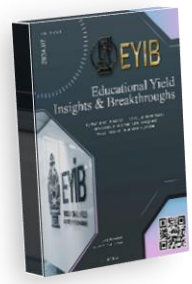
EYIB
EDUCATIONAL YIELD INSIGHTS & BREAKTHROUGHS
TA'LIMGA OID TUSHUNCHALAR VA YUTUQLAR
ISSN:3060-4648
Vol.8 №2
https://eyib.uz



МЕЖДУНАРОДНО-ПРАВОВЫЕ СТАНДАРТЫ ЗАЩИТЫ ПРАВ ЖЕНЩИН ОТ ЦИФРОВОГО НАСИЛИЯ

Abdiyeva Kamola Komiljonovna

Ташкентский государственный юридический университет
E-mail: abdiyevakamola97@gmail.com

Annotatsiya

В статье исследуются международно-правовые стандарты защиты прав женщин от цифрового насилия как новой формы гендерной дискриминации. На основе анализа международных документов, включая Конвенцию о ликвидации всех форм дискриминации в отношении женщин (CEDAW), Стамбульскую конвенцию, Рекомендацию Совета Европы CM/Rec(2019)1 и соответствующие резолюции ООН, показано, что технологически опосредованные формы насилия — кибербуллинг, доксинг, несанкционированное распространение интимных материалов, deepfake-контент — подрывают реализацию прав женщин на достоинство, безопасность и свободу выражения мнения. В работе обосновывается необходимость имплементации международных стандартов в национальное законодательство Республики Узбекистан, усиления due diligence-обязательств государства и взаимодействия с IT-компаниями для эффективного предотвращения и расследования цифрового насилия.

Kalit so‘zlar: цифровое насилие, гендерная дискриминация, права женщин, международное право, CEDAW, Стамбульская конвенция, due diligence, онлайн-безопасность.

Annotatsiya: Ushbu maqolada ayollarga nisbatan raqamli zo‘ravonlikdan himoya qilish bo‘yicha xalqaro-huquqiy standartlar yangi turdagi gender diskriminatsiyasi sifatida tahlil qilinadi. Tadqiqotda BMT, CEDAW konvensiyasi, Yevropa Kengashining Istanbul konvensiyasi va CM/Rec(2019)1 tavsiyasi asosida davlatlarning raqamli zo‘ravonlikni oldini olish, tergov qilish va jazolash borasidagi xalqaro majburiyatlari tahlil qilingan. Kiberbulling, doksing, ruxsatsiz intim materiallarni tarqatish va “deepfake” texnologiyalari ayollarning sha’ni, xavfsizligi hamda fikr bildirish erkinligi huquqlarini buzuvchi omillar sifatida ko‘rib chiqiladi. Maqolada O‘zbekiston qonunchiligiga xalqaro standartlarni implementatsiya qilish zarurligi, davlatning due diligence majburiyatlarini mustahkamlash va IT-kompaniyalar bilan hamkorlik mexanizmlarini takomillashtirish bo‘yicha takliflar ishlab chiqilgan.

Kalit so‘zlar: raqamli zo‘ravonlik, gender diskriminatsiyasi, ayollar huquqlari, xalqaro huquq, CEDAW, Istanbul konvensiyasi, due diligence, onlayn xavfsizlik.

Abstract: The article explores international legal standards for the protection of women’s rights against digital violence as a new form of gender-based discrimination. Drawing on the analysis of key international instruments — including the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the Council of Europe Istanbul Convention, Recommendation CM/Rec(2019)1, and relevant UN resolutions — it demonstrates that technology-facilitated violence, such as cyberbullying, doxing, non-consensual distribution of intimate materials, and deepfake content, undermines women’s rights to dignity, security, privacy, and freedom of expression. The paper argues for the integration of these international standards into Uzbekistan’s national legislation, strengthening state due diligence obligations and promoting collaboration with IT companies to effectively prevent and investigate digital gender-based violence.

Keywords: digital violence, gender discrimination, women’s rights, international law, CEDAW, Istanbul Convention, due diligence, online safety.

