DOI: https://doi.org/10.15407/np.63.050
УДК 004.056.5:342.72/.73:[004.77:316.77]

**Марат Закіров,**
доктор політичних наук, доцент, завідувач відділу,
Національна бібліотека України імені В. І. Вернадського
Голосіївський просп., 3, Київ, 03039, Україна
e-mail: zakirovmarat65@gmail.com
ORCID: https://orcid.org/0000-0003-4897-4325
Web of Science ResearcherID: AAF-6246-2020

**Світлана Закірова,**
кандидат історичних наук, доцент, завідувач відділу,
Національна бібліотека України імені В. І. Вернадського
Голосіївський просп., 3, Київ, 03039, Україна
e-mail: zakirovasvtl@gmail.com
ORCID: https://orcid.org/0000-0002-5396-7210
Web of Science ResearcherID: AAR-6405-2021

# ДИЛЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційна безпека особистості набуває великого суспільно-політичного значення в умовах активного використання комунікаційних технологій у соціально-політичній конкуренції і геополітичному протистоянні. У статті проведено аналіз стану інформаційної безпеки особистості в контексті розробки і застосування новітніх інструментів збору, аналізу та використання особистої інформації користувачів. Визначено характеристики явища безпеки інформації і виявлені особливості інформаційної безпеки особистості. Простежено вплив новітніх інформаційних технологій на індивідуальний простір і конфіденційність особистого життя людини.

*Ключові слова:* дилема інформаційної безпеки, особистий простір, маніпуляція, інформаційне суспільство, особистість.

**Актуальність.** Розвиток інформаційних технологій, що набув вибухового характеру на зламі тисячоліть, сприяв перетворенню еволюції інформаційного простору в одну з ключових складових процесу глобалізації. У нових реаліях рівень інформатизації стає визначальним фактором суспільно-політичного та економічного розвитку, що безпосередньо

впливає на конкурентоспроможність держав і забезпечує технологічний прогрес. Глобалізація інформаційного простору внаслідок розвитку мережевих технологій поряд з безсумнівно позитивним впливом має і негативні наслідки, зокрема зростання можливостей маніпулятивного впливу на суспільну свідомість. Небезпека таких явищ суттєво підсилюється можливостями дистанційного скоєння протиправних дій, через що маніпулятори фізично можуть знаходитися далеко від особи, проти якої спрямовані їхні дії. Відтак питання захисту даних особистості є вкрай важливим як на національному, так і на глобальному рівнях. З огляду на значне зростання потужності інформаційних технологій, масштабне розширення й інтернаціоналізацію аудиторії різноманітних мережевих ресурсів, удосконалення методики адресного розповсюдження цілеспрямованого, маніпулятивного і деструктивного контенту особливої актуальності набуває проблема інформаційної безпеки.

**Аналіз досліджень і публікацій.** Наукове осмислення інформаційних процесів у контексті забезпечення безпеки держави і суспільства знаходиться в центрі дослідницького пошуку вітчизняних і зарубіжних вчених. Зокрема, праця експерта з кібершпіонажу Джорджтаунського університету Б. Бьюкенена присвячена висвітленню важливої проблеми міжнародних відносин, пов'язаної зі специфікою прояву феномену «дилеми безпеки» у сфері цифрових технологій [1]. Маніпулятивні форми переконання і особливості консенсуальних та пропагандистських типів організованої комунікації у сучасних ліберальних демократіях досліджують англійські вчені В. Бакір, Е. Херрінг та ін. [2]. Аналіз інформаційних загроз, пов'язаних з поширенням комунікації у соціальних мережах, і розгляд перспективних засобів протидії можливим загрозам деструктивних впливів на суспільну свідомість проводить у своїй роботі О. Михайлова [3]. Проблеми забезпечення особистих прав і свобод людини в умовах зростаючого впливу інтернет-технологій на політичні і соціально-економічні процеси досліджують М. Єнін і Г. Коржов [4]. Особливості захисту персональних даних особистості в умовах глобалізованого рівня комунікації аналізують В. Брижко, Ю. Муравська, М. Бем, С. Єсімов та ін. Разом з тим слід зауважити, що попри доволі плідну дослідницьку роботу науковців, активний розвиток інформаційних технологій, що суттєво розширює можливості людства, одночасно продукує все нові й нові можливості для організації деструктивних дій. Тому проблема безпеки продовжує залишатися однім з найбільш перспективних напрямів наукового пошуку в інформаційній сфері. Зокрема, більшість фахівців у сфері комунікаційних технологій зосереджують увагу на дослідженнях проблем

забезпечення загальної інформаційної безпеки або протидії злочинним діям у комп'ютерних мережах.

