Примечание: этот перевод доступен благодаря добровольному взносу Центр глобального ИТ-сотрудничества. IGF ему благодарен. Этот перевод не представляет никакой позиции организации

ФОРУМ ПО ВОПРОСАМ УПРАВЛЕНИЯ ИНТЕРНЕТОМ 2022

Аддис-Абебские Послания ФУИ

Настоящий документ[1] представляет собой резюме вопросов, которые были подняты в ходе 17-й ежегодной встречи Форума по вопросам управления Интернетом, проходившей в Аддис-Абебе с 28 ноября по 2 декабря 2022 года.

Взгляды и мнения, представленные в документе, не обязательно совпадают с мнением Секретариата Организации Объединенных Наций. Использованные условные обозначения и термины могут не соответствовать практике Организации Объединенных Наций и не означают выражения какого бы то ни было мнения со стороны Организации.

В рамках обсуждений, проходивших на ФУИ 2022, основное внимание было уделено пяти ключевым темам, которые охватывает Глобальный цифровой договор (ГЦД). Предложение о его разработке было выдвинуто в докладе Генерального секретаря Организации Объединенных Наций «Наша общая повестка дня», опубликованном в 2021 году и приуроченном к 75-летнему юбилею Организации Объединенных Наций, и будет рассматриваться Генеральной Ассамблеей ООН в 2023 году. Это станет одной из составляющих подготовки к Саммиту будущего, который планируется провести в 2024 году.

В ходе ФУИ были рассмотрены следующие темы:

- **подключение всех людей к Интернету и защита прав человека;**
- **недопущение фрагментации Интернета;**
- **управление данными и защита приватности;**
- **обеспечение безопасности, защиты и ответственности;**
- **передовые технологии, включая искусственный интеллект (ИИ).**

Как платформа с участием многих заинтересованных сторон, ФУИ выразил поддержку предложения Генерального секретаря о создании Глобального цифрового договора. Послания, изложенные в настоящем документе, представляют собой вклад со стороны ФУИ в разработку Глобального цифрового договора. Динамичные коалиции ФУИ, которые уже занимаются решением определенных проблем и рассмотрением возможностей, актуальных с учетом предложенных тематических направлений ГЦД, также заявили о своем намерении участвовать как в подготовке, так и в осуществлении процессов ООН, связанных с ГЦД.

[1] Послание, сформулированное в ходе 17-й ежегодной встречи ФУИ. Оно выносилось на публичное обсуждение, в результате которого была собрана обратная связь, впоследствии учтенная в окончательной редакции документа.

Подключение всех людей к Интернету и защита прав человека

Тема

Первым принципом Глобального цифрового договора (ГЦД), создание которого было предложено Генеральным секретарем ООН, является «Подключение всех людей и всех школ к Интернету». Данный принцип основан на том, что подключение и доступ к Интернету стали необходимыми условиями обеспечения средств к существованию, безопасности и образования людей по всему миру, а также на том, что наличие Интернета в школах предусматривает создание ключевых точек доступа, делает информационные ресурсы доступными для всех обучающихся и способствует развитию цифровой грамотности с самого раннего возраста. И все же 2,7 миллиарда человек до сих пор не подключены к Интернету, причем в наиболее неблагоприятном положении находятся жители наименее развитых стран и сельской местности.

Полноценный доступ не ограничивается одним лишь подключением к Интернету и неразрывно связан с защитой прав человека в онлайн-среде. Обеспечение доступа, способствующее росту благополучия обществ, должно опираться на соблюдение прав человека. В числе прочего это предполагает обеспечение возможности свободного выражения мнения пользователями, отсутствие препятствий к политическому и демократическому участию, обеспечение возможности пользования Интернетом всеми людьми без страха подвергнуться преследованию или дискриминации, а также обеспечение реализации прав детей и применения соответствующих мер безопасности, равносильных мерам, существующим в офлайн-пространстве. Интернет является активатором реализации прав и в то же время должен легко инкорпорировать ранее установленные права человека в свою работу, поскольку с течением времени наша цифровая зависимость в части осуществления рутинных функций повышается, а границы между онлайн- и офлайн-средой становятся менее значимыми.