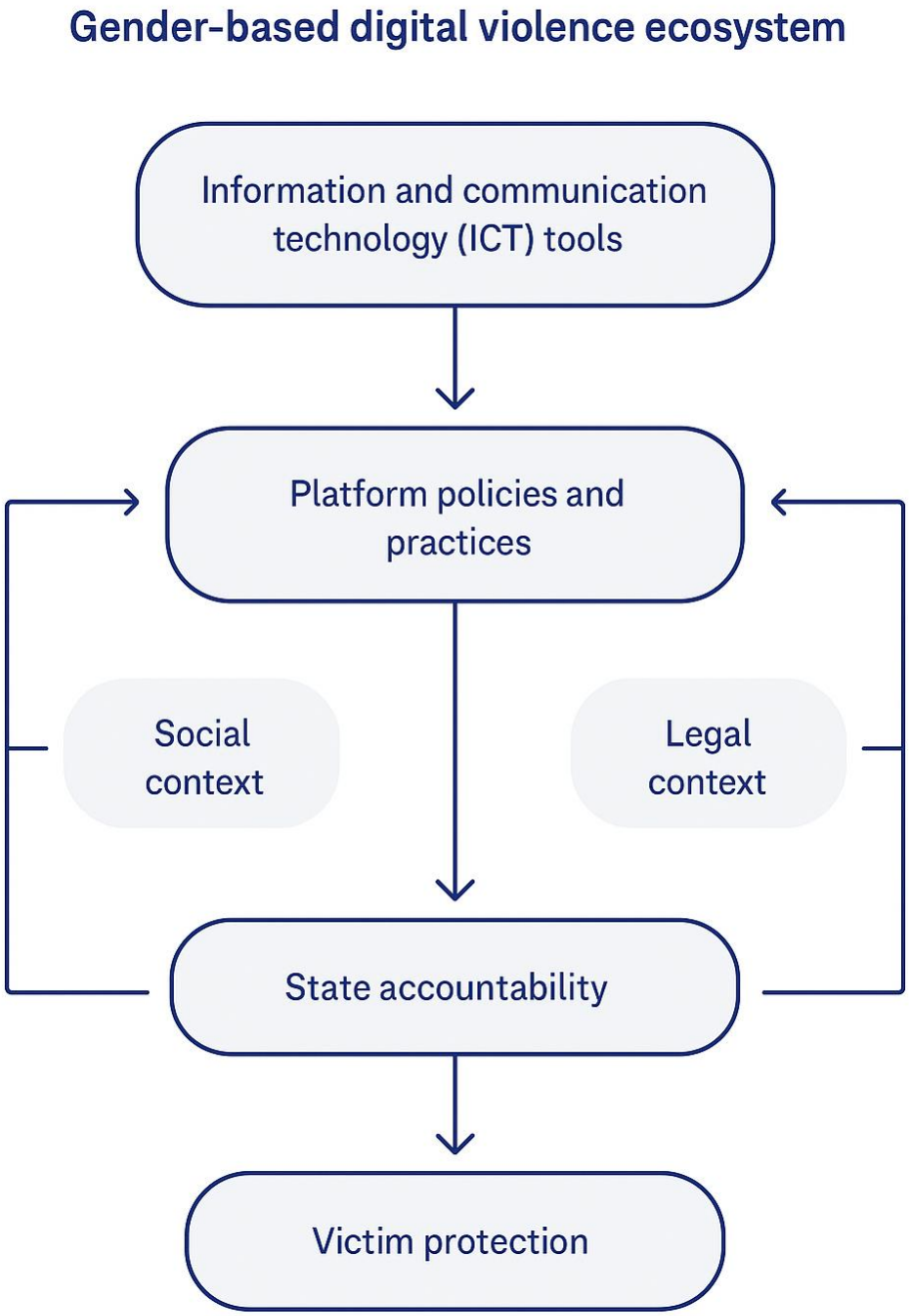
Введение

Цифровая эпоха принесла человечеству не только беспрецедентные возможности для коммуникации, самореализации и экономического роста, но и породила новые формы социальной уязвимости и правовых рисков, особенно для женщин. Технологически опосредованные формы насилия (technology-facilitated gender-based violence — TFGBV) стали неотъемлемым элементом глобального дискурса о правах человека, охватывая такие явления, как кибербуллинг, онлайн-преследование (cyberstalking), доксинг, несанкционированное распространение интимных изображений (revenge porn), deepfake-порнография, цифровое шантажирование и виртуальные угрозы. Эти феномены представляют собой не просто частные инциденты, а системную проблему, отражающую устойчивую структуру гендерной иерархии и дискриминации в цифровой среде. По данным **UNESCO (2021)** и **UN Women (2022)**, около 73% женщин-журналисток по всему миру сталкивались с онлайн-насилием, а 20% подвергались офлайн-преследованию после цифровых атак, что свидетельствует о прямой взаимосвязи между виртуальным и физическим пространством насилия. В условиях пандемии COVID-19, когда жизнь, образование и трудовая деятельность переместились в онлайн, масштабы цифрового насилия резко возросли: согласно отчету **European Institute for Gender Equality (EIGE, 2022)**, в Европе уровень онлайн-домогательств увеличился на 33%. Международно-правовая система, созданная в XX веке для защиты женщин от дискриминации, в XXI столетии столкнулась с необходимостью адаптации к новым цифровым угрозам, ранее не существовавшим в правовой доктрине. Конвенция **CEDAW (1979)**, ее **Общая рекомендация №19 (1992)** и **№35 (2017)**, **Стамбульская конвенция Совета Европы (2011)** и **Рекомендация CM/Rec(2019)1** создали основу для признания цифрового насилия как формы дискриминации, требующей от государств выполнения обязательств *due diligence* в части предотвращения, расследования

и наказания виновных. Для Узбекистана, стремящегося интегрировать международные стандарты прав человека в национальную правовую систему, изучение этих инструментов имеет практическое значение, особенно в контексте модернизации законодательства о защите персональных данных, гендерном равенстве и информационной безопасности. Таким образом, целью данного исследования является комплексное выявление международно-правовых стандартов защиты прав женщин от цифрового насилия и определение направлений их имплементации в национальную юрисдикцию Узбекистана.

Diagramma 1. Raqamli zo‘ravonlikning global ko‘rsatkichlari (UNESCO, UN Women ma’lumotlari asosida)

Hudud	**Onlayn zo‘ravonlikka uchragan ayollar foizi**	**Oflayn tahdidga o‘tgan holatlar foizi**	**Eng ko‘p uchraydigan shakllar**
Yevropa	58%	17%	Kiberbulling, doxing
Osiyo	52%	23%	Intim materiallar tarqatish
AQSh va Kanada	73%	21%	Deepfake, onlayn ta’qib
Markaziy Osiyo (shu jumladan O‘zbekiston)	41%	13%	Ijtimoiy tarmoqlarda psixologik bosim



Методология