**Метою статті** є аналіз дилеми інформаційної безпеки особистості в контексті розробки і застосування новітніх інструментів збору, аналізу й використання особистої інформації користувачів. Для досягнення поставленої мети треба виконати такі завдання: окреслити сутність поняття «інформаційне суспільство», визначити характеристики явища безпеки інформації, виявити особливості інформаційної безпеки особистості, простежити вплив новітніх інформаційних технологій на індивідуальний простір і конфіденційність особистого життя людини.

**Виклад основного матеріалу дослідження.** Наукове осмислення процесів еволюції телекомунікаційних технологій, масової цифровізації і перетворення ІТ-індустрії у провідну галузь світової економіки спонукали дослідників до висновку щодо переходу людства на нову сходинку цивілізаційного розвитку, яка визначає інформаційні технології та інформацію в усіх її проявах як основний чинник суспільного розвитку. У підсумку теоретичних пошуків вчених багатьох країн світу у 60-х роках минулого століття викристалізувався термін «інформаційне суспільство».

На сьогодні вже розроблено чимало визначень поняття «інформаційне суспільство», що вирізняються між собою критеріями феномену, які той чи інший дослідник бере за основу аналізу. Враховуючи зазначену багатогранність проблеми, що виходить за межі нашої роботи, ми спиратимемося на одне з найбільш ґрунтовних і універсальних визначень, що було запропоновано українським дослідником В. Данил'яном: «Інформаційне суспільство нового типу, що формується в результаті нової соціальної революції, породженої вибуховим розвитком та конвергенцією інформаційних і комунікаційних технологій; – суспільство знань, тобто суспільство, у якому головною умовою добробуту кожної людини та кожної держави стає знання, здобуте завдяки безперешкодному доступу до інформації й умінню працювати з нею; інформація в такому суспільстві є найважливішим соціальним і економічним ресурсом, основним джерелом продуктивності праці та влади, умовою добробуту людини і держави; – глобальне суспільство, у котрому обмін інформацією не матиме ні часових, ні просторових, ні політичних меж; яке, з одного боку, сприяє взаємопроникненню культур, а з іншого − відкриває кожному співтовариству нові можливості для самоідентифікації інформаційне суспільство – це якісно новий етап соціотехнологічної еволюції суспільства, що формується в результаті довгострокових тенденцій

попереднього соціально-економічного розвитку, який передбачає збільшення ролі інформації і знань, а також формування та споживання інформаційних ресурсів у всіх системах життєдіяльності суспільства за допомогою розвитку інформаційно-комунікаційних технологій, що існують у глобальних масштабах» [5, с. 22].

Визнання факту і теоретичне осмислення чергового якісного переходу в цивілізаційному розвитку людства, а також всебічний аналіз процесів формування нового суспільства виводить дослідників на виявлення вірогідних викликів і небезпек, що перебувають у діалектичному зв'язку з новими можливостями, які людство отримує внаслідок становлення інформаційного суспільства. Історичний досвід показує, що кожний технологічний прорив потребував суттєвого перегляду підходів до безпеки, нейтралізації негативних наслідків, що супроводжують забезпечення й застосування нових технологій.

Становлення інформаційного суспільства суттєво актуалізувало явище «інформаційної безпеки», оскільки в нових умовах саме інформація в усіх її видах і проявах стає основою ефективного економічного і соціально-політичного розвитку, але водночас пропорційно зростають і деструктивні можливості використання інформації.

Світовою наукою вже накопичений значний масив теоретичних знань щодо визначення поняття «інформаційна безпека», що розрізняються між собою галузевими підходами, критеріями аналізу тощо. Зокрема, українські дослідники І. Дятлова, П. Квіткін і Л. Петрова зазначають, що з початку становлення наукового осмислення проблеми в працях як вітчизняних, так і закордонних дослідників спостерігалося ототожнення понять «інформаційна безпека» і «безпека інформації». Разом з тим, зазначають згадані науковці, більшість дослідників розмежовує поняття «інформаційна безпека» і «безпека інформації», наголошуючи на тому, що при визначенні безпеки інформації об'єктом виступає власне інформація, а інформаційної безпеки – безпека як частина цілого. Наприклад, О. Дзьобань і В. Пилипчук визначають інформаційну безпеку як стан захищеності життєво важливих інтересів людини, суспільства та держави в інформаційній сфері від зовнішніх і внутрішніх викликів і загроз, що забезпечує їхній сталий розвиток [6, с. 49].

