УДК 32.019.51:004.056]:316.346.2
DOI https://doi.org/10.32782/2663-6170/2024.37.27

ГЕНДЕРНО-ЧУТЛИВА ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ЦИФРОВОГО ВРЯДУВАННЯ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКІ РЕАЛІЇ

GENDER-SENSITIVE INFORMATION SECURITY IN THE CONTEXT OF DIGITAL GOVERNANCE: INTERNATIONAL EXPERIENCE AND UKRAINIAN REALITIES

Краснопольська Т. М.,
кандидат політичних наук, доцент,
доцент кафедри політичних теорій
Національного університету «Одеська юридична академія»

У статті досліджується взаємозв'язок між цифровою трансформацією органів публічної влади, інформаційною безпекою та гендерною рівністю. Акцентується увагу на тому, що зростання онлайн-загроз у цифровому просторі, таких як кібербулінг, доксинг, діпфейки та дезінформація, непропорційно спрямоване на жінок у публічному секторі – політикинь, держслужбовиць, громадських діячок. Зокрема, розглянуто приклади кібернападів і гендерно вмотивованої дезінформації в Україні та інших країнах.

У центрі аналізу кейси публічних жінок, які зазнали цифрових атак. Показано, як онлайн-насильство використовується як інструмент гібридної війни, спрямований на витіснення жінок із політики та публічного простору. Особливу увагу приділено зарубіжним практикам: створенню кіберінфраструктури в Естонії (Tallinn Manual, e-Governance), використанню технологічних інструментів підтримки в Канаді (ParityBOT), впровадженню цифрових ID, верифікацій та міждержавного співробітництва.

Обґрунтовано необхідність запровадження в Україні цілісної системи гендерно-чутливої інформаційної безпеки, що включає: інституційні рішення (політико-правові основи, протоколи реагування, спеціальні підрозділи в органах влади), освітні заходи (тренінги для жінок у публічному секторі), технічні рішення (AI-моніторинг, бот-сервіси, верифікація акаунтів), міжнародне співробітництво (обмін досвідом, реагування на атаки, участь у програмах цифрової демократії).

Підкреслено, що гендерна дезінформація та цифрова агресія є системною проблемою, що підриває демократичні інститути, відлякує жінок від політичної участі та сприяє відтворенню патріархальних стереотипів. Інформаційна безпека не може бути ефективною без урахування гендерних аспектів, особливо в умовах гібридної війни. На основі міжнародного досвіду та українського контексту запропоновано рекомендації для інтеграції гендерно-чутливих підходів у цифрове врядування.

Ключові слова: інформаційна безпека, інформаційні технології, гендер, гендерна рівність, демократія, права жінок, мізогінія, онлайн-насильство, е-врядування, кібербулінг, діпфейк, політична комунікація.

This article explores the interrelation between the digital transformation of public authorities, information security, and gender equality. It emphasizes that the rise of online threats in the digital environment–such as cyberbullying, doxing, deepfakes, and disinformation–disproportionately targets women in the public sector, including politicians, civil servants, and civic activists. The analysis focuses on documented cases of cyberattacks and gender-motivated disinformation in Ukraine and other countries.

At the core of the study are case analyses of public women subjected to digital assaults. The research demonstrates how online violence functions as a tool of hybrid warfare aimed at marginalizing women from political and public life. Particular attention is devoted to international practices: Estonia's development of cyber infrastructure (e.g., the Tallinn Manual, e-governance systems), Canada's deployment of technological support tools such as ParityBOT, and the implementation of digital IDs, verification mechanisms, and intergovernmental cooperation.

The article substantiates the urgent need for Ukraine to adopt a comprehensive gender-sensitive information security framework. This should include institutional measures (legal and political frameworks, response protocols, and dedicated units within government institutions), educational initiatives (capacity-building and training for women in public service), technical solutions (AI-powered monitoring systems, support bots, and verified official accounts), and enhanced international cooperation (experience-sharing, coordinated responses to attacks, and participation in digital democracy programmes).

The study highlights that gendered disinformation and digital aggression represent a systemic threat that undermines democratic institutions, deters women from political engagement, and perpetuates patriarchal stereotypes. Effective information security strategies must necessarily integrate gender perspectives–particularly in the context of hybrid warfare. Drawing on international experience and the Ukrainian context, the article offers recommendations for embedding gender-sensitive approaches into digital governance practices.

Key words: information security, information technologies, gender, gender equality, democracy, women's rights, misogyny, online violence, e-governance, cyberbullying, deepfake, political communication.