Послания

Цифровое неравенство

- **Цифровой неравенство различных стран и регионов остается мощным фактором, влияющим на национальное и международное развитие**, в том числе на процесс достижения Целей устойчивого развития (ЦУР). Особую обеспокоенность вызывает положение наименее развитых стран и малых островных развивающихся государств (МОРАГ). Цифровое неравенство связано не только с неравномерным подключением к Интернету. Наряду с подключением к Интернету полноценный доступ включает в себя факторы доступности, приемлемости в ценовом отношении, наличия контента, услуг, развитие цифровой грамотности и других навыков. Приемлемость в ценовом отношении представляет собой особую проблему для многих людей, главным образом на Глобальном Юге.

- **Пандемия COVID-19 выявила роль Интернета в обеспечении личной и экономической устойчивости и в то же время продемонстрировала, насколько неблагоприятным является положение тех, кто не подключен к Интернету или не имеет полноценного доступа к нему**, а также потенциально усугубила прочие формы неравенства. Для того, чтобы установить степень влияния и последствия введения мер, связанных с COVID-19 и касающихся прав человека, доступа к Интернету и его использования, понадобится время.

- **Во всех сообществах существуют группы, которые сталкиваются с более значительными проявлениями цифрового неравенства, чем остальные, или не имеют полноценного доступа к Интернету.** В рамках многих сообществ число женщин, подключенных к Интернету и использующих его, уступает числу мужчин. Особенно неблагоприятным в рассматриваемом контексте является положение уязвимых и маргинализированных сообществ: многие люди испытывают разного рода лишения, обусловленные сочетанием факторов, связанных с возрастом, полом, этнической принадлежностью, языком, социальным положением и так далее. Целевые инициативы в сфере инфраструктуры, устройств и сервисов могут поспособствовать повышению скорости доступа для групп населения, в меньшей степени подключенных к Интернету, но должны сопровождаться мерами, направленными на устранение иных препятствий к обеспечению полноценного доступа, и быть сопряженными с другими мерами по преодолению неравенства и дискриминации.

- **Устойчивость и безопасность цифровой инфраструктуры является ключевым фактором цифровой интеграции. Правительства должны обеспечивать защиту и продвижение требуемой инфраструктуры, в том числе электросетей, автономных энергосистем и сетей связи.** На некоторых территориях Африки и других континентов ввиду значительных расстояний между группами населения, проживающими в сельских и отдаленных районах, в том числе в МОРАГ, обеспечение соединений «последней мили» оказывается коммерчески непривлекательным для частного сектора. Подключение к Интернету, поддержка его скорости и надежности являются важными аспектами создания инфраструктуры. Повышение пропускной способности инфраструктуры и решение проблемы региональных диспропорций, особенно в сельской местности, потребует времени и инвестиций.

- **Для обеспечения и предоставления доступа важно сотрудничество между группами заинтересованных сторон. Правительства и различные заинтересованные стороны, действующие в рамках партнерских отношений, должны поддерживать учреждение и работу эффективных регуляторных органов и нормативно-правовых баз, решать существующие проблемы на коммерчески непривлекательных территориях и поощрять использование инновационных подходов к подключению к Интернету**, в том числе связанных с общественными сетями, надлежащим распределением радиочастотного спектра, доступом, обеспечиваемым низкоорбитальными спутниками, и наличием местного контента, включая контент на местных языках.

Гендерное цифровое неравенство и права женщин

- **Мужчины со значительно большей вероятностью находятся онлайн или имеют доступ к мобильному Интернету, чем женщины**. Гендерный цифровой разрыв особенно велик в наименее развитых странах. Задача 9с ЦУР, направленная на обеспечение всеобщего и приемлемого в ценовом отношении доступа к Интернету, не может быть решена, пока не преодолен данный разрыв.

- **Угроза насилия и преследования сдерживает присутствие женщин в онлайн-пространстве**. Гендерно обусловленное насилие в Интернете является важным фактором, поддерживающим и усиливающим гендерное неравенство в части доступа к Интернету и пользования Интернетом, и приводит к тому, что некоторые женщины покидают онлайн-пространство. Роль технологических сервисов и платформ в распространении гендерно обусловленного насилия должна быть признана и принята во внимание. Необходимо поддерживать женщин,

предоставляя руководство к сопротивлению гендерно обусловленному насилию в Интернете и возмещению причиненного ущерба, в том числе с помощью горячих линий, функционирующих на базе сообществ. Ресурсы, правила сообществ и сервисы для сбора жалоб, имеющиеся на платформах, должны быть доступны на местных языках.