У свою чергу зауважимо, що явище «інформаційна безпека особистості», з огляду на особливість об'єкта, має два взаємопов'язані і взаємозалежні аспекти. Перший аспект – це технологічна безпека, яку можна представити через визначення, що подає українська дослідниця Ю. Муравська, – інформаційна безпека це стан, вільний від загроз,

що сприймаються в основному як надання інформації стороннім особам; шпигунство; саботаж та диверсійні заходи. «Інформаційна безпека являє собою також будь-яку дію, систему або метод, які спрямовані на захист інформаційних ресурсів, що передаються, зберігаються в пам'яті комп'ютерів і телекомунікаційних мереж. Інформаційна безпека – це не тільки захист від несанкціонованого доступу, крадіжки даних або їх знищення. Варто її розуміти набагато ширше. Інформаційна безпека розуміється як компонент фізичної, особисто-організаційної та IT-безпеки господарюючого суб'єкта чи інституції» [7, с. 291].

Другий – гуманітарний або психологічний аспект інформаційної безпеки можна розглядати у формулюваннях, що подаються в праці І. Кукіна, – «інформаційна безпека особистості … визначає захищеність людини від деструктивних інформаційних впливів, що призводять до неадекватного сприйняття дійсності. Внесення деструктивних змін у свідомість особистості може здійснюватися цілеспрямованим застосуванням інформаційних технологій. Їх негативними наслідками можуть бути руйнування цілісності особистості, системи її відносин з іншими людьми та державою» [8, с. 86].

Отже, перший аспект безпосередньо пов'язаний із сучасним рівнем технічного розвитку і передбачає захист особистого простору, конфіденційності інформації людини шляхом розробки й застосування технологічних інструментів, що мають захищати безпосередньо особисті пристрої зберігання даних і обміну інформацією та включати також системи безпеки глобальних комунікаційних мереж.

На відміну від першого аспекту проблеми інформаційної безпеки особистості, що здебільшого є похідним становлення інформаційного суспільства у наш час, другий аспект, який тісно пов'язаний з безпосереднім впливом на людську свідомість, сягає своїм корінням епохи античності. Вже тоді боротьба за ресурси й владу спонукала до винаходу і застосування все нових засобів, що мали забезпечити перевагу над противником, включно із психологічним впливом. Зокрема, С. Закірова зазначає: «Перші свідчення про проведення інформаційних операцій і дій, спрямованих на організацію інформаційного впливу на військових і цивільне населення, трапляються вже у роботах стародавніх авторів. Більшість із них вважали інформаційні дії під час проведення військових кампаній воєнними хитрощами. Однак, виходячи із завдань, які ставили перед собою полководці й стратеги минулого, за своєю суттю такі дії повністю відповідають сучасним поняттям інформаційних стратегій» [9, с. 30]. Психологічний аспект інформаційної безпеки передбачає цілеспря-

мовану підготовку людини до протидії інформаційним впливам, зокрема, визначення сталих світоглядних орієнтирів, розвиток критичного мислення, виховання активної громадянської позиції і культури комунікації тощо.

Проте, незважаючи на зазначене ще в давнину розуміння ролі інформаційних стратегій і відповідно спроби протидії, використання інформації як засобу боротьби і впливу на суспільство у подальшому лише удосконалювалося та розширювалося адекватно наявним можливостям і вимогам часу. Відповідно до історичної логіки розвиток інформаційних технологій у XXI ст. відкрив нові перспективи організації інформаційних операцій і очікувано вивів прийоми порушення інформаційної безпеки особистості на новий рівень.

Зокрема, через застосування різного роду специфічних мобільних додатків, на кшталт, розробленого професором психології Кембриджського університету О. Коганом – This is your digital life («Твоє цифрове життя»), суттєво розширилися можливості контролю індивідуальної та суспільної свідомості. За допомогою подібних програм створюються психологічні портрети користувачів соціальних мереж, а потім саме через ці мережі розповсюджується цілеспрямовано підготовлений контент, створений з урахуванням вже зібраних даних про політичні уподобання й ціннісні орієнтири певної цільової аудиторії. Більш докладно практика застосування зазначеної технології у політичній боротьбі досліджувалася в одній з наших попередніх праць [10, с. 166].

Широке поширення цифрових технологій перетворює інформацію на ефективний інструмент конкуренції в усіх без винятку сферах життєдіяльності суспільства й глобального світу. Рівень доступу до інформаційних технологій дедалі частіше відіграє провідну роль у забезпеченні як соціального успіху окремої людини в конкретному суспільстві, так і визначенні ваги окремих країн у глобальній економіці й політиці. Все більше дослідників виокремлюють проблему інформаційного розшарування суспільства та інформаційної нерівності людей у соціумі і держав у світі.