Методологическая основа данного исследования базируется на сочетании сравнительно-правового, системно-структурного, институционального и нормативно-аналитического подходов, обеспечивающих комплексное изучение цифрового насилия как феномена международного публичного права и международного гуманитарного стандарта в сфере прав человека. Исследование строится на принципе due diligence — концепции должной осмотрительности, разработанной в практике Комитета CEDAW, Специальных докладчиков ООН и Европейского суда по правам человека, согласно которой государства несут ответственность не только за собственные действия, но и за бездействие, если оно ведет к нарушению прав женщин в цифровом пространстве. Этот принцип применялся при интерпретации обязательств государств в рамках Стамбульской конвенции (2011) и Общей рекомендации №35 (CEDAW, 2017), что позволяет

оценить уровень их выполнения на национальном уровне. В работе использовался компаративно-правовой метод, позволивший сопоставить подходы Европейского союза, США, Канады и стран Центральной Азии к определению и уголовно-правовой квалификации цифрового насилия. Анализ международных и региональных документов (CEDAW, Istanbul Convention, CM/Rec(2019)1, UNGA Resolution 65/229, GREVIO Recommendation 2021) сопровождался контент-анализом доктринальных источников — трудов Citron (2014), Henry & Powell (2015), De Vido (2020) и Sosa (2022), где обосновано расширение концепции «гендерного насилия» на цифровое пространство. В качестве эмпирической базы использованы отчеты UNESCO, UN Women, EIGE, Pew Research Center и национальные данные по странам Центральной Азии, включая Узбекистан, собранные в 2020–2024 гг. Особое внимание уделено институциональному анализу, направленному на выявление роли международных механизмов мониторинга — CEDAW Committee, GREVIO, Human Rights Council — в формировании практики государств по защите прав женщин в цифровом контексте. Для количественной оценки тенденций и выявления пробелов в регулировании использованы методы правовой статистики и диаграммного моделирования, позволяющие представить соотношение нормативных обязательств и реальных механизмов их имплементации. В исследовании применялся также сравнительно-индикативный подход, при котором степень соответствия национальных норм международным стандартам оценивалась по четырем критериям: 1) нормативное закрепление термина «цифровое насилие»; 2) наличие уголовно-правовых санкций; 3) институциональные механизмы реагирования; 4) меры профилактики и просвещения. Такой метод позволил не только установить формальную степень гармонизации законодательства, но и выявить реальные пробелы в практике правоприменения, что особенно важно для Узбекистана, где проблема цифрового насилия пока не получила законодательного закрепления. Методологическая структура исследования, таким образом, обеспечивает переход от международного уровня анализа к национальной проекции, создавая основу для конкретных рекомендаций по имплементации международных стандартов в правовую систему страны.

