Міжнародне право

УДК 342.9

Поперечна Ганна Михайлівна
доктор філософії у галузі права, доцент,
доцент кафедри міжнародного права та міграційної політики
Західноукраїнський національний університет
Poperechna Hanna
PhD in Law, Associate Professor,
Associate Professor of the Department of International Law and Migration Policy
West Ukrainian National University
ORCID: 0000-0001-6978-4892

Поперечний Юрій Юрійович
військовослужбовець
Poperechnyi Iurii
Military Serviceman

ГАРАНТІЇ ПРАВ ЛЮДИНИ В УМОВАХ ДЕРЖАВНОГО ВТРУЧАННЯ У СФЕРУ КІБЕРБЕЗПЕКИ: РИЗИКИ ТА ПРАВОВІ ОБМЕЖЕННЯ

HUMAN RIGHTS GUARANTEES IN THE CONTEXT OF STATE INTERFERENCE IN CYBERSECURITY: RISKS AND LEGAL CONSTRAINTS

Анотація. *Вступ. Впровадження цифрових технологій у всі сфери життя змінює уявлення про простір, у якому реалізуються права людини, та висуває нові вимоги до їх правового захисту. У відповідь на зростання кіберзагроз держави все частіше застосовують заходи кібербезпеки, що включають моніторинг, збір даних, обмеження доступу до інформації та алгоритмічну модерацію контенту. Це зумовлює потребу в науковому*

аналізі ризиків державного втручання у сферу кібербезпеки та в розробці ефективних правових механізмів захисту прав людини відповідно до міжнародних стандартів.

Мета. Метою дослідження є здійснення правового аналізу гарантій захисту прав людини в умовах державного втручання у сферу кібербезпеки, зокрема з урахуванням потенційних ризиків для основоположних прав і свобод, а також визначення меж допустимого втручання відповідно до міжнародних стандартів та принципу верховенства права.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правові акти Організації об'єднаних націй, Ради Європи та Європейського Союзу у сфері захисту прав людини та основоположних свобод; 2) національні законодавчі акти, що регулюють діяльність органів державної влади у сфері кібербезпеки; 3) практика Суду справедливості ЄС; 4) положення української та зарубіжної доктрини.

У процесі дослідження застосовувалися загальнонаукові та спеціально-юридичні методи. Метод правового аналізу дозволив виявити основні ризики для прав людини, що виникають у зв'язку з державним втручанням у цифровий простір. Порівняльно-правовий метод був використаний для зіставлення підходів міжнародних та національних правових систем щодо меж допустимого втручання у сферу кібербезпеки. Системно-функціональний підхід дозволив розглянути співвідношення цілей кібербезпеки з принципами прав людини. Метод узагальнення забезпечив цілісне бачення проблеми та інтерпретацію отриманих результатів.

Результати. У статті проаналізовано правові ризики порушення прав людини, що виникають у зв'язку з державним втручанням у сферу кібербезпеки. Визначено основні виклики, пов'язані з застосуванням заходів державного контролю над цифровим середовищем, зокрема масового спостереження, збору даних, алгоритмічної модерації контенту та обмеження доступу до інформації. Розкрито межі допустимого втручання

держави відповідно до міжнародних стандартів захисту прав людини. Обґрунтовано необхідність посилення демократичного контролю за діяльністю органів, що діють у сфері кібербезпеки, та вдосконалення нормативного регулювання з урахуванням принципу пропорційності, правової визначеності та недопущення зловживань.

Перспективи. Подальші наукові дослідження доцільно зосередити на аналізі ефективності існуючих національних правових механізмів захисту прав людини в умовах цифровізації, а також на розробці конкретних пропозицій щодо приведення українського законодавства у відповідність до міжнародних стандартів у сфері прав людини та кібербезпеки.