Поряд з цим наведений нами вище приклад використання соціальних мереж як інструменту маніпулювання свідомістю є яскравим проявом порушення принципу конфіденційності інформації й вторгнення в особисте життя людини. Завдяки створенню загальнодоступної глобальної мережі, яка стає основним інструментом обміну інформацією, людина суттєво розширює свої можливості, відкриває для себе світ, але разом з тим відкривається сама і як наслідок стає більш вразли-

вою. Як бачимо, виникає своєрідна дилема, що певним чином пов'язана з «дилемою кібербезпеки», яку розглядає у своїй книзі американський дослідник Б. Бьюкенен. Зокрема, вчений зазначає: «Проблема безпеки стає найбільш серйозною, коли існує тісний зв'язок між збором розвідувальної інформації та атакою, як у випадку з кібероперaціями. Цей тісний зв'язок робить діяльність із збору даних більш небезпечною…» [1].

У процесі взаємодії й обміну інформацією у глобальній мережі дуже тонка межа між необхідним мінімумом інформації про особу, що забезпечує зручність спілкування, відбір цікавого конкретній людині контенту, і проникненням в її індивідуальний простір за межі допустимого. Проблема збереження цілісності зазначеної межі і є дилемою інформаційної безпеки особистості в інформаційному суспільстві. Як будь-яка дилема вона немає однозначного вирішення, оскільки будь-яка спроба її вирішення веде або до зменшення ефективності роботи в мережі, або відкриває можливості маніпуляції свідомістю за допомогою спеціальних програм створення й подання, на основі зібраної особистої інформації, відповідного цілеспрямованого контенту, що має викликати у людини бажану для ініціатора такої операції реакцію, а згодом і дію.

Одним з найбільш поширених і більш-менш безпечних прикладів вироблення цілеспрямованого контенту є таргетована реклама, яка включає декілька параметрів налаштувань, що дозволяють виокремити певні сегменти цільової аудиторії. Зокрема, соціально-демографічні налаштування орієнтовані на національність, економічний статус, стать, вік, рівень освіти, рівень доходу, професійну діяльність та займану посаду, а психографічні налаштування засновані на способі життя споживача, його переконаннях, цінностях та інтересах [11, с. 111].

Зазначені параметри налаштування мають дещо відсторонений характер і окреслюють орієнтацію на такого собі середньостатистичного користувача, хоча врахування у налаштуваннях цінностей і думок вже передбачає певну індивідуалізацію, що, з огляду на необов'язковість згоди користувача на використання даних, вже можна розцінювати як атаку на особистий простір.

Зокрема, за даними представника Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних І. Берназюк у 2020 р. до Уповноваженого надійшло понад 2000 скарг громадян. Серед причин таких звернень значна частина стосувалися порушень незаконного поширення персональних даних через мережу Інтернет; неправомірного витребування згоди на обробку персональних даних у тих випадках, коли вона не потрібна; поширення персональної інформації у месенджерах

і соціальних мережах; порушення під час впровадження електронних сервісів тощо [12].

Проте застосовуються і ще більш цілеспрямовані параметри налаштування, що передбачають активніше проникнення у особистій простір людини. Наприклад, таргетинг, орієнтований на аналіз поведінки користувача, та його різновид – ретаргетинг, які за допомогою спеціальних програм вивчають історію браузера, що зберігає відомості про покупки та інші недавні дії користувача на сайті, або геотаргетинг, коли використовуються дані зі спеціальних сервісів і програм і формуються карти пересувань користувачів і цілих груп населення. Слід підкреслити, що з метою виявлення цільової аудиторії відбувається «… фіксація щоденних маршрутів, адреси відвідуваних будівель, зупинок і інших відвідуваних точок» [11, с. 111]. Тобто в цих випадках мова вже може йти про дії, які відносно недавно однозначно кваліфікувалися як стеження і могли підпадати під правові санкції й більш того, у випадку застосування цих методів приватною особою, а не глобальними мережевими ресурсами, підпадають і зараз.