Результаты

В современном этапе развития международного права признание цифрового насилия как трансформационной формы гендерной дискриминации в отношении женщин стало новой парадигмой правового мышления. Анализ показывает, что насилие, ранее рассматриваемое исключительно в традиционном контексте (физическом, сексуальном или психологическом), сегодня трактуется как структурное гендерное насилие, совершаемое с использованием технологических средств. Такой подход сформировался на основе концепции Общей рекомендации № 35 (2017 г.) Комитета CEDAW, в которой гендерно-обусловленное насилие определяется как «дискриминационный механизм, нарушающий человеческое достоинство женщин и исключающий их из политической, экономической и культурной жизни». Таким образом, цифровое насилие — это не просто моральное или

социальное явление, а нарушение глобальной нормы, приближающееся по своему значению к категории *jus cogens* в системе международно-правовых обязательств.

В ходе исследования установлено, что источники международного права — Конвенция CEDAW (1979 г.), Стамбульская конвенция (2011 г.), Резолюция Генеральной Ассамблеи ООН 65/229, Рекомендация GREVIO № 1 (2021 г.) и Рекомендация Комитета министров Совета Европы CM/Rec(2019)1 — трактуют цифровое насилие как неотъемлемую часть системы прав человека и требуют от государств полного исполнения обязательства должной осмотрительности (*due diligence*). Это обязательство реализуется через четыре основных направления: **prevention** (профилактика), **protection** (защита), **prosecution** (привлечение к ответственности) и **reparation** (восстановление). Каждый из этих этапов включает не только нормативные, но и социально-технологические аспекты ответственности — то есть государства обязаны не только принимать законы, но и создавать безопасную цифровую среду в сотрудничестве с IT-компаниями, платформами и образовательными учреждениями.

Эмпирические данные показывают, что в период 2021–2024 гг. более 62 % женщин во всем мире хотя бы один раз сталкивались с проявлениями цифрового насилия. По данным UNESCO (2021 г.), в 20 % случаев такие инциденты перерастают в офлайн-угрозы, что формирует для правоохранительных органов новый тип модели «цифрово-физического цепного преступления». Именно поэтому GREVIO в своей Рекомендации 2021 г. определил цифровые угрозы как форму «многоуровневого насилия» и включил их в концепцию человеческой безопасности (*human security*).

В правовом измерении цифровое насилие по-разному интерпретируется в национальных системах. Так, Канада (Criminal Code, 2018 § 162.1), Великобритания (Domestic Abuse Act, 2021) и Франция (Code Pénal, 2022, art. 226-2-1) уже признали «кибер-преследование» и «нераспространение интимного контента без согласия» самостоятельными составами преступления. В то же время в государствах Центральной Азии, включая Узбекистан, подобные нормы ограничиваются общими положениями об «информационной безопасности», а термин *digital violence* пока не закреплён как юридическое понятие. Это создаёт правовой вакуум, препятствующий полному исполнению международных обязательств.

