Гарантії прав людини та громадянина при забезпеченні інформаційної безпеки

Human and Citizen Rights Guarantees While Providing Information Security

Сергій Єсімов [1], **Ростислав Сопільник** [2], **Мирослав Ковалів** [1], **Руслан Скриньковський** [2]
Serhii Yesimov, Rostyslav Sopilnyk, Myroslav Kovaliv, Ruslan Skrynkovskyy

[1] *Lviv State University of Internal Affairs*
26 Horodotska Street, Lviv, 79007, Ukraine

[2] *Lviv University of Business and Law*
99 Kulparkivska Street, Lviv, 79021, Ukraine

DOI: 10.22178/pos.34-6

JEL Classification: K30

Received 20.04.2018
Accepted 20.05.2018
Published online 28.05.2018

Corresponding Author:
Rostyslav Sopilnyk
sopilnyk01@gmail.com

Анотація. З розвитком інформаційних і комунікаційних технологій загострюються проблеми забезпечення інформаційної безпеки. Йдеться про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, про пропаганду сепаратизму та екстремізму тощо.

При забезпеченні інформаційної безпеки в цифровому середовищі зростає роль техніко-юридичних (технічних) гарантій прав людини, за рахунок технічних засобів захисту. Покладання на розробників технічних засобів обов'язків визначає відмінність вищевказаних концепцій від традиційного підходу до забезпечення захисту прав людини та громадянина, при якому обов'язки покладаються на інформаційних посередників, власників конфіденційної інформації.

Технічні гарантії прав людини стають необхідною складовою забезпечення інформаційної безпеки, але ефективність застосування забезпечується у поєднанні з правовими гарантіями прав людини, на що вказує тенденція визнання принципів недоторканності приватного життя на основі проектних рішень у праві Європейського Союзу в якості правових актів.

Забезпечення інформаційної безпеки виступає легітимною метою встановлення обмежень прав людини, оскільки це може бути співвіднесено з нормами міжнародного права. Встановлення обмежень прав людини допускається для досягнення інших цілей – забезпечення державної безпеки, публічного порядку, здоров'я, прав і свобод особи в інформаційній сфері. Легітимність цієї мети визначається її відповідністю цілям, передбачених міжнародними договорами, ратифікованими у встановленому порядку.

У статті розглянуто вплив застосування технічних засобів у сфері забезпечення інформаційної безпеки в аспекті дотримання основоположних прав людини та громадянина в Україні з урахуванням законодавства Європейського Союзу та рішення Європейського суду справедливості. Здійснено порівняльно-правовий аналіз різних чинників, що впливають на обмеження інформаційних прав людини у цифровому середовищі. Розкрито правові гарантії з погляду на концепції недоторканності приватного життя та безпеки за рахунок проектних рішень, з урахуванням ролі та особливостей технічного примусу.

Ключові слова: права людини та громадянина; інформаційна безпека; застосування технічних засобів; правові гарантії.

Abstract. With the development of information and communication technologies, issues of providing information security are becoming more and more aggravated. These are crimes related to the use of electronic computers, systems and computer networks and telecommunication networks, the propaganda of separatism and extremism, etc.

While providing information security in the digital environment, the role of technical and legal human rights guarantees, due to technical means of protection, is increasing. Relying on the developers of technical means of protection determines the difference between the aforesaid concepts and the traditional approach to ensuring the protection of human and citizen rights, in which responsibilities are put on information intermediaries, owners of confidential information.

Technical guarantees of human rights are a necessary component of ensuring information security, but the effectiveness of the application is provided in conjunction with the legal guarantees of human rights, as evidenced by the tendency to recognize the principles of inviolability of privacy on the basis of design decisions in the law of the European Union as legal acts.

Providing information security is a legitimate goal of establishing constraints of human rights, since it can be correlated with the norms of international law. The establishment of constraints of human rights is permissible in order to attain other objectives–ensuring state security, public order, health, rights and freedoms of the person in the information sphere. The legitimacy of this goal is determined by its compliance with the objectives envisaged by international agreements ratified in an established order.

The article examines the impact of the use of technical means in the field of providing information security in the aspect of following the fundamental human and civil rights in Ukraine, taking into account the legislation of the European Union and the decision of the European Court of Justice. The comparative and legal analysis of various factors influencing the restriction of information rights of people in the digital environment is carried out. Legal guarantees from the point of view of the concept of privacy and security due to design decisions, taking into account the role and characteristics of technical primus are revealed.