Постановка проблеми. Цифровізація політичних комунікацій та публічного управління супроводжується не лише перевагами прозорості й доступності, а й зростанням інформаційних загроз, що особливо небезпечні в умовах гібридної війни. Однією з найуразливіших груп у цифровому просторі є жінки, які займають активні позиції в органах публічної влади та громадянському суспільстві. Кібербулінг, діпфейк-атаки, дезінформація й цифрове переслідування все частіше використовуються як інструменти тиску, дискредитації та витіснення жінок із публічного простору. Проте системні підходи до інформаційної безпеки в е-врядуванні часто ігнорують гендерну специфіку загроз, що створює прогалини в захисті прав і репутації посадовиць.

Аналіз останніх досліджень і публікацій. До дослідження проблем інформаційної безпеки в цифровому врядуванні зверталися як зарубіжні, так і вітчизняні вчені. Зокрема, у працях Дж. Зіттрейн та Л. Лессіг розкриваються ризики цифрового контролю та вплив інформаційної архітектури на свободу комунікації. Х. Ніссенбаум та Ф. Брей акцентують увагу на етичних та безпекових аспектах цифрової публічності.

У вітчизняному науковому дискурсі питання інформаційної безпеки в електронному врядуванні розглядають П.Д. Біленчук, С.Л. Гнатюк, О.О. Золотар, В.А. Ліпкан, Н.Б. Новицька, О.Г. Ярема та інші.

З питань гендерної специфіки цифрової взаємодії варто виділити праці І.Г. Бухтіярової, О.А. Бухтіярова, Т.М. Мельник, О.Г. Стрельченко, М.В. Співак, О.І. Суслової, які вказують на асиметрію цифрового досвіду жінок та чоловіків у публічній сфері.

Водночас в українському контексті питання цифрової безпеки жінок у політичному просторі та публічному секторі залишаються фрагментарно дослідженими. Наявні наукові розвідки зосереджуються переважно на загальних аспектах кіберзагроз або на темі гендерного насильства в офлайн-середовищі. Недостатньо уваги приділяється саме аналізу гендерних ризиків цифрової комунікації посадовців, зокрема у розрізі кіберзагроз, дезінформації, дискредитаційних атак, а також відсутності комплексних механізмів реагування з урахуванням гендерної чутливості.

Виділення невирішених раніше частин загальної проблеми. Серед малодосліджених аспектів проблеми слід виділити: гендерно зумовлені особливості інформаційного тиску на посадових осіб у цифровому середовищі; відсутність системного аналізу вразливостей, пов'язаних із представництвом жінок у цифрових платформах е-врядування; недостатній рівень інституційного реагування на кіберзагрози, спрямовані проти жінок-посадовиць; відсутність ефективних механізмів запобігання онлайн-насильству та інформаційній дискримінації в жінок-посадовиць в цифровій комунікації.

Формування цілей статті (постановка завдання). Метою статті є аналіз викликів інформаційної безпеки в контексті цифрової трансформації органів публічної влади з урахуванням гендерної специфіки, вивчення зарубіжного досвіду інтеграції кіберзахисту й гендерної рівності, а також розробка рекомендацій щодо впровадження комплексних механізмів протидії онлайн-насильству та дискредитаційним кампаніям, спрямованим на жінок у публічному секторі України.

Виклад основного матеріалу дослідження. Цифрова трансформація органів публічної влади супроводжується значними викликами в площині інформаційної безпеки, що перетинаються з гендерними вимірами.

Зарубіжний досвід демонструє ефективні практики забезпечення кіберзахисту та захисту прав посадовців. Наприклад, Естонія запроваджує інноваційний кіберзахист як основу інклюзивної держави. Країна характеризується потужним комплексним підходом до кібербезпеки й е-врядування: держава впровадила цифрові ID, i-Voting, електронне резидентство та e-Governance Academy.

Після масованих кібератак у 2007 році Естонія закріпила глобальні норми кіберпростору: створено Центру передового досвіду НАТО з кіберзахисту в Таллінні та випущено «Tallinn Manual» (Талліннський посібник з міжнародного права, що застосовується до кібервійни). В посібнику викладено міжнародні закони, які вважаються застосовними до кіберсфери. Він містить загалом дев'яносто п'ять «правил чорної літери», що стосуються кіберконфліктів. Tallinn Manual працював над забезпеченням глобальної норми в кіберпросторі шляхом застосування чинного міжнародного права до кібервійни. У посібнику стверджується, що держави не мають суверенітету над Інтернетом, але вони мають суверенітет над компонентами Інтернету на своїй території [8; 12].