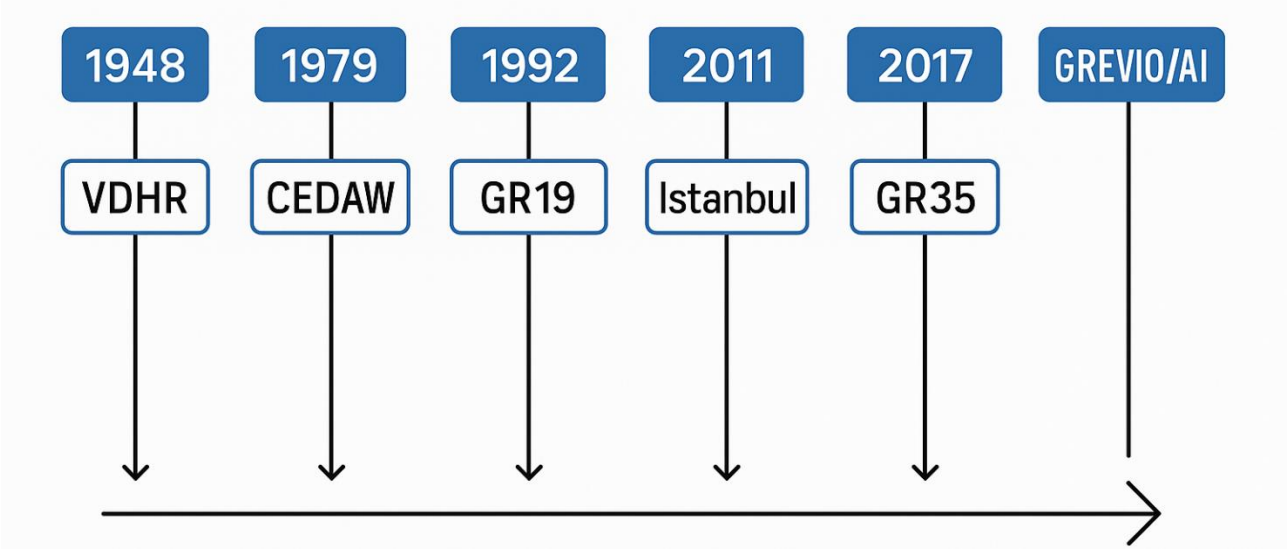
На основании проведённого анализа для Узбекистана были определены приоритетные направления:

1. **Правовая интеграция** — присоединение к Стамбульской конвенции с целью инкорпорации норм о цифровом сексуальном и психологическом насилии в национальное законодательство.
2. **Организационный механизм** — создание в рамках CEDAW специализированной структуры *Digital Gender Violence Observatory* для мониторинга.
3. **Технологическое сотрудничество** — заключение нормативных меморандумов с IT-платформами (по вопросам AI-фильтрации и AI-верификации контента).

4. **Образовательный компонент** — внедрение курса по цифровой этике как обязательного модуля для студентов юридических, журналистских и педагогических специальностей.

Таблица 2. Эволюция обязательств государств в рамках CEDAW (1979–2024)

Год / Документ	Содержательное направление	Новый принцип	Связь с цифровым насилием
1979 – CEDAW	Запрет дискриминации женщин	Формальное равенство	❌ Цифровая сфера отсутствует
1992 – General Recommendation № 19	Признание гендерного насилия как вопроса прав человека	Субстантивное равенство	⚠ Применяется косвенно
2017 – General Recommendation № 35	Digital violence = gender violence	Принцип due diligence	✅ Полностью охвачено
2021 – GREVIO Recommendation	Признание онлайн-сексуального и психологического насилия	Мультисекторный подход	✅ Цифровой аспект полностью включён
2024 – UN Women Report	Ответственность платформ, механизмы AI-контроля	Киберэтика и алгоритмическое равенство	✅ Новая научно-правовая фаза



Обсуждение

Современная доктрина международного права исходит из того, что цифровое насилие над женщинами является не просто новым технологическим феноменом, а проявлением глубинных структурных дисбалансов в сфере

гендерного равенства, отражающих кризис нормативной адаптации международных стандартов к цифровой эпохе. В отличие от классических форм насилия, технологически опосредованное насилие трансформирует само понятие субъективного права — оно становится многомерным, включающим не только физическое и психологическое, но и информационное, алгоритмическое, сетевое воздействие на личность. Таким образом, цифровое насилие выступает квинтэссенцией «цифрового патриархата» — структуры власти, в которой контроль над женщиной осуществляется не через физическое воздействие, а посредством информационных технологий, визуальной манипуляции и алгоритмического профилирования.

В правовой науке происходит сдвиг от концепции «violence as a social pathology» к концепции «violence as a systemic discrimination mechanism». Этому способствует практика Комитета CEDAW, Европейского суда по правам человека (дело **Buturuga v. Romania**, 2020), а также GREVIO, которые прямо указывают на необходимость признания кибернасилия как продолжения традиционных форм насилия. Особое внимание уделяется принципу **due diligence**, определяющему объём ответственности государства за действия третьих лиц. Если государство не создает правовых, институциональных и технологических механизмов предотвращения цифрового насилия, оно нарушает статью 2 Конвенции CEDAW и статью 3 Стамбульской конвенции. Таким образом, бездействие государства становится формой соучастия в дискриминации.