Keywords: human and civil rights; informational security; application of technical means; legal guarantees.

ВСТУП

У зв'язку з активним використанням інформаційно-телекомунікаційних систем та технологій, зокрема Інтернет, зросла кількість загроз мережевих атак з метою несанкціонованого доступу в автоматизовані інформаційні системи державних і комерційних організацій для отримання конфіденційної інформації, забезпечення збоїв в роботі систем, перехоплювання управління критично важливими об'єктами. З розвитком інформаційних і комунікаційних технологій загострюються проблеми забезпечення інформаційної безпеки. Йдеться про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, про пропаганду сепаратизму та екстремізму тощо. Удосконалення правого регулювання забезпечення передбачено Планом заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом (ЄС), Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, затвердженого постановою Кабінету Міністрів України від 25 жовтня 2017 р. № 1106.

Теоретичну основу дослідження склали наукові здобутки таких провідних вчених, як: В. Авер'янова, В. Баскакова, В. Бєлєвцевої, В. Брижка, К. Джонсона, Є. Збінського, В. Ліпкана, Л. Колобова, І. Колеснікової, Р. Кохейна, О. Курмана, Дж. Ная, О. Семенюка, О. Смоляк, О. Огданської, В. Пилипчука, В. Тарана, В. Щербаченко та ін. Водночас при-

йняття Доктрини інформаційної безпеки України та реалізація положень Стратегії кібербезпеки України ставить питання удосконалення системи гарантій прав людини при забезпеченні інформаційної безпеки.

Тому *метою статті* є дослідження гарантій прав людини та громадянина при забезпеченні інформаційної безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Доктрина інформаційної безпеки України розглядає забезпечення інформаційної безпеки як один з видів діяльності і як засіб діяльності, спрямованої на безпечне функціонування та розвиток національного інформаційного простору і його інтеграція у європейський та світовий інформаційний простір. Таку діяльність здійснюють громадяни, інститути громадянського суспільства та державні органи, забезпечуючи життєво важливі інтереси особи, суспільства та держави в інформаційній сфері.

На думку А. Нашинець-Наумової, важливим підґрунтям удосконалення інформаційного законодавства є адекватне сучасним умовам відображення у свідомості нормотворців інформаційної безпеки у всій повноті аспектів, зокрема психологічному, технічному та правовому [1, с. 8]. У країнах ЄС інформаційна безпека спрямована на створення умов, при яких забезпечується стан захищеності прав людини в інформаційній сфері, як основна мета і цінність інформаційної безпеки. В результаті інформаційна безпека стає однією з гарантій прав людини та громадянина в інформаційній сфері.

Під гарантіями прав людини та громадянина розуміють систему умов, засобів і способів, за допомогою яких забезпечуються рівні можливості для здійснення, забезпечення охорони і захисту прав людини та громадянина. Забезпечення інформаційної безпеки як гарантія прав людини нерозривно пов'язана з іншими видами гарантій і в них знаходить своє вираження. Комітет Міністрів Ради Європи в Рекомендації CM/Rec (2014) («Посібник з прав людини для Інтернет-користувачів») зазначає, що існуючі права людини та основні свободи в рівній мірі відносяться як до оффлайн, так і до онлайн простору. Ніхто не повинен бути об'єктом незаконного втручання в здійснення прав людини і основних свобод під час перебування в Інтернеті [2]. Комплекс гарантій, якими забезпечується здійснення і захист прав людини в оффлайн-середовищі, поширюється на права людини в кіберпросторі і цифровому середовищі.

Фахівець Л. Тарасенко зазначає, що цифрове середовище – це ширше поняття, ніж мережа Інтернет. Цифрове середовище включає у себе не лише веб-сайти (і веб-сторінки як складові веб-сайтів), а й електронні документи, файли, в т.ч. оцифровані об'єкти інтелектуальної власності [3].