Ключові слова: *права людини, міжнародне право, право на приватність, міжнародний захист прав людини, кібербезпека, міжнародні договори, відповідальність, суд справедливості ЄС.*

Summary. *Introduction. The active integration of digital technologies into all spheres of life is reshaping the understanding of the space in which human rights are exercised and sets new requirements for their legal protection. In response to growing cyber threats, states increasingly implement cybersecurity measures that include monitoring, data collection, restrictions on access to information, and algorithmic content moderation. This highlights the need for scholarly analysis of the risks associated with state interference in the field of cybersecurity and the development of effective legal mechanisms for the protection of human rights in line with international standards.*

Purpose. The purpose of the study is to carry out a legal analysis of the guarantees for the protection of human rights in the context of state interference in the field of cybersecurity, in particular taking into account the potential risks to fundamental rights and freedoms, as well as determining the limits of permissible interference in accordance with international standards and the principle of the rule of law.

Materials and methods. The materials of the study are: 1) normative legal acts of the United Nations, the Council of Europe and the European Union in the field of protection of human rights and fundamental freedoms; 2) national legislative acts regulating the activities of state authorities in the field of cybersecurity; 3) the case law of the Court of Justice of the European Union; 4) provisions of Ukrainian and foreign legal doctrine.

During the study, general scientific and special legal methods were applied. The method of legal analysis made it possible to identify the main risks to human rights arising from state interference in the digital space. The comparative legal method was used to compare the approaches of international and national legal systems regarding the limits of permissible interference in the field of cybersecurity. The system-functional approach allowed for the examination of the relationship between the goals of cybersecurity and the principles of human rights. The method of generalization provided a comprehensive understanding of the issue and interpretation of the results obtained.

Results. The article analyses the legal risks of human rights violations arising from state interference in the field of cybersecurity. The main challenges related to the use of state control measures over the digital environment, including mass surveillance, data collection, algorithmic content moderation, and restrictions on access to information, are identified. The limits of permissible state interference are clarified in accordance with international human rights protection standards, particularly the case law of the European Court of Human Rights. The necessity of strengthening democratic oversight of the activities of bodies operating in the field of cybersecurity and improving regulatory frameworks based on the principles of proportionality, legal certainty, and prevention of abuse is substantiated.

Prospects. Further scientific research should focus on analysing the effectiveness of existing national legal mechanisms for the protection of human rights in the context of digitalization, as well as developing concrete proposals

for aligning Ukrainian legislation with international standards in the field of human rights and cybersecurity.

Key words: *Human rights, international law, right to privacy, international human rights protection, cybersecurity, international treaties, liability, Court of Justice of the European Union (CJEU).*

Постановка проблеми. Сучасний етап розвитку інформаційного суспільства характеризується тотальною цифровізацією усіх сфер життєдіяльності, що у свою чергу приводить до зміщення традиційного уявлення про простір, в якому реалізовуються права людини. Інтеграція цифрових технологій, зокрема Інтернету речей, штучного інтелекту та автоматизованих систем обробки даних, зумовлює формування нової соціально-правової реальності, в якій фізичний і віртуальний виміри існування особи дедалі тісніше взаємопов'язані.

Водночас у відповідь на зростання кіберзагроз та викликів у сфері національної безпеки держави розробляють та впроваджують комплекс заходів у сфері кібербезпеки, які передбачають втручання в цифрове середовище, серед яких: моніторинг, збирання даних, обмеження доступу до інформації, застосування алгоритмічного контролю тощо. Такі дії, навіть коли вони мають на меті забезпечення публічної безпеки, створюють значні ризики для реалізації основоположних прав і свобод людини, насамперед права на приватність, свободи вираження поглядів, недоторканності особистого життя, свободи зібрань та права на ефективний засіб юридичного захисту. Тому, постає необхідність у комплексному правовому аналізі ризиків, пов'язаних із державним втручанням у сферу кібербезпеки, з одночасним формуванням концептуальних підходів до забезпечення ефективних правових механізмів гарантування прав людини у вказаному контексті. Розв'язання цієї проблеми є особливо актуальним у світлі міжнародних стандартів захисту прав людини та необхідності реалізації

державами своїх міжнародно-правових зобов'язань у сфері прав людини в цифрову епоху.