Естонія разом з партнерами через запровадження «Tallinn Mechanism» у 2023 році Україні [1; 3] надає нам технічну і дипломатичну підтримку: допомагає евакуювати дані держсервісів і координує кібервідповідь.

Корисним є досвід Канади, що розробила та запровадила автоматизовану підтримку політикинь ParityBOT, розвиток якого демонструє проактивний підхід до онлайн-захисту жінок-політикинь [7]. Цей Twitter-бот виявляє образливі твіти на адресу жінок у політиці й автоматично публікує повідомлення на їхню підтримку. Його завдання – формування позитивного онлайн-середовища та захист публічного голосу політикинь в політичних комунікаціях онлайн. Автори зазначають,

що «онлайн-зловживання, такі як ненависницькі твіти, спрямовані на жінок, які займаються політикою, сприяють цій [гендерній] нерівності, особливо твіти, що зосереджені на їхній статі» [6].

ParityBOT являє собою не лише технологічне рішення, а й приклад інтеграції стратегій інформаційної безпеки із захистом гендерної рівності в публічній комунікації.

На нашу думку, поєднання досвіду цих двох країн дасть змогу сформувати необхідні передумови для забезпечення інформаційної безпеки в умовах гендерно чутливого е-врядування та дозволить сформувати гендерно чутливі політичні комунікації.

Вітчизняна практика також має певні досягнення в цій сфері, зокрема розроблений та презентований у 2022 році Міністерством внутрішніх справ України, Національною поліцією України у співпраці з Фондом ООН у галузі народонаселення (UNFPA) мобільний застосунок для боротьби із гендерним насильством (для виклику поліції у випадках домашнього насильства) [2], що демонструє партнерство держави та міжнародних організацій у сфері інформаційної безпеки на гендерно чутливій основі.

Проте на даний час проблема гендерно обумовленого насильства в публічному онлайн просторі залишається актуальною. Серед головних мішеней таких атак політикині, громадські активістки, журналістки та інші.

Отже, забезпечення інформаційної безпеки в е-врядуванні та політичному процесі не може обходитись без врахування гендерної специфіки, особливо в контексті онлайн-агресії, дезінформації та кібербулінгу, спрямованих проти жінок.

Із початком повномасштабної війни проти України зросла хвиля цифрової агресії, спрямованої проти жінок, які займають активні позиції в публічному просторі – журналісток, держслужбовиць. Онлайн-атаки стають системною зброєю, яку використовують як інструмент деморалізації, залякування та інформаційної ізоляції.

Серед основних типів загроз та їх проявів можна назвати такі, як: дискредитація (знецінення професійної позиції, спотворення фактів), кібербулінг (серії зневажливих, загрозливих повідомлень), доксинг (публікація персональних даних – адреса, сім'я, місце роботи), гендерний тролінг (сексуалізовані образи, мізогінія, «вивід з публічності»), маніпулятивні фото/відео (діпфейки або підроблені матеріали) тощо.

Найбільш резонансним прикладом є діпфейк атака на народну депутатку 2014-2019 років Світлану Заліщук. У 2017 році проти неї було здійснено інформаційну атаку із використанням AI-згенерованих еротичних зображень (діпфейк), з метою дискредитації. Фейкова публікація твіту стверджувала, що політикиня начебто пообіцяла «бігати голою вулицями Києва» у випадку поразки України. Поряд із постом були опубліковані фальшиві зображення повністю оголеної депутатки. Цей допис викликав широкий резонанс – так, німецький журналіст навіть запитав її про це на форумі ООН з питань жінок.

Як зазначає колишня виконавча директорка цільової групи з боротьби з дезінформацією Міністерства внутрішньої безпеки США, Ніна Янкович: «мене справді непокоїло, що журналіст з європейської країни поставився до цього так серйозно, що згадав про Організацію Об'єднаних Націй» [9]. Аналітик стверджує, що такі діпфейк-атаки використовуються «як сексуалізована зброя» і вже негативно вплинули на кар'єру Світлани Заліщук.

В результаті інцидент завдав сильного удару по репутації тодішньої народної депутатки: запитання на міжнародному рівні (в ООН) надало загального розголосу та вплинув на її політичну кар'єру (у 2019 році вона не пройшла до парламенту).

Цей приклад – один із найперших задокументованих випадків застосування діпфецк-технологій як інструменту гібридної інформаційної війни проти жінок-посадовиць, що служить яскравим підтвердженням необхідності включення гендерно-специфічних підходів в систему інформаційної безпеки.

Ще один приклад – напади на голову громадської організації «Точка росту освіти і науки», координаторку Dissergate Світлану Вовк. Так, у 2020-2021 роках після публічних викриттів плагіату чиновників активістка зазнала серії кібернападів: понад 10 спроб злому електронної пошти, систематичні доксинг (фіксація особистих даних, фото з її адреси), письмові й електронні погрози зґвалтування та вбивства з доказами стеження (включно з фото сім'ї) [14]. Було відкрито кримінальне провадження пізніше перекваліфіковане на загрозу або насильство стосовно державного діяча, проте справа просувалась дуже повільно.

Жінки-посадовиці (як особливо вразлива група, оскільки вони поєднують функції представниць влади з публічною видимістю) зазнають як психологічних, так і фізичних загроз у цифровому середовищі, кібернапади (доксинг, хакерські атаки) використовуються як інструмент тиску та залякування.

До особливостей гендерно мотивованих нападів слід віднести те, що онлайн-атаки супроводжуються офлайн-погрозами, з порушенням права на безпечність; цифрові та фізичні атаки мають один корінь: стереотипи та мізогінія, що підсилюються як у фізичному просторі, так і в інтернеті; цифрові методи дискредитації (хакерство, доксинг, цифрове переслідування) використовуються як частина політичного тиску; в той же час відсутність своєчасної реакції правоохоронних органів погли-

блює проблему безкарності. Гендерна природа атак (сексуалізована агресія, мізогінія, інформаційна дискредитація) підкреслює потребу у спрямованих заходах захисту.

Аналітики зазначають, що гендерна дезінформація та використання жінок як мішеней фейкових новин є доволі поширеною практикою у регіоні Східного партнерства. Зокрема Г. Маммадова вважає, що російське керівництво давно використовує транснаціональну дезінформацію як стратегічний інструмент для підриву суспільної згуртованості в країнах регіону, орієнтуючись на різні політичні групи, прагне посіяти страх у суспільстві та підірвати довіру до урядів, що протистоять РФ. Особливе місце в цих кампаніях займають гендерні наративи, які, якщо їм не протидіяти, можуть загрожувати стабільності цих країн [11].

Дослідниця відзначає, що гендерна дезінформація особливо ефективна через домінування патріархальної політичної культури, особливо у сільських регіонах, а використання гендеру як зброї гальмує демократичний розвиток та послаблює демократичні інституції.

Дезінформація також спекулює на стигматизованих та чутливих питаннях, щоб дискредитувати суспільство під час конфліктів. Як зазначає Г. Маммадова, «з початком війни в Україні кількість гендерної дезінформації проти українських жінок у російському сегменті соцмереж значно зросла, наприклад, у випадку звинувачення жінки, яка народила після вибуху у пологовому будинку Маріуполя, у тому, що вона нібито акторка, найнята Україною» [11].

Тактики гендерної дезінформації включають дискредитаційні кампанії, фальшиві медіаоперації, армії ботів, що погрожують і переслідують жінок онлайн, а також поширення фейкових історій, фото, відео та аудіо.

Хоча гендерна дезінформація часто непомітна, складна для ідентифікації та недостатньо обговорена, вона посилює політичну поляризацію і загрожує демократичному розвитку, одночасно посилюючи патріархальні стереотипи. Слід погодитись з висновком У. Маммадової у тому, що необхідний новий підхід для протидії гендерній дезінформації, що враховуватиме перетини вразливостей і зменшить поширення неправдивої інформації про жінок [11].

Проте і в інших регіонах світу простежується чимало прикладів, що відображають особливості вразливості жінок-посадовиць до інформаційних атак, кібербулінгу та дискредитаційних кампаній. Наприклад, у Новій Зеландії у 2019 році відбувались атаки на стиль лідерства і зовнішність прем'єр-міністерки Джасінди Ардерн. Незважаючи на високу популярність, вона неодноразово ставала жертвою сексистських нападів в інтернеті. Її стиль лідерства (поєднання емпатії та рішучості) піддавали критиці як «занадто жіночому» або «занадто м'якому». Також у соцмережах поширювали негативні коментарі щодо її зовнішнього вигляду. Сексизм у політичній сфері часто проявляється через критику жіночого образу, що відволікає увагу від їхніх професійних досягнень [10].