Умови захисту прав людини в цифровому і оффлайн середовищах розрізняються. З погляду на Стратегію кібербезпеки України, для цифрового середовища характерні технічні гарантії прав людини, які представлені у формі технічних і програмних засобів та технічних норм. Технічні та програмні засоби (далі – технічні засоби) охоплюють обчислювальні машини та спеціалізовані пристрої на їх основі, операційні системи, системи програмування, загальносистемне та прикладне програмне забезпечення [4, с. 121]. Техніко-юридичні норми визначають умови проектування, виготовлення та використання технічних засобів. При забезпеченні інформаційної безпеки в цифровому середовищі зростає роль техніко-юридичних (далі – технічних) гарантій прав людини, за рахунок технічних засобів захисту. У зазначеному аспекті, доцільно погодитися з думкою О. Харитонової та інших вчених, що Інтернет-відносини – це новий тип суспільних відносин, які виникають, змінюються та припиняються в кіберпросторі [5, с. 160].

Технічнім гарантіям прав людини відповідають концепції «недоторканність приватного життя за рахунок проектних рішень» і «безпека за рахунок проектних рішень».

Недоторканність приватного життя за рахунок проектних рішень передбачає вбудовану в технічні засоби систему захисту інформації про особу, при якій виключається її передача іншим особам. Безпека за рахунок проектних рішень не обмежена захистом права на недоторканність приватного життя, але і охоплює захист прав усіх учасників інформаційної взаємодії, що допускає передачу конфіденційної інформації, необхідної для захисту прав ін-

ших осіб. Принципи недоторканності приватного життя за рахунок проектних рішень сформульовані *A. Cavoukian* [6]: проактивність (профілактичний не корекційний вплив); конфіденційність як параметр за замовчуванням; конфіденційність вбудована в дизайн; повна функціональність; постійна безпека (повний захист життєвого циклу); видимість і прозорість; повага до конфіденційності користувачів.

Принципи безпеки за рахунок проектних рішень засновані на забезпеченні безпеки для всіх учасників інформаційної взаємодії: принцип мінімальної привілеї рекомендує, щоб облікові записи мали найменшу кількість привілеїв, необхідних для виконання бізнес-процесів; принцип захисту в глибині говорить про те, що елементи управління використовуються з умовою забезпечити баланс інтересів усіх учасників; за допомогою безпечного кодування можна мати форму багаторазової перевірки [7]. Дана концепція не орієнтована на захист виключно або переважно прав особи, що використовує технічні засоби.

Покладання на розробників технічних засобів обов'язків визначає відмінність вищевказаних концепцій від традиційного підходу до забезпечення захисту прав людини, при якому обов'язки покладаються на інформаційних посередників, власників конфіденційної інформації. Виробники технічних засобів (*Microsoft, Hewlett-Packard, Sun Microsystems, IBM* тощо) впровадили принципи недоторканності приватного життя за рахунок проектних рішень. На думку *Ira S. Rubinstein, Google, Facebook, Twitter* та інші сервіси недоторканність приватного життя забезпечуватимуть при розробці та удосконаленні програмного забезпечення [8, с. 1389, 1401].

Технічні гарантії прав людини стають необхідною складовою забезпечення інформаційної безпеки, але ефективність застосування забезпечується у поєднанні з правовими гарантіями прав людини, на що вказує тенденція визнання принципів недоторканності приватного життя на основі проектних рішень у праві Європейського Союзу в якості правових актів.

Вчений П. Сухорольський зазначає, що за останні роки звичним для багатьох став факт, що оператори пошукових систем чи соціальних мереж мають власну політику щодо свободи і обмежень в Інтернеті та накладають обмежувальні заходи на основі самостійно розроблених критеріїв і способів бачення міжнародних проблем. Це свідчить про поступове набуття ними функцій із регулювання суспільних відносин [9, с. 346].

Без визнання та дотримання базових правових принципів забезпечення інформаційної безпеки на основі принципів недоторканності приватного життя за рахунок проектних рішень не зможе виступати гарантією відповідного права людини. Правові гарантії спрямовані на визначення порядку застосування технічних засобів, забезпечення контролю дотримання технічних вимог (стандартів, регламентів), реалізації відповідальності за порушення. У правовій державі створення та введення в дію технічних норм, на підставі яких здійснюється розробка відповідних технічних засобів не замінює, а доповнює правове регулювання.