Аналіз останніх досліджень і публікацій. Значний внесок у дослідженні гарантій прав людини в умовах втручання у сферу кібербезпеки зроблено як національними, так і зарубіжними дослідниками. Британські вчені Кор Д. (Korff D.), Вагнер Б. (Wagner B.), Авіла Р (Avila R.) [14] аналізують режими державного спостереження у контексті забезпечення прозорості, підзвітності та ефективного нагляду відповідно до міжнародних стандартів прав людини. Французький дослідник Вантр Д. (Ventre D.) [18] аналізує інформаційну війну як інструмент державного впливу в кіберпросторі, зосереджуючись на загрозах безпеці та обмеженнях прав людини в умовах цифрових конфліктів. Соесанто С. (Soesanto S.) [15] розглядає питання відповідальності за кібератаки, аналізуючи підходи НАТО до визначення моменту, коли кібератака може вважатися збройним нападом і потребувати відповідної реакції. Американський дослідник Гадсон Дж. (Hudson J.) [12] аналізує зміну пріоритетів ФБР, зосереджуючи увагу на зсуві акценту від правоохоронної діяльності до завдань національної безпеки, зокрема в сфері кіберзагроз. Українські науковці Предместніков О. та Батирова А. [6] досліджують кібербезпеку як важливу складову захисту прав людини в інформаційному суспільстві, розкриваючи взаємозалежність технологічних загроз і гарантій прав людини. Дослідниця Андрущенко О. [0] аналізує забезпечення прав людини в умовах тотальної інформатизації суспільства, зокрема в аспекті прозорості державної інформаційної політики. Українські автори Карвацька С., Маник А. Строїч М. [2] розглядають сучасні виклики кібербезпеки та міжнародно-правові рамки щодо захисту даних, з особливою увагою до впливу GDPR і Конвенції Ради Європи про кіберзлочинність. Кучер В.О. [4] аналізує роль інформаційної безпеки як складової захисту прав людини під час воєнної агресії, акцентуючи ризики порушень у надзвичайних режимах.

Український дослідник Хоббі Ю. [9] досліджує право людини на кібербезпеку як окрему категорію інформаційних прав, визначаючи його як невід'ємне право на захист при використанні кіберпростору.

Разом з тим, залишаються невирішеними низка проблемних питань, зокрема: відсутність ефективних міжнародних механізмів протидії втручанню з боку іноземних спецслужб, діяльності транснаціональних приватних компаній, які виконують функції цифрових підрядників на замовлення антидемократичних урядів, та поширення терористичної пропаганди через онлайн-мережі. Це створює суттєві виклики для забезпечення балансу між національною безпекою, інформаційною свободою та захистом фундаментальних прав людини у глобалізованому цифровому середовищі.

Метою статті є здійснення правового аналізу гарантій захисту прав людини в умовах державного втручання у сферу кібербезпеки, зокрема з урахуванням потенційних ризиків для основоположних прав і свобод.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правові акти Організації об'єднаних націй, Ради Європи та Європейського Союзу у сфері захисту прав людини та основоположних свобод; 2) практика Суду справедливості ЄС щодо втручання держави в права людини у цифровому середовищі; 3) положення правової доктрини, присвячені питанням кібербезпеки, цифрових прав і обмежень державної влади.

У процесі дослідження застосовувалися загальнонаукові та спеціально-юридичні методи. Метод правового аналізу дозволив виявити основні ризики для прав людини, що виникають у зв'язку з державним втручанням у цифровий простір. Порівняльно-правовий метод був використаний для зіставлення підходів правових систем щодо меж допустимого втручання у сферу кібербезпеки. Системно-функціональний підхід дозволив розглянути співвідношення цілей кібербезпеки з

принципами прав людини. Метод узагальнення забезпечив цілісне бачення проблеми та інтерпретацію отриманих результатів

Виклад основного матеріалу. У сучасних умовах цифрової трансформації дедалі більшого значення набуває забезпечення прав людини в інформаційному середовищі. Суттєву загрозу в цьому контексті становлять дії авторитарних урядів, терористичних формувань та інших суб'єктів, що використовують цифрові технології як інструмент впливу, контролю або репресивного тиску. У відповідь на зазначені виклики держави та міжнародні організації розробили низку нормативно-правових актів, які стали основою для формування національного законодавства у сфері кібербезпеки та захисту прав людини в Інтернеті.