Аналізуючи досвід Нової Зеландії, Є. Корлетт відзначає: «жінки-депутатки борються з постійно зростаючою хвилею мізогінних образ – від зґвалтування та погроз смертю до зневажливих коментарів щодо зовнішності та сумнівів у їхній кваліфікації – значна частина яких поширюється в Інтернеті людьми, що ховаються за анонімними акаунтами в соціальних мережах» [5]. Новозеландські жінки-політики активно борються зі зростанням мізогінії.

У Великій Британії також наявні подібні приклади. Зокрема, погрози та образи спонукають жінок-депутаток залишити парламент Великобританії. За даними The New York Times, вісімнадцять жінок-членів парламенту не бажали переобратися на парламентських виборах 2019 року через шквал онлайн та офлайн образ [13].

Проведене С. Колліньон на основі даних опитування дослідження зловживань та переслідувань під час виборів 2019 року у Великобританії показало, що жінки стають мішенню в соціальних мережах та через електронну пошту. 54% жінок-кандидаток та 39% чоловіків отримували неналежні повідомлення у Twitter, Facebook або інших соціальних мережах. Крім того, 42% жінок та 32% чоловіків отримували електронні листи з образами. Дані показали, що темпи зростання обсягу електронних листів такого характеру швидші для жінок (збільшення на 16% порівняно з 12% зростанням серед чоловіків). Поширення дезінформації непропорційно спрямоване на жінок, оскільки 32% жінок та 23% чоловіків повідомили про поширення оманливої інформації про них особисто під час виборчої кампанії 2019 року [4]. Ці цифри прямо підтверджують: онлайн-атаки на жінок-кандидаток, спрямовані на залякування та витіснення їх з політики, були системними та інтенсивними.

Отже, вітчизняна та зарубіжна практика демонструє різні прояви вразливості жінок-посадовиць: від сексистської критики зовнішності і стилю, до організованих дискредитаційних кампаній та психологічного тиску через кібербулінг.

Жінки в публічному секторі стають мішенню гібридної війни, яка виходить за межі фронту і проникає в персональні акаунти, репутацію та безпеку. Саме тому інформаційна безпека в е-врядуванні повинна враховувати гендерну специфіку як обов'язковий елемент.

Для подолання гендерно спрямованих ризиків цифрової комунікації посадовців та учасників публічного просторі необхідно запровадження

комплексних дій. До основних векторів слід віднести:

− інституційні заходи (запровадження обов'язкових протоколів реагування на онлайн-насильство в органах публічної влади, аналогічно до протоколів протидії дискримінації; розширення політико-правового регулювання, зокрема кваліфікації кібербулінгу; створення окремого контактного пункту у Міністерстві цифрової трансформації України або іншому органі центральної влади, що займатиметься виявленням та модерацією випадків кібербулінгу щодо посадовиць в центрі та регіонах),

− тренінги для жінок-посадовиць (медіатренінги з цифрової безпеки, включно з управлінням власним цифровим слідом, розпізнаванням інформаційних атак; психологічна підтримка – створення гарячих ліній та анонімного консультування);

− технічні рішення (впровадження верифікованих акаунтів посадовців, які легше відрізнити від фейкових; автоматизовані алгоритми моніторингу hate speech на сторінках публічних службовців – на основі AI інструментів, наприклад HateLab або GenderScope; запровадження ботів / сервісів підтримки жінок на національному рівні по прикладу канадського ParityBOT);

− розвиток міжнародного співробітництва для обміну досвідом та впровадження найбільш ефективних практик боротьби з загрозами (наприклад, участь у програмах OSCE, UN Women, що підтримують жінок у цифровій демократії, удосконалення е-контейнерів та резервування даних спільно з міжнародними партнерами) та оперативного реагування у випадку нападів (партнерство з платформами Facebook, Telegram, X/Twitter для швидкого реагування на запити щодо онлайн-насильства) та інші.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Проведений аналіз засвідчив, що цифрова трансформація державних інституцій супроводжується значними інформаційними загрозами, що мають яскраво виражений гендерний вимір, особливо у вигляді онлайн-агресії, дезінформації, кібербулінгу та сексуалізованих нападів на жінок у публічній сфері. Приклади Естонії, яка впроваджує комплексні механізми кіберзахисту і міжнародні норми, та Канади, що використовує технологічні інструменти для підтримки жінок-політикинь, демонструють ефективність інтегрованого підходу до інформаційної безпеки з гендерною чутливістю. Вітчизняна практика має перші успіхи, однак потребує посилення та систематизації заходів із урахуванням гендерних ризиків. Для забезпечення надійного, інклюзивного і демократичного цифрового врядування слід впроваджувати комплексні інституційні, технічні та освітні рішення, а також розвивати міжнародне співробітництво і швидке реагування на кіберзагрози, спрямовані проти жінок у публічному просторі. Перспективним є подальше вивчення інструментів протидії гендерно мотивованим цифровим атакам і розробка механізмів їхньої превенції та реагування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. 10 країн запустили Талліннський механізм для кібердопомоги Україні. *Європейська правда*. URL: https://www.eurointegration.com.ua/news/2023/12/20/7175933/