Технічні засоби можуть виступати гарантією прав людини тільки при наявності правових гарантій, які надають механізми правового захисту від їх довільного використання. Такі правові гарантії забезпечуються державою у межах здійснення функції забезпечення безпеки суспільства в цілому та реалізуються на основі Законів України від 15.01.2015 р. № 124-VIII «Про технічні регламенти та оцінку відповідності», від 05.06.2014 р. № 1314-VII «Про метрологію та метрологічну діяльність», інших нормативно-правових актів.

Забезпечення інформаційної безпеки виступає однією з цілей, для досягнення якої встановлюються обмеження прав людини. Водночас принцип правової держави не зводиться до захисту людини від державних домагань, а переслідує мету в рівній мірі обмежувати та забезпечувати діяльність держави.

Конституційний Суд України вважає, що обмеження щодо реалізації конституційних прав і свобод не можуть бути свавільними та несправедливими, вони мають встановлюватися виключно Конституцією і законами України, переслідувати легітимну мету, бути обумовленими суспільною необхідністю досягнення цієї мети, пропорційними та обґрунтованими, у разі обмеження конституційного права або свободи законодавець зобов'язаний запровадити таке правове регу-

лювання, яке дасть можливість оптимально досягти легітимної мети з мінімальним втручанням у реалізацію цього права або свободи і не порушувати сутнісний зміст такого права [10]. Зазначене забезпечується у першу чергу у контексті реалізації принципу правової пропорційності.

Європейським судом з прав людини для вироблення однакового підходу до застосування в практиці національних судів і Суду справедливості Європейського Союзу, сформульовано критерії, що визначають межі обмежень прав людини. Обмеження повинні бути встановлені: для досягнення легітимної мети; дійсно сприяти її досягненню; бути мінімально необхідними та пропорційними в строгому сенсі.

Роль принципу пропорційності полягає у зіставленні заходів, які вживаються органами державної влади для забезпечення інформаційної безпеки, з правами людини. Принцип пропорційності є універсальним в тому сенсі, що він застосовний для перевірки легітимності будь-яких обмежень прав людини, встановлених з метою забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки виступає легітимною метою встановлення обмежень прав людини, оскільки це може бути співвіднесено з нормами міжнародного права. Встановлення обмежень прав людини допускається для досягнення інших цілей – забезпечення державної безпеки, публічного порядку, здоров'я, прав і свобод особи в інформаційній сфері. Легітимність цієї мети визначається її відповідністю цілям, передбачених міжнародними договорами, ратифікованими у встановленому порядку.

В Україні забезпечення інформаційної безпеки як мета обмеження прав людини розглядається в Конституції України у частині 3 статті 34, згідно з якою здійснення прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Судова перевірка пропорційності обмежень прав людини дозволяє виявити нерелевантні обмеження при оцінці їх відповідності тієї мети, для досягнення якої вони були встановлені. Висновок про нерелевантність обмеження прав людини, що полягає в суцільній фільтрації та блокуванні обміну повідомленнями в файлообмінних мережах, міститься в різних рішеннях Суду справедливості Європейського Союзу. Обмеження, встановлені з метою захисту авторських прав, визнавалися судом такими, що порушують свободу вираження поглядів і права на недоторканність приватного життя, оскільки зачіпали обмін повідомленнями, не пов'язаними з використанням об'єктів авторських прав. Для забезпечення релевантності недостатньо часткової відповідності обмеження прав людини щодо мети встановлення. Обмеження не є релевантним, якщо між кожним випадком реалізації і метою встановлення відсутній раціональний зв'язок, при якому обмеження неминуче веде до результату, відповідного досягненню заданої мети. Нерелевантні обмеження в даному випадку обумовлені технічними особливостями способу реалізації. Блокування сайту в Інтернеті інформаційним посередником за рішенням суду або органу виконавчої влади на основі відомостей про IP-адресу сайту може призводити до одночасного блокування інших сайтів, які прив'язані до цієї IP-адреси. Відповідність обмеження прав людини при забезпеченні інформаційної безпеки в мережі Інтернет щодо цілі встановлення залежить від особливостей реалізації, через які навіть за умови легітимності цілі обмеження може стати нелегітимним.

При забезпеченні інформаційної безпеки правове регулювання доповнюється саморегулюванням, що створює умови для вирішення конфліктів з мінімальною участю органів державної влади, втручання яких в основному обмежується притягненням до відповідальності за правопорушення. Саморегулювання при забезпеченні інформаційної безпеки здійснюється відповідно до принципу субсидіарності, який полягає в тому, що регулюючий вплив носить додатковий характер щодо правового регулювання завдяки використанню технічних засобів.