- **Понятия «гендерное равенство», «интеграция», «защита женщин и обеспечение их прав» должны быть включены в Глобальный цифровой договор** (ГЦД), в соответствии с предложением структуры «ООН-Женщины».

Права человека и цифровое развитие

- **Всеобщий доступ должен быть обеспечен с учетом прав человека, так чтобы Интернет стал доступным и безопасным для всех**. К данным правам относятся право на свободу выражения мнения, право на свободу объединения с другими, право на неприкосновенность частной жизни и другие гражданские, политические, экономические, социальные и культурные права, изложенные в международных стандартах в области прав человека. Структуры, занимающиеся вопросами управления Интернетом и разработкой цифровых технологий, должны соблюдать данные права. Организации, разрабатывающие стандарты, должны рассмотреть возможность приглашения экспертов в области прав человека в Интернете из всех заинтересованных сообществ к участию в своей работе.

- **Прозрачность, ответственность и должная осмотрительность в части обеспечения прав человека входят в зону ответственности всех заинтересованных групп, включая межправительственные и международные организации, правительства, частный сектор, техническое сообщество и гражданское общество**. Это потребует соответствия практик ведения бизнеса цифровым правам, а также сотрудничества заинтересованных сторон, направленного на решение проблем, связанных с дезинформацией, дискриминацией и разжиганием ненависти, особенно в периоды политической нестабильности, выборов и передачи власти.

- **Доступ в Интернет играет ключевую роль в обеспечении доступа к информации и возможности выражения мнений.** Правительствам следует избегать отключения Интернета, поскольку оно имеет негативные последствия для реализации прав человека и достижения экономического благополучия. Социальные медиа и технологические компании должны поддерживать усилия граждан по защите своих прав и интересов, связанные с отключением Интернета.

- **Важно улучшать мониторинг соблюдения цифровых прав и процесс их осуществления.** Был сделан ряд предложений по созданию международных механизмов в рамках системы ООН с привлечением многих заинтересованных сторон. Данные механизмы могли бы дополнить и развить существующие механизмы, включая как те из них, которые связаны с цифровым развитием и правами, так и те, которые действуют в иных сферах, например в сфере изменения климата.

- **Интернет обеспечивает возможности для расширения прав на образование** в рамках более общей стратегии улучшения образования. Качество образования на Глобальном Юге, особенно во время пандемии, пострадало вследствие отсутствия подключения к Интернету. Несмотря на то что ИКТ могут обеспечить обучающимся полноценный доступ, различия в глобальных и

местных темпах внедрения технологий обострили неравенства, существовавшие до пандемии. Опыт, полученный во время пандемии, может быть использован для повышения эффективности использования цифровых ресурсов в будущем.

- **Необходимо предпринимать усилия по содействию малому и местному бизнесу в получении максимальной выгоды от пользования Интернетом**. Уровень применения цифровых инструментов малыми и средними предприятиями существенно вырос с 2020 года, однако микропредприятия по-прежнему сталкиваются со значительными трудностями при попытках провести цифровую трансформацию бизнес-процессов.

- **Изменения на рынке труда, связанные с функционированием онлайн-платформ, предоставляют возможности для создания рабочих мест и повышения их качества и одновременно служат причиной возникновения соответствующих трудностей**, особенно для женщин, которые составляют бóльшую долю рабочей силы в неформальной экономике, чем мужчины, в большинстве стран. Во многих случаях недостаточная профессиональная подготовка остается барьером, препятствующим тому, чтобы человек в полной мере использовал свой трудовой потенциал.

- **Необходимо развивать цифровые компетенции и адаптировать методики преподавания, обучения и подготовки к новым парадигмам** образования и трудоустройства. Важно выявить и преодолеть разрыв между потребностями промышленности, с одной стороны, и среднего профессионального и высшего образования – с другой.

Недопущение фрагментации Интернета

Тема

Поддержка глобального, открытого и интероперабельного (функционально совместимого) Интернета является ключевой ценностью ФУИ. