УДК 351.741
DOI https://doi.org/10.32782/2524-0374/2024-5/66

АКТУАЛЬНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ЛЮДИНИ І ГРОМАДЯНИНА В ЄВРОПІ

CURRENT THREATS TO THE INFORMATION SECURITY OF PEOPLE AND CITIZENS IN EUROPE

Волох О.К., к.ю.н.,
доцент кафедри публічного управління та адміністрування
Національна академія внутрішніх справ

Печеряга М.В., студент ІІ курсу магістратури
Навчально-науковий інститут заочного та дистанційного навчання Національної академії внутрішніх справ

У статті досліджено окремі правові проблеми, пов'язані з забезпеченням інформаційної безпеки в Україні. Розглянуто проблеми чіткого формулювання інтересів у сфері інформаційної безпеки. Виявлено факти бездіяльності уповноважених суб'єктів щодо інформаційного шпигунства з боку Сполучених Штатів Америки.

У Стратегії інформаційної безпеки, затвердженій указом Президента України від 28 грудня 2021 року № 685/2021, термін «інформаційна безпека України» визначається як складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом».

Слід більш детально проаналізувати вищезазначене визначення, сформульоване в нині діючій Стратегії інформаційної безпеки.

Вважаємо, що неправильно, по-перше, звужувати термін «інформаційна безпека» до однієї з її складових, визначаючи лише те, як треба розуміти словосполучення «інформаційна безпека *України*» (тобто – держави).

Як відомо, стратегічна ціль 4 Стратегії інформаційної безпеки 2021 року передбачає забезпечення дотримання прав особи на захист приватного життя.

У зв'язку із зазначеним треба звернути увагу та зробити відповідний аналіз змісту Резолюції Європейського парламенту від 12 березня 2014 року про програму спостереження АНБ США, органи спостереження в різних державах-членах та їхній вплив на фундаментальні права громадян ЄС і на трансатлантичне співробітництво у сфері юстиції та внутрішніх справ.

Ключові слова: національна безпека, державна безпека, інформаційна безпека, права і свободи людини і громадянина, Європейський Союз.

The article examines certain legal problems related to ensuring information security in Ukraine. The problems of clear formulation of interests in the field of information security are considered. The facts of the inaction of the authorized subjects regarding information espionage by the United States of America have been revealed.

In the Information Security Strategy, approved by the decree of the President of Ukraine dated December 28, 2021 No. 685/2021, the term "information security of Ukraine" is defined as an integral part of the national security of Ukraine, the state of protection of state sovereignty, territorial integrity, democratic constitutional order, and other vital human interests , society and the state, under which the constitutional rights and freedoms of a person to collect, store, use are properly ensured and dissemination of information, access to reliable and objective information, there is an effective system of protection and countermeasures against harm caused by the spread of negative informational influences, including the coordinated dissemination of false information, destructive propaganda, other information operations, unauthorized dissemination, use and violation of the integrity of information with limited access".

We believe that it is wrong, first of all, to narrow the term "information security" to one of its components, defining only how the phrase "information security of Ukraine" (that is, the state) should be understood.

As you know, strategic goal 4 of the Information Security Strategy of 2021 provides for ensuring compliance with the individual's rights to the protection of private life.

In connection with the above, it is necessary to pay attention and make an appropriate analysis of the content of the Resolution of the European Parliament dated March 12, 2014 on the US NSA surveillance program, surveillance bodies in various member states and their impact on the fundamental rights of EU citizens and on transatlantic cooperation in the field of justice and internal affairs.

Key words: national security, state security, information security, human and citizen rights and freedoms, European Union.

На наш погляд, неправильно, по-перше, звужувати термін «інформаційна безпека» до однієї з її складових, визначаючи лише те, як треба розуміти словосполучення «інформаційна безпека *України*» (тобто – держави). Тим більше, що виходячи із визначення терміну «забезпечення державної безпеки» у Стратегії забезпечення державної безпеки, затвердженій Указом Президента України від 16 лютого 2022 року № 56/2022, термін «державна безпека» розуміється як захищеність державного суверенітету, територіальної цілісності та демократичного конституційного ладу й інших життєво важливих національних інтересів від реальних і потенційних загроз Україні [2].

Тобто у двох указах Президента України наявне дуже схоже визначення різних термінів («інформаційна безпека» і «державна безпека»), що є юридично некоректним.

Зрозуміло, що інформаційна безпека є складовою державної безпеки. Але не можна забувати про те, що згідно загальноприйнятої точки зору є три об'єкти захисту у сфері інформаційної безпеки (так само це стосується сфер *національної* безпеки та *державної* безпеки): а) людина і громадянин, б) суспільство, і вже – в останню чергу – в) держава.

Саме такий підхід відповідає нормам Конституції України, зокрема її статті 3, згідно якої людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю [3].

Отже, в тому числі й *інформаційна безпека людини* визнається на рівні Основного Закону України найвищою соціальною цінністю.

По-друге, аналізуючи чинне визначення терміну «інформаційна безпека», необхідно констатувати ще одну

неточність: адже важко віднести захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу до числа життєво важливих інтересів *людини*. Скоріше, це є життєво важливими інтересами держави.

Також, як стверджується далі у Стратегії інформаційної безпеки, за умови функціонування механізму забезпечення інформаційної безпеки «належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації» [1].

Безумовно, дотримання державою права, передбаченого частиною другою статті 34 Конституції України, є важливим, але існують і більш важливі – з огляду на напрям даної Стратегії – права людини.

Якщо ми обговорюємо питання, що стосуються інформаційної безпеки людини, то більшою мірою слід наголошувати на забезпеченні прав людини на недоторканність її особистого і сімейного життя та на захист персональних даних.

При цьому, дотримання з боку державних інституцій вказаних конституційних прав і свобод людини є не якоюсь сверхзадачею, а кореспондуючим обов'язком держави (якщо це – не поліцейська, а демократична, правова держава, – як це закріплено у статті 1 Конституції України).

Таким чином, на наше переконання, визначення інформаційної безпеки у цій Стратегії слід доповнити фразою про необхідність належного забезпечення конституційних прав людини на недоторканність її особистого і сімейного життя та на захист персональних даних.

На нашу думку, якщо ми говоримо про феномен «інформаційної безпеки», необхідно відзначити фактичну недосяжність бажаного стану захищеності життєво важливих інтересів людини, суспільства і держави.

Забезпечення належного стану інформаційної безпеки, на нашу думку, потрібно розпочати з того, що на нормативно-правовому рівні будуть чітко сформульовані життєво важливі інтереси людини, суспільства, держави – окремо і по пунктах.

Цього у чинній Стратегії інформаційної безпеки немає взагалі. Слово «інтереси» використано по тексту в 11 випадках, але перелік інтересів відсутній.

Це є серйозним недоліком, оскільки тільки виходячи із переліку більш менш чітко сформульованих інтересів (у тому числі життєво важливих) людини і громадянина, суспільства і держави в інформаційній сфері можуть бути сформульовані загрози інформаційній безпеці (відповідно, людини і громадянина, суспільства і держави). А вже – як висновок з цього – завдання державної політики у вказаній сфері.

Стратегія інформаційної безпеки, як констатується у її розділі «Загальні положення», визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам [1].

Перелік актуальних викликів та загроз є, на нашу думку, занадто обмеженим, однобічним і не відображає всього спектру проблем у сфері забезпечення інформаційної безпеки.

У тексті Стратегії присутній термін «інформаційна загроза», сутність якого сформульовано як потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації *національних* інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні [1].

Одночасне посилання на можливість завдання шкоди і *національним* інтересам, і інтересам *держави, її національній безпеці та обороні* є, на наше переконання, зайвим.

Крім того, у тексті Стратегії зустрічаються терміни «гібридні загрози», «загрози в інформаційному просторі», «широкий спектр загроз, зокрема в інформаційній сфері», «потенційні та реальні загрози інформаційній безпеці України», які жодним чином не розтлумачуються, що створює простір для вільного трактування і наділення відповідних суб'єктів забезпечення інформаційної безпеки надмірною кількістю дискреційних повноважень.

Враховуючи вищевказане, слід наголосити, що за правилами нормопроектувальної техніки, терміни повинні бути зрозумілими однозначно. Інакше необхідно констатувати їх невідповідність вимозі щодо юридичної визначеності, яка є складовою принципу верховенства права.

Національні інтереси, у свою чергу, визначені у Стратегії національної безпеки, затвердженій указом Президента України від 14 вересня 2020 року № 392/2020. Так, згідно пункту 1 Стратегії людина, її життя і здоров'я, честь і гідність, недоторканність і безпека – найвища соціальна цінність в Україні. Реалізація цієї норми Конституції України – головна ціль державної політики національної безпеки [4].

Як відомо, стратегічна ціль 4 Стратегії інформаційної безпеки 2021 року передбачає забезпечення дотримання прав особи на захист приватного життя [1].

У зв'язку із зазначеним треба звернути увагу та зробити відповідний аналіз змісту Резолюції Європейського парламенту від 12 березня 2014 року про програму спостереження АНБ США, органи спостереження в різних державах-членах та їхній вплив на фундаментальні права громадян ЄС і на трансатлантичне співробітництво у сфері юстиції та внутрішніх справ (2013/2188(INI)) [5].

Необхідно наголосити, що окремі її пункти були використані в рішенні Європейського суду з прав людини від 12 січня 2016 року у справі «САБО І ВІШІ (SZABO AND VISSY) ПРОТИ УГОРЩИНИ» для обґрунтування порушення за статтею 8 ЄКПЛ (право на повагу до особистого життя) [6].

Крім того, необхідно вказати, що своє продовження Резолюція Європейського парламенту від 12 березня 2014 року знайшла у його ж Резолюції від 29 жовтня 2015 року і мала у підзаголовку відповідну назву: *щодо подальших дій на виконання резолюції Європейського парламенту від 12 березня 2014 року щодо електронного масового стеження за громадянами ЄС* [7].

Європейські парламентарі висловили значне занепокоєння з приводу існування системи широкомасштабного стеження за громадянами ЄС з боку США.

Зокрема, у Розділі «Вплив масового стеження» вказується наступне:

– захист даних і конфіденційність є основними правами;

– заходи безпеки, у тому числі заходи боротьби з тероризмом, повинні здійснюватися через верховенство права та повинні підпорядковуватися зобов'язанням у сфері фундаментальних прав, у тому числі тим, що стосуються конфіденційності та захисту даних;

– інформаційні потоки та дані, які сьогодні домінують у повсякденному житті та є частиною цілісності будь-якої людини, мають бути такими ж захищеними від вторгнення, як і приватні будинки;

– викриття, засновані на документах, оприлюднених колишнім співробітником Агентства національної безпеки США Едвардом Сноуденом, зобов'язують політичних лідерів вирішити проблеми нагляду та контролю за діяльністю розвідувальних служб та оцінки впливу їх діяльності на основні права та верховенство права в демократичне суспільство [5].

Викриття з червня 2013 року викликали численні занепокоєння в ЄС щодо:

– обсягів систем стеження, виявлених як у США, так і в країнах-членах ЄС;

– порушення правових стандартів ЄС, основних прав і стандартів захисту даних;

– можливості використання цих операцій масового спостереження з причин, відмінних від національної безпеки та боротьби з тероризмом у строгому сенсі, наприклад, економічне та промислове шпигунство або профілювання з політичних мотивів;

– підриву свободи преси та комунікацій представників професій, які мають право на конфіденційність, включаючи адвокатів і лікарів;

– все більш розмитих меж між діяльністю правоохоронних органів і розвідки, що призводить до того, що кожен громадянин розглядається як підозрюваний і підлягає нагляду;

– загрози конфіденційності в цифрову еру та впливу масового стеження на громадян і суспільства [5].

Влада США спростувала частину оприлюдненої інформації, але не заперечувала переважну її більшість.

Європейський парламент серйозно поставився до свого зобов'язання пролити світло на викриття практики невибіркового масового стеження за громадянами ЄС. При цьому, у Резолюції від 12 березня 2014 року підкреслюється, що згідно з відкритим меморандумом, поданим президенту Обамі колишніми керівниками вищої ланки АНБ/Ветеранами розвідки за розсудливість (VIPS) 7 січня 2014 року, масовий збір даних не покращує здатність запобігати майбутнім терористичним атакам [5].

Тобто, декларована мета програм масового стеження насправді не може бути досягнена завдяки їх використанню.

Отже, справжня мета таких програм є відмінною від декларованої.

Фундаментальні права, зокрема свобода вираження поглядів, преси, думки, совісті, релігії та асоціації, приватне життя, захист даних, а також право на ефективний засіб правового захисту, презумпцію невинуватості та право на справедливий суд і недискримінацію, як це закріплено в Хартії основних прав Європейського Союзу та в Європейській конвенції з прав людини, є наріжними каменями демократії.

Масове стеження за людьми несумісне з демократією.

В контексті зростаючої глобалізації та всесвітньої комунікації, законодавець ЄС стикається з новими проблемами щодо захисту персональних даних і комунікацій.

Діяльність з масового стеження дає розвідувальним службам доступ до персональних даних, які зберігаються або іншим чином обробляються особами з ЄС згідно з угодами про хмарні послуги з великими хмарними провайдерами США. Розвідувальні органи США отримали доступ до персональних даних, які зберігаються або іншим чином обробляються на серверах, розташованих на території ЄС, підключаючись до внутрішніх мереж Yahoo та Google;

Така діяльність, як вказується у Резолюції, є порушенням міжнародних зобов'язань та стандартів європейських основних прав, включаючи право на приватне та сімейне життя, конфіденційність комунікацій, презумпцію невинуватості, свободу вираження поглядів, свободу інформації, свободу зібрань та асоціацій та свободу вести бізнес; Парламентарі не виключали, що до інформації, яка зберігається в хмарних службах державними органами чи підприємствами та установами держав-членів, також мали доступ розвідувальні органи [5].

Також у Резолюції від 12 березня 2014 року вказано такі факти:

– розвідувальні служби США дотримуються політики систематичного підриву криптографічних протоколів і продуктів, щоб мати можливість перехопити навіть зашифроване спілкування;

– Агентство національної безпеки США зібрало величезну кількість так званих «експлойтів нульового дня» (вразливостей ІТ-безпеки, про які ще не відомо громадськості чи постачальнику продукту);

– така діяльність значно підриває глобальні зусилля щодо покращення ІТ-безпеки [5].

Далі, в Резолюції Європарламенту від 12 березня 2014 року зауважується, що розвідувальні служби в демократичних суспільствах наділені спеціальними повноваженнями та можливостями для захисту основних прав, демократії та верховенства права, прав громадян і держави від внутрішніх і зовнішніх загроз, а також підлягають демократичній підзвітності та судовому нагляду.

Але вони наділені спеціальними повноваженнями та можливостями лише з цією метою; відповідні повноваження повинні використовуватися в рамках правових обмежень, встановлених фундаментальними правами, демократією та верховенством права, а їх застосування має суворо перевірятися, оскільки інакше вони втрачають легітимність і ризикують підірвати демократію.

Європарламентарями зроблено наступні висновки.

1) Викриття в пресі інформаторами та журналістами разом із експертними свідченнями, наданими під час цього розслідування, визнаннями органів влади та недостатньою реакцією на ці звинувачення, призвели до переконливих доказів існування далекосяжних, складних і надзвичайно технологічно просунутих систем, розроблених розвідувальними службами США та деяких держав-членів для збору, зберігання та аналізу комунікаційних даних, у тому числі даних вмісту, даних про місцезнаходження та метаданих усіх громадян у всьому світі, у безпрецедентних масштабах, невибірково та без будь-яких обґрунтованих підозр (пункт 1);

2) Європарламент особливо вказує на розвідувальні програми АНБ США, які дозволяють здійснювати масове стеження за громадянами ЄС через:

– прямий доступ до центральних серверів провідних інтернет-компаній США (програма PRISM),

– аналіз вмісту та метаданих (програма Xkeyscore),

– обхід онлайн-шифрування (BULLRUN).),

– доступ до комп'ютерних і телефонних мереж, а також

– доступ до даних про місцезнаходження, а також до систем британського розвідувального агентства GCHQ. Що дає можливість збирання і зберігання 200 мільйонів текстових повідомлень на день (програма Dishfire) (пункт 2);

3) Європарламент засуджує широкомасштабне і систематичне збирання персональних даних невинуватих осіб, часто включаючи інформацію інтимного характеру; підкреслює, що використовувані службами розвідки системи невибіркового масового стеження являють собою серйозне втручання в основоположні права громадян; підкреслює, що право на приватність – це не розкіш, а основа вільного та демократичного суспільства; підкреслює далі, що масове стеження потенційно серйозно впливає на свободу слова, думки та поглядів, а також на свободу зібрань і асоціацій, а також породжує значний потенціал для зловживання при використанні інформації, зібраної відносно політичних противників; наголошує, що ця діяльність із масового стеження також тягне за собою незаконні дії спецслужб і викликає питання щодо екстериторіальності національних законів (пункт 10);

4) Європарламент вважає вкрай важливим, щоб професійна конфіденційність адвокатів, журналістів, лікарів та представників інших регульованих професій була захищена від заходів масового стеження; підкреслює, зокрема, що будь-яка невизначеність щодо конфіденційності спілкування між адвокатами та їхніми клієнтами може негативно вплинути на право громадян ЄС на доступ до юридичної консультації та доступ до правосуддя та право на справедливий судовий розгляд (пункт 11);

5) Європарламент розглядає програми стеження як ще один крок у напрямі до створення повноцінної превентивної держави, до зміни усталеної парадигми кримінального права в демократичних суспільствах, згідно з якою будь-яке втручання в основоположні права підозрюваних

має відбуватися за рішенням судді чи прокурора на підставі обґрунтованої підозри та повинно бути врегульовано законом, – з пропонуванням замість цього набору розвідувальних та правоохоронних заходів з розмитими та ослабленими правовими гарантіями, які часто не відповідають демократичним нормам стримувань і противаг і основоположним правам, особливо презумпції невинуватості; нагадує у зв'язку з цим про рішення Федерального конституційного суду Німеччини про заборону використання превентивних розшукових заходів («präventive Rasterfahndung»), за відсутності доказів конкретної небезпеки для інших охоронюваних законом прав високого рівня, в силу чого загальна загрозлива ситуація або міжнародна напруженість не є достатньою підставою для виправдання таких заходів (пункт 12);

6) Вищезазначені занепокоєння посилюються швидким технологічним і суспільним розвитком, оскільки Інтернет і мобільні пристрої є скрізь у сучасному повсякденному житті («повсюдне обчислення»), а бізнес-модель більшості інтернет-компаній базується на обробці персональних даних; Європарламент вважає, що масштаб цієї проблеми є безпрецедентним та зазначає, що це може створити ситуацію, коли інфраструктура для масового збору та обробки даних може використовуватися неправомірно у випадках зміни політичного режиму (пункт 14);

7) відсутні будь-які гарантії ані для державних установ ЄС, ані для громадян, що їхня ІТ-безпека чи конфіденційність можуть бути захищені від атак добре оснащених зловмисників (пункт 15).

Крім того, даними викриттями Едварда Сноудена зацікавилася і Парламентська Асамблея Ради Європи. Відповідно до пункту 13 Резолюції ПАРЄ № 1954 (2013) «Асамблея занепокоєна нещодавніми оприлюдненнями про величезні масштаби стеження секретними службами за комунікаціями і вирішила простежити за цим важливим питанням у доцільний час» [8].