Провайдери доступу до мережі Інтернет, у межах угод між органами державної влади та

провайдерами, утворюють гарячі лінії, приймають кодекси поведінки галузевих асоціацій, розвивають інші форм партнерства між державою та недержавними організаціями, на основі яких інформаційні посередники здійснюють блокування та фільтрацію інформації, тим самим обмежуючи свободу вираження поглядів та право на доступ до інформації.

Обмеження прав людини в цифровому середовищі, формально закріплені в нормативно-правових актах, доповнюються фактичними обмеженнями, що виражаються в обов'язках здійснення дій технічного характеру, які покладаються на розробників технічних засобів і інформаційних посередників. Такі обов'язки встановлюються або технічними нормами, або актами правозастосування.

Технічний характер обмежень прав людини обумовлений тим, що сфера здійснення прав людини з використанням Інтернет спочатку обмежена функціональними можливостями технічних засобів, за допомогою яких людина отримує доступ до кіберпростору або користується певними соціальними благами. Зміна або використання даних функціональних можливостей призводить до розширення сфери реалізації або обмеження прав людини.

Покладаючи на розробників технічних засобів і інформаційних посередників обов'язки, органи державної влади фактично обмежують права осіб, які використовують відповідні технічні засоби або отримують послуги інформаційних посередників. У даному випадку здійснюється примусове виконання рішень органів державної влади навіть у випадках, коли особа, права якої обмежують, знаходиться за межами національної території. Примус особи до певної поведінки досягається за рахунок створення умов, при яких інша поведінка стає неможливою. В ЄС допускається тільки примус, який має правові підстави та процедурно-правові форми здійснення. При дотриманні даних умов примус не створює надмірних обмежень прав людини по відношенню до тих, які передбачені законом.

Примус в інформаційній сфері, що здійснюється з використанням технічних засобів, може стати одним із способів забезпечення доступу державних органів до інформації про особу і, тим самим, виступає в якості обмеження права на недоторканність приватного життя.

Не всі інформаційні посередники надають державним органам інформацію за запитами, особливо ті, які розташовані за межами національної території. Отримуючи доступ до інформації, державні органи не завжди мають можливість встановити її зміст через застосовуваних засобів шифрування. Наслідком є вироблення заходів технічного примусу, в результаті застосування яких забезпечується доступ державних органів до інформації незалежно від волі інформаційних посередників або особи.

У результаті відбувається підміна прав людини, які фактично піддаються обмеженням, обов'язками юридичних осіб, які здійснюють діяльність в інформаційній сфері. Європейський суд з прав людини підходить до питань легітимності технічного примусу на основі принципу пропорційності, тобто аналізуючи легітимність покладання обов'язків на інформаційних посередників і розробників технічних засобів у контексті легітимності пов'язаних з ними обмежень прав людини в онлайн-середовищі.

На думку Європейського суду з прав людини, висловлену у справі «Класс та інші проти Німеччини», право ведення таємного спостереження за громадянами, яке характерно для поліцейської держави, терпимо відповідно до Конвенції тільки тоді, коли воно суворо необхідно для збереження демократичних інститутів. Держави не можуть в ім'я боротьби проти шпигунства та тероризму робити дії, які вони вважають потрібними [12].

Загальний регламент захисту даних (англ. *General Data Protection Regulation, GDPR; Regulation (EU) 2016/679*) забороняє передачу персональних даних громадян держав – членів Європейського Союзу в держави, що не входять до Європейського економічного співтовариства. Винятком є передача персональних даних третім країнам, які забезпечують адекватний рівень захисту. Водночас прийнято: Директиву (ЄС) 2016/680 Європейського Парламенту і Ради від 27.04.2016 р. «Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення або переслідування злочинця злочину або виконання кримінальних покарань, а також про вільне переміщення таких даних, і скасування Рамкового рішення Ради

2008/977/ПВД»; Директиву (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.2016 р. «Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину» [13, с. 47].

Вступ у дію Загального регламенту захисту даних Європейського Союзу дозволив вирішити юридичні і технічні проблеми, які виникнули між ЄС і США у 2015–2026 рр. у сфері обміну персональними даними за схемою «безпечної гавані» [14].