Разом з тим, варто звернути увагу на потенційні ризики, які супроводжують реалізацію державної політики у сфері кібербезпеки. Зокрема, втручання держави в цифрову сферу, навіть якщо воно має на меті забезпечення національної безпеки, може призводити до надмірного обмеження основоположних прав і свобод. Таке втручання може становити загрозу для свободи вираження поглядів, права на приватність, свободи зібрань та інших прав, гарантованих Міжнародним пактом про громадянські і політичні права (1966 р.) [5], Конвенцією про захист прав людини і основоположних свобод (1950 р.) [3] та Хартією основних прав Європейського Союзу (2000 р.) [8].

Серед найпоширеніших втручань держав у сферу захисту прав людини у мережі Інтернет вчені виділяють: кібернапади з боку держав на інші держави, масове стеження, яке здійснюють розвідувальні органи в інтересах національної безпеки та боротьби з тероризмом, обов'язкове зберігання даних; загальний моніторинг соціальних мереж, медіа та приватних соціальних сервісів із метою блокування «незаконного» або «небажаного» контенту та підриву наскрізного шифрування, застосування новітніх технологій політичного контролю, зокрема: дистанційна

біометрична ідентифікація в публічних місцях; алгоритмічне «виявлення» потенційно небезпечних осіб і передбачення їх поведінки; розпізнавання емоцій (із похибками), біометрична класифікація та превентивна поліція; збір інформації та доказів у рамках кримінальних розслідувань у кіберпросторі з боку правоохоронних органів.

Вважаємо доцільним розпочати аналіз ризиків порушення прав людини з боку держав із дослідження цифрових війн. У сучасній юридичній літературі поняття кібервійни розкривається як цілеспрямоване використання комп'ютерних систем для дестабілізації роботи державних органів або організацій, передусім шляхом втручання в інформаційні інфраструктури задля досягнення політичних або військових цілей [10]; застосування кібертехнологій для агресивних дій у цифровому середовищі, спрямованих проти військових об'єктів, держави чи її громадян. Такий тип збройного протистояння характеризується тим, що принаймні один з його елементів: цілі, мотиви чи засоби, ґрунтується на використанні комп'ютерних або цифрових ресурсів [18, с.80]. Окрім того, дане поняття міститься у низці міжнародних нормативно-правових актах. Так, у резолюції Резолюція Генеральної Асамблеї ООН 3314 від 14.12.1974 р. кібервійна визначається як використання комп'ютерів або цифрових засобів урядом або за його явного схвалення проти іншої держави або її приватної власності, та включає наступні дії: доступ до систем іншої держави; перехоплення даних; пошкодження цифрової інфраструктури чи інфраструктури, керованої цифровими методами; виробництво та поширення пристроїв, що можуть бути використані для підриву внутрішньої активності [7; 1].

Сучасні конфлікти найчастіше пов'язані із застосуванням кіберзасобів для проведення операцій у цифровому просторі проти військових об'єктів, державних структур або населення. Проте у міжнародному праві досі немає чіткого розуміння, коли саме кібератака може вважатися «збройною агресією». Слід зазначити, що позиція НАТО щодо реагування на кібератаки

є неоднозначною. З одного боку, Альянс визнає можливість трактування окремої кібератаки як підстави для застосування статті 5 Північноатлантичного договору. Водночас, на практиці для реалізації колективного захисту за цією нормою зазвичай необхідним вважається сукупний вплив кількох атак, що разом досягають порогу, співмірного з актом збройної агресії. [15].

Окремої уваги заслуговує питання кібератак, що здійснюються недержавними акторами за підтримки або під контролем держав. Встановлення відповідальності за такі дії в цифровому середовищі є надзвичайно складним, що, у свою чергу, створює правову невизначеність щодо можливості повноцінного застосування норм міжнародного гуманітарного права в подібних ситуаціях.