Разом з тим сьогодні у Європі відомі факти прямого притягнення до відповідальності великих гравців на ринку послуг за порушення у сфері захисту персональних даних. Наприклад, у 2020 р. шведський орган управління захисту даних (DPA) наклав штраф у розмірі 75 млн шведських крон (приблизно 7 млн євро) на Google як оператора пошукової системи за невиконання вимог GDPR («Регламенту в межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони», 2018 р.) щодо вилучення персональних даних через неточність або оскільки така інформація була зайвою. У тому ж році італійський наглядовий орган наклав два штрафи в розмірі 8,5 млн та 3 млн євро на італійського постачальника електроенергії та газу Eni Gas e Luce (EGL). Перший – за те, що компанія незаконно обробляла особисті дані, здійснюючи маркетингові дзвінки особам, які відмовилися від отримання таких дзвінків. Другий – за те, що EGL укладала контракти з понад 7 тис. клієнтів без їх повідомлення [13].

До певної міри ситуація ускладнюється тим, що людина реєструється на сайті добровільно і так само добровільно розміщує про себе багато інформації, але, як правило, згоду на збір особистої інформації, а тим більше на її подальше використання у користувача не запитують. Більш того, різноманітні мережеві ресурси використовують спеціальні файли coocies, які полегшують користування сайтом, але одночасно збирають особисту інформацію користувача. У контексті використання елект-

ронних систем конфіденційність користувача і автономність його даних зменшується, оскільки під час реєстрації він змушений йти вздовж лінії, визначеної електронною системою. Це часто має негативний вплив, оскільки реєстрація або подальше використання даних не відповідає очікуванням про те, що є розумним [14, с. 94].

Отже, повертаючись до згаданої вище «дилеми кібербезпеки», виробники реклами збирають «розвідувальну інформацію» за допомогою вивчення людини, її особистого життя, уподобань і орієнтирів шляхом моніторингу соціальних мереж. Причому слід наголосити, що оскільки, за слушною думкою Б. Бьюкенена, між збором інформації й атакою існує тісний зв'язок, цілком імовірно, що збирач «розвідувальної інформації» у намаганні створити найбільш повну картину дуже легко, і навіть непомітно для себе перейде в атаку, грубо порушуючи і конфіденційність інформації, і межі особистого життя людини, вирішуючи дилему безпеки особистості на користь проникнення за грань допустимого.

Особливу суспільно-політичну небезпеку такі дії мають у випадку використання зазначеної методики в політичній боротьбі. Зокрема, свого часу було встановлено, що Facebook не тільки збирав інформацію про своїх користувачів, аналізував їхні повідомлення, зв'язки, але й купував додаткову інформацію в різних брокерів даних. У Facebook подібні дії виправдовували тим, що за допомогою аналізу персональної інформації клієнтів вони «показують більш релевантну рекламу». Саме ці дані, зібрані за допомогою згаданого вище додатку This is your digital life, були передані Cambridge Analytica і Strategic Communication Laboratories і згодом були використані під час виборчої кампанії президента США Д. Трампа й Brexit-кампанії [15].

Завдяки застосуванню таких методик політичні актори отримують можливість вироблення специфічної політичної реклами та агітаційних матеріалів з використанням відповідних параметрів налаштування, що орієнтовані на конкретні цільові аудиторії. Таким чином, єдиний інформаційний простір розбивається на окремі сегменти, у яких політична сила використовує різні прийоми й матеріали, пропонуючи кожній групі виборців максимально прийнятний для неї набір лозунгів і обіцянок. У цьому випадку ми вже бачимо, що дилема безпеки вирішується на користь ескалації – збір інформації перетворюється на атаку, відбувається порушення кордонів особистої свободи, маніпуляція свідомістю людей з метою досягнення політичних цілей.

Особливу небезпеку застосування маніпулятивних технологій набуває в умовах гібридних і відкритих військових конфліктів. Основним завданням

маніпуляторів є внесення «сенсаційної» інформації в середовище користувачів соціальних мереж з метою подальшої трансляції ними цієї інформації серед своїх друзів. У соціальних мережах широко використовують і прийом соціального доказу, розрахований на використання групового інстинкту «масової людини», яка переймає нав'язану їй ілюзорну поведінку більшості. Спрацьовує так званий «ефект натовпу» – «як більшість, так і я» [16, с. 37]. Отже, маніпулятори в першу чергу орієнтуються на первинні інстинкти людей: цікавість до нового, прагнення до успіху, почуття єдності з іншими тощо. Таким чином, одним з головних інструментів протидії маніпулятивним впливам є критичне мислення користувачів соціальних мереж, здатність до самостійної оцінки отриманої інформації і усвідомлена громадянська позиція. Не менш важливим шляхом покращення інформаційної безпеки особистості виступає підвищення загального рівня правової культури громадян у сфері інтернет-комунікації, відповідального ставлення до персональних даних і системи їх захисту.

**Висновки.** Наукове осмислення корінних і всеосяжних суспільно-економічних змін, що відбулися в другій половині XX – на початку XXI ст. під впливом стрімкого розвитку телекомунікаційних технологій і масової цифровізації усіх сфер діяльності людства, зумовило виникнення поняття «інформаційне суспільство», що характеризує нову якісну ступень цивілізаційного розвитку. Суттєве розширення комунікаційних можливостей, які надають сучасні інформаційні технології, поряд із значним позитивним ефектом супроводжується зростанням небезпеки здавна використовуваних і добре відомих методів деструктивного використання інформації і винайдення й застосування новітніх, ще більш дієвих засобів впливу на свідомість і порушення конфіденційності інформації. Залучення соціальних мереж, озброєних потужними інструментами збору й аналізу великих обсягів інформації, у політичне і соціально-економічне життя зумовило виникнення дилеми інформаційної безпеки особистості як форми рівноваги між необхідним доступом до особистої інформації і порушенням конфіденційності. Проблема забезпечення інформаційної безпеки особистості поряд із захистом приватних інтересів людини має велике суспільно-політичне значення, оскільки вдосконалення й застосування методів різного роду маніпулятивних впливів активно використовується як у політичному житті окремих країн, так і у міждержавному, і навіть геополітичному протистоянні. З огляду на зазначене, актуальним є дослідження теоретичних підвалин створення ефективної моделі інформаційної безпеки особистості, що враховуватиме перспективні напрями розвитку комунікаційних технологій.

**Список бібліографічних посилань**

1. Buchanan B. (2017). The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. *Oxford University Press*. https://doi.org/10.1093/acprof:oso/9780190665012.001.0001.

2. Bakir V., Herring E., Miller D., & Robinson P. (2019). Organized Persuasive Communication: A new conceptual framework for research on public relations, propaganda and promotional culture. *Critical Sociology*, 45(3), 311–328. https://doi.org/10.1177/0896920518764586.

3. Михайлова О. Соціальні мережі як чинник змін політичних практик в Україні: ризики і перспективи. *Стратегічна панорама.* № 1–2. С. 93–99. https://doi.org/10.53679/2616–9460.1–2.2019.09.

4. Єнін М., Коржов Г. Мережева комунікація: ризики та перспективи (на основі соціологічних опитувань громадської думки в країнах Євросоюзу). *Вісник НТТУ «КПІ» Політологія. Соціологія. Право.* № 1(49). 2021. С. 22–20. https://doi.org/10.20535/2308–5053.2021.1(49).232789.

5. Даніл'ян В. Інформаційне суспільство та перспективи його розвитку в Україні (соціально-філософський аналіз). Харків, 2008. 184 с.

6. Квіткін П., Дятлова І., Петрова Л. Інформаційна безпека особистості: теоретико-методологічний аналіз. *Вісн. Нац. юрид. ун-ту ім. Ярослава Мудрого.* 2021. № 4 (51). С. 46–62. https://doi.org/10.21564/2663–5704.51.241998.

7. Муравська Ю. Інформаційна безпека суспільства: концептуальний аналіз. *Економіка та суспільство.* 2017. Вип. 9. С. 289–294.

8. Кукін І. Рівні інформаційної безпеки особистості в системі національної безпеки держави. *Вчені записки ТНУ ім. В. І. Вернадського. Серія: Державне управління.* Т. 30 (69). № 5. 2019. С. 85–90. https://doi.org/10.32838/2663–6468/2019.5/15.

9. Закірова С. Полемологічні виміри інформаційних стратегій минулого. *Наук. пр. Нац. б-ки України ім. В. І. Вернадського.* 2018. Вип. 49. С. 21–33. https://doi.org/10.15407/np.49.021.

10. Закіров М., Закірова С. Мережева політична взаємодія в структурі соціальних комунікацій. *Наук. пр. Нац. б-ки України ім. В. І. Вернадського.* 2020. Вип. 57. С. 163–175. https://doi.org/10.15407/np.57.163.

11. Євсейцева О., Меркулова Д. Таргетинг – цілеспрямований вплив на споживача. *Економіка та держава.* 2019. № 3. С. 107–113. https://doi.org/10.32702/2306–6806.2019.3.107.

12. Посилення законодавчого забезпечення захисту персональних даних в Україні обговорено під час круглого столу у Верховній Раді.

*Верховна Рада України.* 1.04.2021. URL: https://www.rada.gov.ua/news/news_kom/205937.html.