Підхід до питань легітимності технічного примусу в Україні відповідає вимогам Європейського Союзу. Цей підхід, зокрема, виражається в обов'язки оператора персональних даних, який здійснює збір персональних даних, в тому числі за допомогою мережі Інтернет, забезпечувати запис, систематизацію, накопичення, зберігання, уточнення (оновлення, зміна), витяг персональних даних громадян України з використанням баз даних, що знаходяться на території України. Законодавець визначає вимоги до місцезнаходження баз даних, в яких містяться персональні дані, незалежно від волі суб'єктів персональних даних.

Знаходження відповідних баз даних на території України, з одного боку, спрощує контроль і нагляд за відповідністю обробки персональних даних вимогам законодавства України у сфері персональних даних і одночасно доступ до баз даних для органів виконавчої влади, але з іншого – призводить до обмеження прав суб'єктів персональних даних, які при визначенні способу їх обробки вже позбавлені можливості самостійно визначати територію його реалізації.

Покладання на інформаційних посередників відповідних обов'язків забезпечує додаткові умови для запобігання, припинення та розслідування злочинів, але й створює мінімальні ризики для необґрунтованого втручання в приватне життя.

Легітимність забезпечення інформаційної безпеки як цілі щодо здійснення технічного примусу не викликає сумніву. Однак, для визнання легітимності самого технічного примусу недостатньо підвести правові підстави під відповідні обов'язки розробників технічних засобів і інформаційних посередників. Умовою легітимності є створення правових гарантій прав людини, на які накладаються обмеження в результаті виконання обов'язків розробників технічних засобів і інформаційних посередників.

ВИСНОВКИ

Розвиток правових гарантій прав людини, виражених в деталізації матеріальних і процесуальних правових норм, на підставі яких здійснюються обмеження, є тенденцією в Європейському Союзі. Забезпечення інформаційної безпеки є однією з гарантій прав людини та громадянина в інформаційній сфері, яка нерозривно пов'язана з іншими видами гарантій, де знаходить своє вираження. У цифровому середовищі зростає роль технічних гарантій, виражених в технічних засобах та технічних нормах.

У Європейському Союзі створення та введення в дію технічних норм, на підставі яких здійснюється розробка відповідних технічних засобів не замінює, а доповнює правове регулювання. Технічні засоби можуть виступати гарантією прав людини тільки при наявності правових гарантій, які надають механізми правового захисту від довільного використання. Водночас забезпечення інформаційної безпеки виступає підставою для обмеження прав людини. Створення правових гарантій прав людини від надлишкових і надмірних обмежень з метою забезпечення інформаційної безпеки, засновано на принципі пропорційності. Поряд з правовими обмеженнями прав людини при забезпеченні інформаційної безпеки відбувається розвиток фактичних обмежень, які виражені в технічному примусі, що полягає в покладанні обов'язків на інформаційних посередників і розробників технічних засобів, виконання яких впливає на межі прав людини. Для легітимності технологічного примусу мало юридичного закріплення обов'язків розробників технічних засобів і інформаційних посередників. Легітимність обумовлена деталізацією правового регулювання, яке виступаючи підставою для технічного примусу, що дозволяє створити правові гарантії від надлишкових і надмірних обмежень прав людини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES

1. Nashynets-Naumova, A. Yu. (2017). *Informatsiina bezpeka: pytannia pravovoho rehuliuvannia* [Information security: issues of legal regulation]. Kyiv: Helvetyka (in Ukrainian)
[Нашинець-Наумова, А. Ю. (2017). *Інформаційна безпека: питання правового регулювання*. Київ: Гельветика].

2. Voron, M. (2016). *Prava liudyny v Interneti* [Human rights on the Internet]. Retrieved April 1, 2018, from http://nmcio.ippo.kubg.edu.ua/?p=2213 (in Ukrainian)
[Ворон, М. (2016). *Права людини в Інтернеті*. Актуально на 01.04.2018. URL: http://nmcio.ippo.kubg.edu.ua/?p=2213].