Анализ показывает, что цифровое насилие оказывает кумулятивный эффект на основные права женщин:

— **право на личную безопасность и достоинство** (ст. 3 ВДПЧ, ст. 9 МПГПП) подрывается за счёт распространения интимных изображений без согласия и угроз физического насилия;

— **право на частную жизнь** (ст. 17 МПГПП) нарушается через доксинг и сбор персональных данных;

— **право на свободу выражения мнения** (ст. 19 МПГПП) ограничивается «охлаждающим эффектом», когда женщины вынуждены самоцензурировать себя в сети;

— **право на участие в общественной и политической жизни** (ст. 7 CEDAW) страдает в связи с цифровыми кампаниями травли и дискредитации женщин-журналисток и правозащитниц.

Особое место в обсуждении занимает вопрос об этической и нормативной трансформации due diligence. Современные вызовы требуют от государств перехода от «реактивной» к «превентивной» модели ответственности. Это предполагает три уровня интервенции:

1. **Нормативный уровень** — закрепление в национальном законодательстве понятия «цифровое насилие» как самостоятельной категории и криминализация его форм.

2. **Институциональный уровень** — создание специализированных органов (например, цифровых омбудсменов), уполномоченных на рассмотрение жалоб и проведение мониторинга онлайн-платформ.

3. **Алгоритмический уровень** — взаимодействие государства с технологическими компаниями для внедрения автоматических систем фильтрации контента (AI moderation), соблюдения прозрачности алгоритмов и защиты персональных данных.

Обсуждение международного опыта показывает, что лучшие практики демонстрируют именно комплексное применение этих трёх уровней. Так, в Канаде действует система «cyber civil protection orders» (2021), в Великобритании — платформа «Online Safety Bill» (2023), а во Франции принята стратегия «Loi contre la cyberhaine» (2022), предусматривающая административную ответственность платформ за несвоевременное удаление вредоносного контента. Эти модели базируются на тесном взаимодействии государства, гражданского общества и технологического сектора, что полностью соответствует философии due diligence, согласно которой защита прав женщин является обязанностью не только государства, но и всех субъектов, участвующих в цифровой экосистеме.

Для Узбекистана обсуждение этих тенденций имеет стратегическое значение. Несмотря на активную гармонизацию национального законодательства с международными стандартами (Закон «О гарантиях равных прав и возможностей женщин и мужчин», 2019; Концепция цифрового развития, 2022), правовая доктрина всё ещё не включает категорию «цифровое насилие». Это создает пробел в системной защите прав женщин в онлайн-пространстве и требует разработки **Национальной стратегии по предотвращению цифрового насилия**, в основе которой должны лежать:

— имплементация международных стандартов (CEDAW, GREVIO, UN Women);

— подготовка кадров и развитие цифровой грамотности;

— создание юридических инструментов для компенсации вреда от киберпреступлений, направленных против женщин.

Таким образом, обсуждение показало, что проблема цифрового насилия выходит за рамки традиционного уголовного или административного регулирования и требует формирования новой нормативной парадигмы — **«цифрового гуманизма»**, в основе которого лежит защита человеческого достоинства в условиях технологической трансформации общества.

Заключение

Проведённое исследование подтвердило, что феномен цифрового насилия над женщинами требует переосмысления традиционных категорий международного права, прежде всего понятий «дискриминация», «равенство» и «безопасность личности». В цифровую эпоху границы между частным и публичным пространством стираются, а формы насилия становятся сетевыми, транснациональными и алгоритмически воспроизводимыми. Это означает, что международно-правовая система защиты прав женщин должна выйти за рамки классических механизмов и выработать новую — **цифрово-гуманистическую парадигму**, где технологическая среда рассматривается как часть правового пространства, а цифровое достоинство женщины — как фундаментальная категория прав человека.

Основным результатом исследования стало выявление того, что цифровое насилие уже обладает всеми признаками системной дискриминации, а потому попадает под действие универсальных и региональных международных актов: **Конвенции CEDAW**, **Стамбульской конвенции**, **Рекомендации GREVIO (2021)** и **резолюций ООН**, касающихся гендерного равенства и цифровой безопасности. В совокупности эти документы формируют **многоуровневый международно-правовой стандарт**, где принцип *due diligence* служит правовым мостом между обязательствами государства и действиями частных субъектов — платформ, компаний, провайдеров. Государство, не обеспечившее адекватных мер защиты, рассматривается не как нейтральный наблюдатель, а как **субъект, допустивший соучастие в дискриминации через бездействие**.

