програмним забезпеченням) [5, с. 9]. Подальший розвиток інформаційного суспільства на вітчизняних просторах, впровадження та розробка сучасних інформаційно-комунікативних технологій уможливить ефективне формування національної моделі електронного бізнесу з урахуванням вже існуючого позитивного досвіду інших країн у цій сфері.

У цьому контексті важливо акцентувати увагу на тому, що оскільки питання економічного розвитку, надання відповідних дозволів тощо знаходиться у розпорядженні органів публічної влади, то серед першочергових завдань постає інтеграція та систематичне оновлення інформаційно-комунікаційних технологій у роботі органів державної влади та органів місцевого самоврядування.

Розглядаючи якісно нову роль економічної системи суспільства як важливого елементу для забезпечення національної безпеки, необхідно усвідомити, що ми наближаємося до принципово нових форм взаємовідносин в умовах яких підхід до подальшого використання власності (основи сучасної економічної системи) визначатиметься не статками окремих осіб, а призначенням для задоволення суспільних потреб.

Таким чином, тематика наукового пізнання економічної системи як важливого елементу забезпечення національної безпеки України має визначну теоретичну та прикладну роль й зосереджує політико-правові аспекти науки теорії держави і права та галузевих юридичних наук. Сьогодні як міжнародна спільнота, так і українське суспільство в активному пошуку та процесі модернізації більш ефективної моделі економічної системи з метою створення економічного балансу соціального розвитку. Існування різних форм власності, забезпечення, охорона, повага суспільства та влади до приватної власності, демократичні ринкові відносини є умовами ефективного забезпечення національної безпеки. Інформаційні та комунікаційні технології стали основою формування нового типу економіки – «кіберекономіці», у зв'язку з наданням унікальних можливостей в області пересування капіталу, товарів і послуг. Сучасна економічна система суспільства України змушена пристосовуватися до інформаційної та комп'ютерної реальності. Світові тенденції зумовлюють здійснити інноваційно-структурну перебудову вітчизняної економічної системи суспільства, оскільки сьогодні відсутність вказаного значно послаблює позиції системи національної безпеки України.

1. Система менеджменту інституціональної трансформації економіки України (теоретико-методологічний аспект): [колективна монографія] / [О. Д. Гудзинський, С. М. Судомир, Ю. С. Гудзинська та інші]; за заг. ред. О. Д. Гудзинського Київ: Аграр Медіа Груп, 2012. 771 с.

2. Гудзинський О. Д., Судомир С. М. Розвиток соціально-економічних систем в умовах структурної трансформації економіки України. *Збірник наукових праць Таврійського державного агротехнологічного університету (економічні науки).* 2017. № 1-2. С. 25-31.

3. Соціально-економічний потенціал сталого розвитку України та її регіонів: вектори реального поступу : національна доповідь. За ред. Е. М. Лібанової, М. А. Хвесика. Київ: ДУІЕПСР НАН України, 2017. 864 с.

4. Єфремова К. В. Державна політика та електронний бізнес в Україні. *Право та інновації.* 2015. № 1. С. 50-54.

5. Воробйова О. П. Впровадження електронного бізнесу в Україні: державно-управлінський аспект: автореф. дис. ... канд. наук з держ. упр. Київ, 2013. 20 с.

6. Ситник І. П., Головіна А. В. Електронний бізнес і його розвиток в Україні. *Молодий вчений*. 2016. № 2. С. 79-82.

Ядловська Ольга Степанівна
доцент кафедри
соціально-гуманітарних дисциплін
Дніпропетровського державного
університету внутрішніх справ,
кандидат історичних наук

ШЛЯХИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ

Протягом останніх десятиліть основним джерелом спілкування стають соціальні мережі за посередництвом різноманітних технічних можливостей через мережу Інтернет. Такий прогрес спричинив фактично інформаційну революцію та значно наблизив користувачів одне до одного, також передача інформації за змістом, обсягом, якістю стала надзвичайно мобільною та швидкісною, що сприяє розвитку ділових стосунків, відслідковуванню інформації, перевірці на достовірність. Разом з тим, виникла нагальна потреба захисту персональних даних як у розрізі використання особистої інформації, так і даних певного підп-

риємства. Постійною є необхідність захисту даних у соцмережах, що транслюють особисті дані, дані компанії, до якої відноситься користувач, зміст діяльності та дозвілля, поле друзів (контактів) і, найголовніше, − персональна інформацію, яка може бути використана сторонньою організаціє чи под. У цілому, існує ряд законодавчих ініціатив щодо захисту персональних даних. Однак технічно цим питанням займаються саме ті особи (підприємства), які володіють акаунтами, сайтами, профілями.