3. Tarasenko, L. L. (n. d.). *Tsyfrove seredovyshche yak mistse zdiisnennia prav intelektualnoi vlasnosti* [The digital environment as a place of realization of intellectual property rights]. Retrieved April 1, 2018, from https://goo.gl/HYymYb (in Ukrainian)
[Тарасенко, Л. Л. (н. д.). *Цифрове середовище як місце здійснення прав інтелектуальної власності*. Актуально на 01.04.2018. URL: https://goo.gl/HYymYb].

4. Pavlysh, V. A., & Holinenko, L. K. (2013). *Osnovy informatsiinykh tekhnolohii i system* [Fundamentals of Information Technology and Systems]. Lviv: Lvivcka politekhnika (in Ukrainian)
[Павлиш, В. А., & Голіненко, Л. К. (2013). *Основи інформаційних технологій і систем*. Львів: Львівська політехніка].

5. Kharytonova, O. I., Ulianova, H. O., Kyryliuk, A. V., Symonian, Yu. Yu., Baadzhy, N. P., Pozova, D. D. …, Martyniuk, I. V. (2015). Problemni pytannia vyznachennia pravovoi pryrody i struktury pravovidnosyn intelektualnoi vlasnosti, shcho vynykaiut u merezhi Internet [Problematic issues of determining the legal nature and structure of intellectual property rights arising in the Internet]. *Naukovi pratsi NU OIuA*, 159–200 (in Ukrainian)
[Харитонова, О. І., Ульянова, Г. О., Кирилюк, А. В., Симонян, Ю. Ю., Бааджи, Н. П., Позова, Д. Д. …, Мартинюк, І. В. (2015). Проблемні питання визначення правової природи і структури правовідносин інтелектуальної власності, що виникають у мережі Інтернет. *Наукові праці НУ ОЮА*, 159–200].

6. Privacy by Design Centre of Excellence. (n. d.). *The Seven Foundational Principles*. Retrieved April 1, 2018, from https://goo.gl/ofgwa6

7. The Open Web Application Security Project (OWASP). (2016). *Security by Design Principles*. Retrieved April 1, 2018, from https://www.owasp.org/index.php/Security_by_Design_Principles

8. Rubinstein, I., & Good, N. (2012). Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2128146

9. Repetskyi, V. M., & Hutnyk, V. V. (Ed.) (2017). *Suchasni problemy mizhnarodnoho prava. Liber Amicorum do 60-richchia prof. M. V. Buromenskoho* [Current problemsof international law. Liber Amicorum Professor Mykhaylo Buromenskiy in Honour of His 60th Birthday]. Lviv, Odesa: Feniks (in Ukrainian)
[Репецький, В. М., & Гутник, В. В. (Ред.) (2017). *Сучасні проблеми міжнародного права. Liber Amicorum до 60-річчя проф. М. В. Буроменського*. Львів, Одеса: Фенікс].

10. Rishennia Konstytutsiinoho Sudu Ukrainy [Decision of the Constitutional Court of Ukraine] (Ukraine), 01 June 2016, No 2-рп/2016. Retrieved April 1, 2018, from http://zakon2.rada.gov.ua/laws/show/v002p710-16 (in Ukrainian)
[Рішення Конституційного Суду України (Україна), 01 червня 2016, № 2-рп/2016. Актуально на 01.04.2018. URL: http://zakon2.rada.gov.ua/laws/show/v002p710-16].

11. Barak, A. (2012). *Proportionality: Constitutional rights and their limitations*. New York: Cambridge University Press.

12. Class and Others v. Germany (Council of Europe, European Court of Human Rights), 06 September 1978. Retrieved April 1, 2018, from http://zakon5.rada.gov.ua/laws/show/980_093 (in Ukrainian)

[Класс та інші проти Німеччини (Рада Європи, Європейський Суд з прав людини), 06 вересня 1978. Актуально на 01.04.2018. URL: http://zakon5.rada.gov.ua/laws/show/980_093].

13. Bryzhko, V. M. (2016). Suchasni osnovy zakhystu personalnykh danykh v yevropeiskykh pravovykh aktakh [Modern bases of protection of personal data in European legal acts]. *Informatsiia i pravo, 3*(18), 45–57 (in Ukrainian)
[Брижко, В. М. (2016). Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і право, 3*(18), 45–57].
14. European Commission. (2017). *EU – U.S. Privacy Shield – First annual Joint Review*. Retrieved April 1, 2018, from https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/12/WP-29-Privacy-Shield-Opinion.pdf