Незважаючи на оприлюднені у 2013 році факти, програми стеження не були припинені з боку США. Як відзначається у публікації від 13 квітня 2024 року в газеті «Нью-Йорк таймс», великомасштабне стеження США за союзниками знову викликало широке невдоволення та гнів. У статті вказується, що конфіденційні документи Міністерства оборони США, які нещодавно були злиті у ЗМІ, викрили шпигунські операції країни по всьому світу; велика кількість співробітників американської розвідки розміщені та збирають розвіддані в "дружніх країнах" Сполучених Штатів, таких як Німеччина, Єгипет, Південна Корея, Україна, Арабські Емірати.

У статті відзначається, що дії США викликали невдоволення в країнах, за якими ведеться спостереження. Тисячі людей у Берліні вийшли на вулиці на знак протесту, Франція терміново викликала посла США у Франції для проведення розслідування, а президент Бразилії Лула скасував свій візит до Сполучених Штатів. У статті цитуються слова Міжнародного політолога Чарльза Купгана про те, що з того часу, як Едвард Сноуден розкрив інцидент з «воротами призми» у 2013 році, стеження США за союзниками стало загальновідомою «старою новиною». Опитування думок 44 країн по всьому світу, проведене Pew Center, показало, що понад 73% опитаних респондентів виступали проти таємного стеження у Сполучених Штатах [9].

Слід наголосити, що всі висновки, сформульовані у Резолюції Європарламенту від 12 березня 2014 року, нині є актуальними для України.

На наше переконання, програми масового стеження несумісні з принципами демократичного суспільства, в першу чергу, з принципом верховенства права. Вони є актуальною загрозою національній безпеці та її складовим: інформаційній, державній, економічній безпеці.

Виявлена присутність співробітників американської розвідки, які розміщені та збирають розвідувальні дані зокрема і в Україні, у поєднанні з розслідуванням щодо програм масового стеження, проведеним за ініціативою Європарламенту, результати якого відображені у Резолюції від 12 березня 2014 року № 2013/2188, прямо свідчить про масштаби загрози інформаційній безпеці людини і громадянина, суспільства та держави Україна.

Але з боку уповноважених у сфері забезпечення інформаційної безпеки суб'єктів, зокрема Ради національної безпеки і оборони України, Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України жодних заяв з цього приводу немає.

З незрозумілих причин немає і заяв політичного характеру з боку керівництва нашої держави.

ЛІТЕРАТУРА

1. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 22.05.2024).
2. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки": Указ Президента України від 16.02.2022 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text (дата звернення: 22.05.2024).
3. Конституція України від 28.06.1996 р. (в редакції від 01.01.2020) https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 22.05.2024).
4. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки": Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n12 (дата звернення: 22.05.2024)
5. Резолюція Європейського парламенту від 12 березня 2014 року про програму спостереження АНБ США, органи спостереження в різних державах-членах та їхній вплив на фундаментальні права громадян ЄС і на трансатлантичне співробітництво у сфері юстиції та внутрішніх справ (2013/2188(INI)). URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52014IP0230 (дата звернення: 22.05.2024).
6. Резолюція Європейського парламенту від 29 жовтня 2015 року щодо подальших дій на виконання резолюції Європейського парламенту від 12 березня 2014 року щодо електронного масового стеження за громадянами ЄС (2015/2635(RSP)) (2017/C 355/07). URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52015IP0388 (дата звернення: 22.05.2024).
7. Рішення Європейського суду з прав людини від 12 січня 2016 року у справі «САБО І ВІШІ (SZABO AND VISSY) ПРОТИ УГОРЩИНИ». URL: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-160020%22]} (дата звернення: 22.05.2024).
8. Національна безпека та доступ до інформації. Резолюція Парламентської асамблеї Ради Європи № 1954 (2013). URL: https://w1.c1.rada.gov.ua/pls/mpz2/docs/1824_rez_1954_(2013).htm (дата звернення: 22.05.2024).
9. "Нью-Йорк таймс" заявила, що широкомасштабне стеження за союзниками з боку США вкотре викликало широке невдоволення» URL: https://ukrainian.cri.cn/2023/04/17/ARTI6IByMyg6E5IbQbI1cbkM230417.shtml (дата звернення: 22.05.2024).