Метою статті є необхідність окреслити основні шляхи захисту персональних даних в соціальних мережах та необхідність популяризувати обов'язкове впровадження захисних систем та шляхів захисту.

Розвиток інформаційних технологій та глобалізація, активізація та зростання значення соціальних мереж значною мірою змінили процес та методи збирання та обробки персональних даних, здійснення доступу до них та їх використання.

Наявність загроз інформаційній безпеці людини в соціальних мережах зовсім не означає, що треба обмежувати користування ними або видалятися одразу. Для безпечного користування слід, по-перше, не вказувати ні в якому разі свої персональні дані, інформацію, що стосується близьких людей, родичів, по-друге, використовувати антивірусне програмне забезпечення на ПК, по-третє, не заповняти всі поля, які пропонує заповнити соціальна мережа (адреси навчання, роботи, проживання і т.д.). Намагатись не наводити додаткову інформацію про себе в Інтернеті, бо зазвичай найслабшою ланкою в мережі є людина, а не програмний код [3, с. 144]. Отже, наявність додаткової інформації про особу розширює коло даних як про неї, так і про «друзів».

Право на контроль включає в себе право користувачів вирішувати, які з їхніх «друзів» можуть дозволяти службі розкривати свої персональні дані стороннім вебсайтам і додаткам. Соціальні мережі повинні питати дозволу на зміну будь-яких можливостей щодо використання персональних даних [5, с. 826]. Необхідно використовувати відповідні функції соцмереж щодо обмеження поширення даних лише для окресленого кола контактів.

Окреме дослідження доцільно проводити щодо використання даних проти юридичних осіб. Адже соціальні мережі відстежують діяльність користувачів своїх сайтів та сайтів своїх партнерів по маркетингу та здатні зібрати безпрецедентну кількість вторинної інформації на своїх користувачів, іноді навіть без їхньої згоди. Якщо ж цю інформацію збирають державні органи і використовують її для контролю за громадянами, то виникає т. зв. «архітектура вразливості». Серед багатьох ризиків для прайвесі у соціальних мережах варто виокремити, принаймні, три: 1) повна поінформованість про особу; 2) повідомлення інформації злочинцям; 3) відсутність у особи реального контролю за домірністю інформації про себе [5, с. 824].

Звичайно, існують і певні обмеження, наприклад, якщо дані використовуються з метою свободи самовираження, у засобах масової інформації, і, зрозуміло, якщо в цьому випадку є певна правова неузгодженість, а також, якщо держава або приватна компанія має право обробляти ці дані відповідно до визначеної законної мети їх обробки. Тож обмеження існують, хоча в цілому права фізичної особи мають бути гарантовані, якщо немає підстав для подібних обмежень [2, с.67].

Проблемою сайтів багатьох соціальних мереж є те, що їх параметри, встановлені за замовчуванням, роблять користувачів уразливими. Частина користувачів не підозрюють про необхідність зміни налаштувань з метою власного захисту. Наприклад, за замовчуванням сайти соціальних мереж можуть дозволяти використання HTML у коментарях, що дає змогу їх користувачам обмінюватися гіперпосиланнями, вставляти картинки і т.д. Це. натомість, спрощує хакеру задачу впровадження шкідливого ПЗ, оскільки дає можливість вставити таким чином посилання на розташований за межами сайту шкідливий код, який, наприклад, може відкрити зловмисникам доступ до внутрішньої мережі компанії [1, с. 2].

Інший проблемний аспект забезпечення приватності в соціальних мережах – неможливість повністю та остаточно видалити свої дані з соціальної мережі, що порушує так зване фундаментальне право фізичної особи у сфері захисту персональних даних – «право бути забутим» (right to be forgotten). Це право існувало в Європі з 1995 р. в усіх країнах-членах ЄС (з прийняттям базової Директиви 95/46/ЄС). Кожна людина може вимагати видалити свої дані у будь-який момент.