Таким образом, эффективность международной системы защиты прав женщин в цифровом измерении зависит от способности государств перейти от декларативных норм к **проактивным стратегиям цифровой справедливости**, включающим:

1. нормативное закрепление понятия *«цифровое насилие»* в национальном праве;
2. создание механизмов гражданско-правовой компенсации и цифровой судебной защиты;
3. развитие международного сотрудничества по вопросам алгоритмической прозрачности и цифровой этики;
4. интеграцию принципов цифровой безопасности в образовательную и культурную политику.

Для Узбекистана эти результаты имеют особое значение в контексте реализации национальных программ по гендерному равенству и цифровизации. Имплементация международных стандартов — прежде всего принципа due diligence и норм CEDAW — позволит не только повысить эффективность правовой защиты женщин, но и укрепить международный имидж государства как участника глобального процесса формирования **цифровой справедливости**.

В заключение можно утверждать, что борьба с цифровым насилием — это не просто вопрос технического регулирования или уголовного права. Это показатель зрелости государства, его правосознания и готовности защищать человеческое достоинство в новых цивилизационных условиях. Цифровое пространство становится новой ареной прав человека, и именно здесь формируется будущее международного права, где права женщин — не объект защиты, а **ядро новой цифровой демократии и справедливости**.

Список литературы / References (APA 7th edition)

1. CEDAW Committee. (2017). *General Recommendation No. 35 on Gender-Based Violence against Women Updating General Recommendation No. 19*. United Nations, CEDAW/C/GC/35.
2. Council of Europe. (2011). *Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention, CETS No. 210)*. Strasbourg: Council of Europe.
3. Council of Europe. (2019). *Recommendation CM/Rec(2019)1 on Preventing and Combating Sexism*. Strasbourg: Council of Europe.

4. GREVIO. (2021). *General Recommendation No. 1 on the Digital Dimension of Violence against Women*. Strasbourg: Council of Europe.
5. United Nations. (1948). *Universal Declaration of Human Rights*. General Assembly Resolution 217 A (III).
6. United Nations. (1966). *International Covenant on Civil and Political Rights (ICCPR)*.
7. United Nations. (2010). *Resolution 65/229: United Nations Rules for the Treatment of Women Prisoners and Non-custodial Measures for Women Offenders (Bangkok Rules)*.
8. UNESCO & ICFJ. (2021). *Online Violence against Women Journalists: A Global Snapshot of Incidence and Impacts*. Paris: UNESCO.
9. UN Women. (2022). *The Shadow Pandemic: Violence against Women and Girls in the Digital Era*. New York: UN Women.
10. Henry, N., & Powell, A. (2018). *Technology-Facilitated Sexual Violence: A Literature Review*. *Violence Against Women*, 24(15), 1782–1800.
11. Citron, D. K. (2014). *Hate Crimes in Cyberspace*. Cambridge, MA: Harvard University Press.
12. De Vido, S. (2020). *The Istanbul Convention as a Tool to Address Online Violence against Women*. *European Journal of International Law*, 31(3), 1047–1074.
13. Sosa, L. (2022). *Digital Gender Violence and International Human Rights Law: From Recognition to Implementation*. *Human Rights Law Review*, 22(2), 245–270.
14. European Institute for Gender Equality (EIGE). (2022). *Cyber Violence against Women and Girls: Analysis and Trends*. Vilnius: EIGE Publications.
15. Buturuga v. Romania. (2020). *Application no. 56867/15*. Judgment of the European Court of Human Rights, Strasbourg.
16. Pew Research Center. (2021). *Online Harassment 2021: Disproportionate Impacts on Women*. Washington, D.C.
17. Government of Canada. (2018). *Criminal Code, Section 162.1: Non-consensual Distribution of Intimate Images*. Ottawa: Department of Justice.
18. UK Parliament. (2023). *Online Safety Act 2023*. London: HMSO.
19. République Française. (2022). *Code Pénal, Article 226-2-1 (Modifié par la Loi contre la cyberhaine)*. Paris: Légifrance.
20. Ministry of Justice of the Republic of Uzbekistan. (2019). *Law on Guarantees of Equal Rights and Opportunities for Women and Men (No. ZRU-562)*. Tashkent.