Ще однією важливою проблемою є втручання держав або пов'язаних із ними недержавних суб'єктів у внутрішньополітичні процеси інших країн шляхом поширення пропаганди та дезінформації в цифровому середовищі.

Якщо раніше пропаганда традиційно розглядалася як інструмент ведення збройного конфлікту, то в сучасних умовах її дедалі частіше трактують як складову кібервійни. У відповідь на такі дії держави застосовують заходи протидії, які самі по собі нерідко мають ознаки кібервтручання в контексті міждержавного протистояння [2]. Водночас більшість таких дій здійснюється поза межами правового режиму збройного конфлікту та припадає на період формального миру, хоча й підвищеної міжнародної напруги.

Однією з ключових проблем у сфері кібербезпеки є масове стеження, що здійснюється розвідувальними службами під приводом захисту національної безпеки та протидії тероризму [4; 9]. З одного боку, такі практики можуть слугувати ефективним інструментом для виявлення потенційних загроз і запобігання терористичним актам. З іншого боку, масштабне збирання персональних даних та втручання в комунікацію

громадян можуть розглядатися як порушення права на приватність, гарантованого міжнародними стандартами у сфері прав людини.

У контексті збройних конфліктів шпигунство традиційно не розглядається як порушення норм міжнародного права. Водночас у мирний час діяльність розвідувальних органів щодо збору інформації про фізичних осіб часто виходить за межі правового регулювання. Саме через цю специфіку в міжнародному праві подібні структури зазвичай позначаються як «таємні служби». Протягом тривалого часу їхнє існування залишалося офіційно невизнаним — так, наприклад, уряд Великої Британії публічно підтвердив існування Секретної розвідувальної служби (MI6) лише у 1992 році [17].

У сучасну епоху цифрових технологій технічні можливості для стеження досягли безпрецедентного рівня. Після терористичних атак 11 вересня 2001 року багато держав істотно розширили повноваження своїх розвідувальних органів у сфері збору інформації. Зокрема, йдеться про можливість перехоплення приватної комунікації, відстеження пересування осіб, моніторинг соціальних мереж та інтернет-активності, часто, без належного демократичного контролю чи згоди осіб, яких це стосується.

Сучасні виклики безпеки зумовлюють необхідність забезпечення ефективного захисту держави без порушення фундаментальних прав і свобод громадян. Досягнення оптимального балансу між гарантуванням національної безпеки та збереженням індивідуальних свобод є ключовим завданням правового регулювання. Для цього необхідно впровадити чітке та справедливе законодавство, забезпечити незалежний контроль за діяльністю розвідувальних органів, а також гарантувати їхню прозорість і підзвітність. Відсутність таких механізмів підвищує ризик перетворення системи безпеки на засіб тиску і порушень прав людини. Наступною з ключових особливостей сучасного розвитку безпекових систем є розмивання меж між такими напрямами, як зовнішня оборона, радіоелектронна та зовнішня

розвідка, внутрішня боротьба з тероризмом, зовнішні заходи протидії терористичним загрозам, а також правоохоронна діяльність. Ця тенденція відображається не лише в теоретичних підходах, а й у структурних змінах відповідних інституцій [14; **Ошибка! Источник ссылки не найден.**].

Так, Сполучених Штатах Федеральне бюро розслідувань (*FBI*) офіційно виконує функції як правоохоронного органу, так і агенції національної безпеки та розвідки. У Сполученому Королівстві Агентство урядового зв'язку (*GCHQ*), яке займається електронною розвідкою, на підставі чинного законодавства отримало повноваження безпосередньо співпрацювати з правоохоронними органами у боротьбі з тероризмом, а також іншими злочинами, зокрема, розповсюдженням дитячої порнографії. Подібні процеси простежуються і в багатьох інших державах [12].

Варто підкреслити, що внаслідок зазначених трансформацій потенційна шкода від кібероперацій спецслужб у рамках таємної діяльності вже виходить за межі окремих груп і специфічних умов, таких як зони активних бойових дій. Натомість вона може поширюватися на цілі суспільства, включно з країнами, які формально перебувають у мирному стані, але водночас стикаються із загрозою терористичних атак. Викриття, здійснені Едвардом Сноуденом, виявили існування масштабних систем масового спостереження, організованих Сполученими Штатами Америки, Великою Британією та іншими державами, що входять до розвідувального альянсу «П'ять очей» (Австралія, Канада, Нова Зеландія). Аналогічні практики були виявлені і в діяльності спеціальних служб інших держав, зокрема Німеччини, Франції та Південної Африки, при цьому іноді такі дії здійснюються без належного інформування або санкціонування з боку урядових структур, парламентів чи наглядових органів [14]. Наведені факти свідчать про те, що навіть у державах, які формально визнають принципи верховенства права, можуть системно впроваджуватись заходи масового електронного стеження. Що ж до авторитарних режимів, таких як росія та

Китай, то можна припустити, що аналогічна діяльність здійснюється там за відсутності будь-яких ефективних правових обмежень чи незалежного контролю.

Зазначені заходи передбачають масове перехоплення як змісту електронних комунікацій, так і відповідних метаданих, часто без наявності конкретних підозр щодо окремих осіб. Крім того, включають умисне послаблення криптографічного захисту з метою забезпечення доступу до зашифрованої інформації. Такі дії зазвичай обґрунтовуються необхідністю забезпечення національної безпеки та протидії тероризму, як міжнародного, так і внутрішнього. Показовим прикладом законодавчого закріплення подібних практик є ухвалення у 2016 році у Великій Британії «Закону про слідчі повноваження», який експерти характеризують як один із найжорсткіших нормативних актів щодо спостереження у демократичних державах. Цей документ передбачає, зокрема, обов'язок інтернет-провайдерів зберігати історію переглядів усіх користувачів і надавати ці дані державним органам за запитом, а також надає можливість державним структурам здійснювати втручання у комп'ютерні системи шляхом їх несанкціонованого доступу [13].

Водночас такі заходи становлять значне втручання в реалізацію фундаментальних прав, зокрема права на повагу до приватного життя, захист персональних даних та свободу вираження поглядів. У низці прецедентних рішень, серед яких: *Digital Rights Ireland [11], Tele2 Sverige AB/Watson [16]* Суд Європейського Союзу однозначно вказав на непропорційність масового збору персональних даних без належних правових підстав, відсутність незалежного контролю та ефективних механізмів запобігання зловживанням, в тому числі збору персональних даних громадян інших держав. Законодавчі акти, що передбачають загальне зберігання великої кількості персональних даних без диференціації, обмежень або винятків, посилаючись лише на досягнення певної мети, а

також не встановлюють об'єктивних критеріїв щодо меж доступу і порядку використання таких даних, не відповідають принципу пропорційності. Відтак, вони є несумісними з положеннями Хартії основоположних прав Європейського Союзу [8].

Висновки і перспективи подальших досліджень. Проведене дослідження засвідчує, що зростаюча активність іноземних спецслужб, незаконних та терористичних організацій у кіберпросторі становить серйозну загрозу для прав і свобод людини, насамперед права на приватність, свободу вираження поглядів і безпеку персональних даних. Такі кібервтручання часто здійснюються поза межами правового поля, що створює ризики як для окремих осіб, так і для національної безпеки загалом.

В умовах гібридних конфліктів та інформаційних війн держава має не лише реагувати на подібні виклики, а й забезпечувати ефективний захист своїх громадян. Це вимагає посилення правового регулювання діяльності національних спецслужб, запровадження дієвого демократичного контролю за кібероперaціями, а також чіткого дотримання міжнародних стандартів у сфері прав людини. Особливого значення набуває прозорість, підзвітність та превентивний нагляд за використанням цифрових технологій у сфері безпеки, аби запобігти зловживанням, які можуть призвести до ерозії фундаментальних свобод.

Література

1. Андрущенко О. Забезпечення прав людини в умовах тотальної інформатизації суспільства . *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2023. 4(59). DOI: https://doi.org/10.21564/2663-5704.59.289661.

2. Карвацька С., Маник А., Строїч М. Сучасні виклики кібербезпеки та міжнародно-правові рамки щодо захисту даних. *Вісник правничих наук*.

2023. Вип. 4 (65). С. 45–59. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/325629 (дата звернення: 10.06.2025).

3. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 10.06.2025).

4. Кучер В.О. Інформаційна безпека як складова захисту прав людини під час воєнної агресії. *Вісник правничих наук*. 2022. Вип. 3 (62). С. 112–124. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/300549 (дата звернення: 10.06.2025).

5. Міжнародний пакт про громадянські і політичні права. Міжнародний документ від 16.12.1966. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення:10.06.2025).

6. Предместніков О., Батирова А. Кібербезпека як важлива складова захисту прав людини в інформаційному суспільстві. *Scientific Collection «InterConf»*. 2023 (160). С. 188–191. URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/3967 (дата звернення: 10.06.2025).

7. Резолюція Генеральної Асамблеї ООН 3314 від 14.12.1974 р. URL: https://zakononline.com.ua/documents/show/169633___169633 (дата звернення: 10.06.2025).

8. Хартія основних прав Європейського Союзу. *Європейське право*. 2013. № 1-2. С. 294-304. URL: http://nbuv.gov.ua/UJRN/evrpr_2013_1-2_25 (дата звернення: 10.06.2025).

9. Хоббі Ю.С. Право на кібербезпеку як категорія інформаційних прав людини. *Наукові записки Одеського національного університету*. 2021. Вип. 1 (85). С. 78–87. URL: https://dspace.onua.edu.ua/items/c192f469-04d2-453f-ab8d-22cfb09cbafb (дата звернення: 10.06.2025).

10. Definition of cyberwar in English. URL: https://en.oxforddictionaries.com/definition/cyberwar (дата звернення: 10.06.2025).

11. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others (Joined Cases C-293/12 and C-594/12): Judgment of the Court (Grand Chamber) of 8 April 2014 URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 (дата звернення: 10.06.2025).

12. Hudson J. FBI Drops Law Enforcement as «Primary» Mission. *The Cable.* URL: https://foreignpolicy.com/2014/01/05/fbi-drops-law-enforcement-as-primary-mission/?utm_source=chatgpt.com (дата звернення: 10.06.2025).

13. Investigatory Powers Act 2016 : Government Bill, originated in the House of Commons. 2016. URL: https://www.legislation.gov.uk/ukpga/2016/25/enacted (дата звернення: 10.06.2025).

14. Korff D., Wagner B., Powles J., Avila R., Buermeyer U. Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes. Global Report, January 2017. University of Cambridge Faculty of Law Research Paper No. 16/2017. URL: https://ssrn.com/abstract=2894490 (дата звернення: 10.06.2025).

15. Soesanto S. When Does a Cyber Attack Demand Retaliation? NATO Broadens Its View – A set of «malicious cumulative cyber activities» may now amount to an armed attack. *DefenseOne*. 30 June 2021. URL: https://www.defenseone.com/ideas/2021/06/when-does-cyber-attack-demand-retaliation-nato-broadens-its-view/175028/ (дата звернення: 10.06.2025).

16. Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others (Joined Cases C-203/15 and C-698/15): Judgment of the Court (Grand Chamber) of 21 December 2016 URL: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=CELEX%3A62015CJ0203. (дата звернення: 10.06.2025).

17. UK must retaliate against cyber-attacks says chancellor. *BBC News*. URL: https://www.bbc.com/news/technology-37821867 (дата звернення: 10.06.2025).

18. Ventre D. Information Warfare. 2016. 352 p.

References

1. Andrushchenko, O. (2023). Zabezpechennia prav liudyny v umovakh totalnoi informatyzatsii suspilstva [Ensuring human rights under conditions of total informatization of society]. *Visnyk Natsionalnoho yurydychnoho universytetu imeni Yaroslava Mudroho. Seriia: Filosofiia, filosofiia prava, politolohiia, sotsiolohiia*. № 4(59). URL: https://doi.org/10.21564/2663-5704.59.289661 [in Ukrainian].