13.Матола В. «Баги» державних реєстрів, або як захистити персональні дані. *LB.ua.* 19 трав. 2020. URL: https://lb.ua/pravo/2020/05/19/457892_bagi_derzhavnih_reiestriv_abo_yak.html.

14. Гуйван П. Юридичне регулювання електронної обробки персональних даних. *Актуальні проблеми вітчизняної юриспруденції.* 2018. № 6. С. 92–96.

15. Фейсбук збирає усі дані про дзвінки та смс користувачів свого мобільного додатку. Ракурс.UA. 26 березня 2018. URL: https://racurs.ua/ua/n102739-feysbuk-zbyraie-usi-dani-pro-dzvinky-ta-sms-korystuvachiv-svogo-mobilnogo-dodatku.html.

16. Шемаєв В., Присяжнюк М., Онофрійчук А. Соціальні мережі в аспекті інформаційної безпеки. *Наука і оборона.* 2019. № 3. С. 36–39. https://doi.org/10.33099/2618–1614–2019–8-3–36–39.

**References**

1. Buchanan, B. (2017). The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. *Oxford University Press*. https://doi.org/10.1093/acprof:oso/9780190665012.001.0001 [in English].

2. Bakir, V., Herring, E., Miller, D., & Robinson, P. (2019). Organized Persuasive Communication: A new conceptual framework for research on public relations, propaganda and promotional culture. *Critical Sociology*, *45*(3), 311–328. https://doi.org/10.1177/0896920518764586 [in English].

3. Mykhailova, O. (2019). Sotsialni merezhi yak chynnyk zmin politychnykh praktyk v Ukraini: ryzyky i perspektyvy [Social networks as a factor of changes in political culture and political practices in Ukraine: risks and perspectives]. *Stratehichna panorama – Strategic Panorama, 1–2*, 93–99. https://doi.org/10.53679/2616–9460.1–2.2019.09 [in Ukrainian].

4. Yenin, M., Korzhov, H. (2021). Merezheva komunikatsiia: ryzyky ta perspektyvy (na osnovi sotsiolohichnykh opytuvan hromadskoi dumky v krainakh Yevrosoiuzu) [Online communication: risks and prospects (on the basis of sociological study of public opinion in the EU countries)]. *Visnyk NTTU «KPI» Politolohiia. Sotsiolohiia. Pravo – National Technical University of Ukraine Journal. Political science. Sociology. Law, 1*(49), 22–29. https://doi.org/10.20535/2308–5053.2021.1(49).232789 [in Ukrainian].

5. Danilyan, V. (2008). Informatsiine suspilstvo ta perspektyvy yoho rozvytku v Ukraini (sotsialno-filosofskyi analiz) [Information society and

prospects of its development in Ukraine (socio-philosophical analysis)]. Kharkiv. 184 p.

6. Kvitkin, P., Diatlova, I., Petrova, L. (2021). Informatsiina bezpeka osobystosti: teoretyko-metodolohichnyi analiz [Personal information security: theoretical and methodological analysis]. *Visnyk Natsionalnoho yurydychnoho universytetu imeni Yaroslava Mudroho – The Bulletin of Yaroslav Mudryi National Law University. Series: Philosophy, Philosophies of Law, Political Science, Sociology, 4* (51), 46–62 [in Ukrainian].

7. Muravska, Y. (2017). Informatsiina bezpeka suspilstva: kontseptualnyi analiz [Information security of society: conceptual analysis]. *Ekonomika ta suspilstvo – Ekonomy and Society. Mukachevo, 9*, 289–294 [in Ukrainian].

8. Kukin, I. (2019). Rivni informatsiinoi bezpeky osobystosti v systemi natsionalnoi bezpeky derzhavy [Levels of the individual information security in the state national security system]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Derzhavne upravlinnia – Scientific Notes of the Taurian V. I. Vernadsky National University, 5,* 85–90. https://doi.org/10.32838/2663–6468/2019.5/15 [in Ukrainian]

9. Zakirova, S. (2018). Polemolohichni vymiry informatsiinykh stratehii mynuloho [Polymological Measurements of Information Strategies of the Past]. *Naukovi pratsi Natsionalnoi biblioteky Ukrainy imeni V. I. Vernadskoho – Transactions of V. I. Vernadsky National Library of Ukraine. 49,* 21–33. https://doi.org/10.15407/np.49.021 [in Ukrainian].

10. Zakirov, M., Zakirova, S. (2020). Merezheva politychna vzaiemodiia v strukturi sotsialnykh komunikatsii [Network Political Interaction in the Structure of Social Communications]. *Naukovi pratsi Natsionalnoi biblioteky Ukrainy imeni V. I. Vernadskoho – Transactions of V. I. Vernadsky National Library of Ukraine*, *57*, 163–175. https://doi.org/10.15407/np.57.163 [in Ukrainian].