2. МВС та UNFPA за підтримки першої леді запустили мобільний додаток для виклику поліції у випадках домашнього насильства. 03.08.2022. *Офіційне інтернет-представництво Президента України*. URL: https://president.gov.ua/news/mvs-ta-unfpa-za-pidtrimki-pershoyi-ledi-zapustili-mobilnij-d-76861?fbclid=IwAR3m-iblCw-2krul-OMwBYkdOUHfj9nBuEkZvTfY5uvkgD0rN-RCfWHcdcM

3. Талліннський механізм: Україна та міжнародні партнери започаткували новий інструмент співпраці у кіберпросторі. *Кабінет Міністрів України*. URL: https://www.kmu.gov.ua/news/tallinnskyi-mekhanizm-ukraina-ta-mizhnarodni-partnery-zapochatkuvaly-novyi-instrument-spivpratsi-u-kiberprostori

4. Collignon S. Representative Audit of Britain. The Constitution Unit Blog. November 6, 2020. URL: https://constitution-unit.com/tag/representative-audit-of-britain/

5. Corlett E. Here be trolls_ New Zealand's female politicians battle rising tide of misogyny. New Zealand. 8 Apr 2022. *The Guardian*. https://www.theguardian.com/world/2022/apr/09/here-be-trolls-new-zealands-female-politicians-battle-rising-tide-of-misogyny

6. Cuthbertson L., Kearney A., Dawson R. etc. Women, politics and Twitter: Using machine learning to change the discourse. 2019. *AI for Social Good workshop at NeurIPS. Vancouver, Canada*. URL: https://aiforsocialgood.github.io/neurips2019/accepted/track1/pdfs/36_aisg_neurips2019.pdf

7. Forani J. "ParityBOT" offsets negative tweets with positive message. October 08, 2019. *CTV News – Breaking News and Video, Canada News Today*. URL: https://www.ctvnews.ca/lifestyle/article/paritybot-offsets-negative-tweets-with-positive-message/

8. Herzog S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*. 2011. Volume 4, No. 2. P. 49-60. URL: http://dx.doi.org/10.5038/1944-0472.4.2.3

9. How Putin is poised to weaponise AI-created deep fake PORN with cyber army in bid to tear down democracies in the West. *The Sun*. URL: https://www.thesun.co.uk/news/26256097/how-putin-is-poised-to-weaponise-ai-created-deep-fake-porn-with-his-cyber-army-in-bid-tear-down-democracies-in-the-west/

10. Jacinda Ardern: 'Very little of what I have done has been deliberate. It's intuitive'. 6 Apr 2019. *The Guardian*. URL: https://www.theguardian.com/world/2019/apr/06/jacinda-ardern-intuitive-courage-new-zealand

11. Mammadova G. Gendered disinformation_ Women as a target of fake news in Eastern Partnership region. 13.12.2022. *Top-center.org*. URL: https://top-center.org/en/expert-opinion/3456/gendered-disinformation-women-as-a-target-of-fake-news-in-eastern-partnership-region

12. Shackelford, Scott J. Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks. *Journal of Internet Law, Forthcoming*. November 4, 2009. URL: https://ssrn.com/abstract=1499849

13. Specia M. Threats and Abuse Prompt Female Lawmakers to Leave U.K. Parliament. Nov. 1, 2019. *The New York Times*. URL: https://www.nytimes.com/2019/11/01/world/europe/women-parliament-abuse.html

14. Ukraine: Svitlana Vovk threatened, harassed and smeared (joint communication). 31 January 2022. *UN SR Human Rights Defenders*. URL: https://srdefenders.org/ukraine-vovk-threatened-harassed-and-smeared-joint-communication/