного документооборота. Поскольку упомянутый Институт кибернетики имени В. М. Глушкова представлен на нашем «круглом столе», то хотел бы предложить его представителю озвучить их позицию относительно обсуждаемого вопроса.

ФАЛЬ Олексій Михайлович,
провідний науковий співробітник Інституту кібернетики імені В. М. Глушкова Національної академії наук України

Так, я провідний науковий співробітник Інституту кібернетики імені В. М. Глушкова Національної академії наук України, але зараз я хотів би виступити як член підкомітету захисту інформації технічного комітету інформаційних технологій.

Сьогодні ніхто не згадував про важливість стандартів, особливо в технологічному аспекті, а також про важливість їх розроблення. На жаль, нині в Україні щодо цього дуже погані справи. У міжнародному комітеті при *ISO* існує підкомітет захисту інформації, а в ньому – робоча група, яка відповідає за *privacy*, тобто забезпечення невтручання в особисте життя. Там на сьогодні вже є дуже багато напрацювань, складено дорожню карту, плани, велику кількість стандартів випущено. І заплановано їх теж багато, особливо з погляду управління інформаційною безпекою, у т.ч. інформаційного захисту ПД. Тут згадувалося, що в Україні є Комплексна система захисту інформації, а в міжнародному масштабі дуже важливу роль відіграє стандарт 27001, який так і називається – «Менеджмент інформаційної безпеки». 1 жовтня прийнято його нову редакцію – 27001 і 27002. Перший документ – це вимоги, а другий – рекомендації, вибір заходів, необхідних для виконання цих вимог.

На базі цих стандартів відбувається сертифікація систем управління в організаціях. Вони поєднують широке коло питань, як ор-

ганізаційних, так і технічних, і є дуже корисними. Особливо підхід, пов'язаний з оцінюванням ризиків. Є окремий стандарт, який називається *Privacy Impact Assessment*, тобто оцінювання ризиків у питаннях *privacy*.

Хотів би також підкреслити, що розрізняють питання *security* – безпеки і питання *privacy*. Якщо безпека стосується переважно ресурсів організації, то *privacy* – це якраз захист суб'єктів ПД. Однак вони поєднуються довкола питань безпеки ПД: у доповіді було правильно сказано, що один із принципів – це принцип захисту персональних даних у системах.

Загалом зараз уже є дуже багато напрацювань, і я вважаю, що необхідно порушити ці питання в Україні і знайти ресурси для дії зазначених міжнародних стандартів. Вони дуже корисні.

ГНАТЮК С. Л.:

Скажіть, будь ласка, а в Україні бодай якусь роботу вже розпочато? Я знаю, що за деякими локальними, галузевими, стандартами, наприклад, за «хмаровими» технологіями, стандарти *ISO* лише на кінець 2014 р. обіцяють. А українські стандарти? Просто уточнюю. У мене є деяка інформація, але цікаво почути фахівця.

ФАЛЬ О. М.:

Ні, разом із Службою ми розробили стандарт 29100, і я був науковим керівником розробки; він називається *Privacy framework*, тобто основні положення захисту. Зараз відбувається його затвердження, і цей процес є дуже непростим. Рік тому ми його підготували, і рік знадобився, щоб його просунути і затвердити. Труднощі виникають постійно. Про «хмари». Зараз є міжнародний проект, спеціально щодо вибору заходів для «хмарових» обчислень – 27018. І ще є деякі, їх чимало. Але якщо Вам потрібно, я можу цю інформацію Вам надати.

КУКАРІН Олександр Борисович,
заступник завідувача кафедри інформаційної політики та технологій Національної академії державного управління при Президентові України

Було надано перелік усіх трьох аспектів, але якщо не буде четвертого – кадрового, то про всі інші можна забути. Кадри вирішують усе. Тут йшлося про освічених, талановитих. Наш навчальний заклад – Національна академія державного управління – готує такі кадри. Зокрема, у нас вперше в Україні відкрито підготовку за спеціальністю «Електронне урядування». Ми системно всьому цьому навчаємо. Тут розповідали, як розроблялася законодавча база, – ми

теж брали в цьому участь. У нас на експертизі був пакет цих трьох законів. Я набирав особисто 26 сторінок порівняльних таблиць. Дещо, зрештою, врахували – тож є внесок. І у майбутньому ми теж готові брати участь у робочих групах, таких нарадах тощо.

ДУБОВ Д. В.:

Дякую за Ваші уточнення з цього питання. Сподіваюся, що всі, хто бажав сьогодні висловитися, мали таку можливість. Щиро дякую всім за виступи.

ЗМІСТ

Аналітична доповідь

Матеріали засідання «круглого столу»

Наукове видання

Серія «Інформаційні стратегії». Випуск 3

ГНАТЮК Сергій Леонідович

ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СУЧАСНОМУ КІБЕРПРОСТОРІ: ПРАВОВІ ТА ТЕХНІКО-ТЕХНОЛОГІЧНІ АСПЕКТИ

Аналітична доповідь

Літературні редактори: *І. С. Сандул, І. О. Коваль*
Коректори: *І. С. Сандул, І. О. Коваль*
Комп'ютерне верстання: *Є. Ю. Стрижеус*

Відповідальна за випуск: *І. О. Коваль*

Оригінал-макет підготовлено
в Національному інституті стратегічних досліджень:
вул. Пирогова, 7-а, Київ-30, 01030
Тел/факс: (044) 234-50-07
e-mail: info-niss@niss.gov.ua

Формат 60х84/16. Ум. друк. арк. 5,35.
Тираж 200 пр. Зам. № 500.

ДП «НВЦ «Пріоритети»
01014, м. Київ, вул. Командарма Каменєва, 8, корп. 6
тел./факс: 254-51-51

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
ДК № 3862 від 18.08.2010

ДЛЯ НОТАТОК