Слід зазначити також про етичну проблему щодо існування акаунтів померлих людей. На сьогодні у соцмережах (наприклад, Facebook) представлено нові функції для управління «меморіальними» акаунтами та алгоритми, які будуть контролювати появу профілю померлого в стрічці користувачів. Це дозволить близьким померлого обмежувати коло тих, хто може публікувати або переглядати повідомлення на цій сторінці. Також батьки, що втратили непо-

внолітніх дітей, отримали доступ до їх облікового запису і можуть продовжувати вести стрічку, акаунт [4]. Вводять додатковий контролю для людей, які керують меморіальними обліковими записами, запроваджують покращений штучний інтелект, щоб профіль померлої людини не з'являвся у хворобливих проявах, тобто як живої людини (привітання з днем народження, нагадування про події декількох років тому) [4]. Зазначимо, що для людей, відомих широкому загалу, вже функціонує стрічка-надпис в акаунті про те, що ця людина померла, відповідно дії з цим акаунтом припиняється щодо питань своєрідних «нагадувань» від соцмережі. У випадках з непублічними особами поки що не завжди спрацьовує ця функція.

Сучасні інформаційні технології пропонують такі шляхи захисту даних. Встановлення паролів на всі пристрої, якими користуєтеся (PIN-код у телефоні, пароль на вхід до облікового запису Windows тощо). Періодично створення резервних копій, важливих файлів через хмарні сервіси або на зовнішні переносні пристрої. Блокування пристрій щоразу, коли здійснюється вхід від нього (наприклад, у Windows — за допомогою комбінації клавіш Win+L). Встановлення повного шифрування на всі диски комп'ютера. Для Windows можна скористатися шифруванням за допомогою програми BitLocker (безплатно, працює з версіями Windows 8 і вище, за винятком серії Home), яка зашифрує повністю диск чи USB-носій. Для операційної системи Mac OS X існує аналог FileVault [6, с.10].

Необхідно також проводити аналіз вхідного і вихідного трафіку, вибірковий контроль соціальних мереж, останнє сприятиме дотриманню етика компанії, постійно провадити використання кеш-пам'яті. За умов користування особистими акаунтами слід створити стійкий пароль (з комбінаціями цифр, букв, букв великих), приховувати інформацію про день народження. Для захисту своєї конфіденційності, відключити загальнодоступний пошук (в розділі Пошуку засобів управління конфіденційністю Facebook обирати «Результати пошуку Facebook» доступні тільки для друзів).

Необхідно прослідковувати також фішінгові повідомлення, тобто такі які надходять на електронну пошту, акаунти соцмереж, а також онлайн як оголошення та пропонують певну інформацію (акції, пропозиції, бонуси), задля скористання якої необхідно навести власні дані: логін, пароль, особисті дані. Фахівці наполягають на обережному використанні таких оголошень.

Загалом, відповідальність за персональні дані фізичних та юридичних осіб покладаються на власників-носіїв таких даних. Перш за все, вони повинні проводити аутентифікацію (можливо, двохфакторну аутентифікацію) стосовно того куди представляються дані, додатково закріплені договором про відповідальність за розповсюдження інформації. Технічно ці персональні дані повинні зберігатися на локальних носіях, власних серверах компанії (власника) або фізичної особи, захищених сучасними інформаційними технологіями.

Слід підкреслити, що запровадження вищезазначених методів збереження даних надає можливість технічно легко прослідкувати джерело витоку та розповсюдження інформації. Необхідно своєчасно та постійно оновлювати програмне забезпечення та захищати свої продукти нововведеннями. Проте, на сучасному етапі недостатньо зазначених норм і принципів для регулювання інформаційних процесів в соціальних мережах, глобальний характер яких зумовлює необхідність створення уніфікованих інформаційних норм для врегулювання правових відносин у соціальних мережах та відповідних технічних норм.

1.Кухарська Н.П., Кухарський В.М. Вплив соціальних мереж на корпоративну інформаційну та економічну безпеку. URL: http://science.lpnu.ua/sites/default/files/journalpaper/2017/jun/3740/kukharskanpkukharskyivm.pdf

2.Мельник К.С. Обробка та захист персональних даних в соціальних мережах. *Інформація і право.* № 3(12), 2014. С. 64-69

3. Москаленко М.В. Захист інформації в соціальних мережах. Актуальні задачі та досягнення у галузі кібербезпеки. *Матеріали Всеукраїнської науково-практичної конференції, 23-25 листопада 2016 р., м. Кропивницький*. Кропивницький, 2016. С. 143-144.

4.Making It Easier to Honor a Loved One on Facebook After They Pass Away. URL: https://about.fb.com/news/2019/04/updates-to-memorialization/

5.Серьогін В. О. Соціальні мережі як загроза прайвесі. *Форум права.* № 2. 2011. С. 822–827

6.Як підсилити інформаційну безпеку в Інтернеті під час конфлікту. рекомендації для стейкхолдерів. К. : Вид-во «К.І.С.», 2017. 43 с.