11. Yevseytseva, O., Merkulova, D. (2019). Tarhetynh – tsilespriamovanyi vplyv na spozhyvacha. [Targeting is a focused impact on the consumer]. *Ekonomika ta derzhava – Economy and State, 3*, 107–113. https://doi.org/10.32702/2306–6806.2019.3.107 [in Ukrainian].

12. Posylennia zakonodavchoho zabezpechennia zakhystu personalnykh danykh v Ukraini obhovoreno pid chas kruhloho stolu u Verkhovnii Radi. [Strengthening the legislative provision for the protection of personal data in Ukraine was discussed during a round table in the Verkhovna Rada]. *Verkhovna Rada of Ukraine*. April 1, 2021. URL: https://www.rada.gov.ua/news/news_kom/205937.html [in Ukrainian].

13. Matola, W. (2020). «Bahy» derzhavnykh reiestriv, abo yak zakhystyty

personalni dani [«Bugs» of state registers, or how to protect personal data]. *LB.ua.* May 19, 2020. URL: https://lb.ua/pravo/2020/05/19/457892_bagi_derzhavnih_reiestriv_abo_yak.html [in Ukrainian].

14. Huivan, P. (2018). Yurydychne rehuliuvannia elektronnoi obrobky personalnykh danykh. [Legal regulation of electronic processing of personal data]. *Aktualni problemy vitchyznianoi yurysprudentsii – Actual Problems of Native Jurisprudence, 6*, 92–96 [in Ukrainian].

15. Feisbuk zbyraie usi dani pro dzvinky ta sms korystuvachiv svoho mobilnoho dodatku [A facebook collects all data about rings and sms of users mobile to addition]. *Racurs.Ua*. March 26, 2018. URL: https://racurs.ua/ua/n102739-feysbuk-zbyraie-usi-dani-pro-dzvinky-ta-smskorystuvachiv-svogo-mobilnogo-dodatku.html [in Ukrainian].

16. Shemaiev, V., Onofriichuk, A., Prysiazhniuk, M. (2019). Sotsialni merezhi v aspekti informatsiinoi bezpeky. [Social networks in the aspect of information security]. *Nauka i oborona – Science and Defense*, *3*, 36–39. https://doi.org/10.33099/2618–1614–2019–8-3–36–39 [in Ukrainian].

Стаття надійшла до редакції 14.02.2022.

**Marat Zakirov,**
Dr. Sci. (Political Science), Associate Professor, Head of Department,
V. I. Vernadsky National Library of Ukraine
3 Holosiivskyi Ave., Kyiv 03039, Ukraine
e-mail: zakirovmarat65@gmail.com
ORCID: https://orcid.org/0000-0003-4897-4325
Web of Science ResearcherID: AAF-6246-2020

**Svitlana Zakirova,**
PhD (History), Associate Professor, Head of Department,
V. I. Vernadsky National Library of Ukraine
3 Holosiivskyi Ave., Kyiv 03039, Ukraine
e-mail: zakirovasvtl@gmail.com
ORCID: https://orcid.org/0000-0002-5396-7210
Web of Science ResearcherID: AAR-6405-2021

**The Dilemma of Information Security of the Individual in the Information Society**

The paper presents an analysis of the state of information security of the individual in the context of development and application of the latest tools for collecting, analyzing and using personal information of users. The concept of «information society» are clarified. The characteristics of the phenomenon of information security are determined

and the features of information security of the individual are revealed. The influence of the latest information technologies on the individual space and confidentiality of personal life is traced. Scientific understanding of the current stage of civilizational development resulted in the *information society* concept.

The phenomenon of *personal information security* has two interrelated and interdependent aspects. The first aspect involves the protection of privacy, the confidentiality of human information through the development and application of technological tools that should directly protect personal storage and information exchange devices and also include security systems of global communications networks. The second aspect of the humanitarian or psychological aspect of information security involves purposeful guiding people how to counter information influences, in particular, the articulation of sustainable worldviews, the development of critical thinking, education of active citizenship and communication culture, and more.

The problem of maintaining a balance between the minimum of information about a person in the network and the violation of personal confidentiality is a dilemma of individual' information security in the information society. The main tool to counteract manipulative influences is the critical thinking of social networks users, the ability to self-assess the information received, and a conscious civic position.

*Keywords:* information security dilemma, personal space, manipulation, information society, personality.