2. Karvatska, S., Manyk, A., Stroich, M. (2023). Suchasni vyklyky kiberbezpeky ta mizhnarodno-pravovi ramky shchodo zakhystu danykh [Current challenges of cybersecurity and international legal frameworks for data protection]. *Visnyk pravnychykh nauk*. № 4(65). Pp. 45–59. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/325629 [in Ukrainian].

3. Konventsiia pro zakhyst prav liudyny i osnovopolozhnykh svobod (z protokolamy) (Ievropeiska konventsiia z prav liudyny) vid 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text [in Ukrainian].

4. Kucher, V.O. (2022). Informatsiina bezpeka yak skladova zakhystu prav liudyny pid chas voiennoi ahresii [Information security as a component of human rights protection during military aggression]. *Visnyk pravnychykh nauk*. № 3(62). Pp. 112–124. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/300549 [in Ukrainian].

5. Mizhnarodnyi pakt pro hromadianski i politychni prava. Mizhnarodnyi dokument vid 16.12.1966. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text [in Ukrainian].

6. Predmestnikov O., Batyrova A. (2023) Kiberbezpeka yak vazhlyva skladova zakhystu prav liudyny v informatsiinomu suspilstvi [Cybersecurity as an important component of human rights protection in the information society]. *Scientific Collection «InterConf».* No. 160. Pp. 188–191. URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/3967 [in Ukrainian].

7. Rezoliutsiia Heneralnoi Asamblei OON 3314 vid 14.12.1974 r. URL: https://zakononline.com.ua/documents/show/169633___169633 [in Ukrainian].

8. Khartiia osnovnykh prav Yevropeiskoho Soiuzu. Yevropeiske pravo. 2013. № 1-2. S. 294-304. URL: http://nbuv.gov.ua/UJRN/evrpr_2013_1-2_25 [in Ukrainian].

9. Khobbi, Yu.S. (2021). Pravo na kiberbezpeku yak katehoriia informatsiinykh prav liudyny [The right to cybersecurity as a category of informational human rights]. *Naukovi zapysky Odeskoho natsionalnoho universytetu*. № 1(85). Pp. 78–87. URL: https://dspace.onua.edu.ua/items/c192f469-04d2-453f-ab8d-22cfb09cbafb [in Ukrainian].

10. Definition of cyberwar in English. URL: https://en.oxforddictionaries.com/definition/cyberwar

11. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others (Joined Cases C-293/12 and C-594/12) : Judgment of the Court (Grand Chamber) (2014). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

12. Hudson J. FBI Drops Law Enforcement as 'Primary' Mission. *The Cable.* URL: https://foreignpolicy.com/2014/01/05/fbi-drops-law-enforcement-as-primary-mission/?utm_source=chatgpt.com

13. Investigatory Powers Act 2016: Government Bill, originated in the House of Commons. URL: https://www.legislation.gov.uk/ukpga/2016/25/enacted

14. Korff D., Wagner B., Powles J., Avila R., Buermeyer U. (2017). Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes. Global Report, January 2017. University of Cambridge Faculty of Law Research Paper No. 16/2017. URL: https://ssrn.com/abstract=2894490

15. Soesanto S. (2021). When Does a Cyber Attack Demand Retaliation? NATO Broadens Its View – A set of "malicious cumulative cyber activities" may now amount to an armed attack. *DefenseOne*, URL: https://www.defenseone.com/ideas/2021/06/when-does-cyber-attack-demand-retaliation-nato-broadens-its-view/175028/

16. Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others (Joined Cases C-203/15 and C-698/15): Judgment of the Court (Grand Chamber) (2016). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0203

17. UK must retaliate against cyber-attacks says chancellor. *BBC News*. URL: https://www.bbc.com/news/technology-37821867

18. Ventre D. (2016). Information Warfare. 2016. 352 p.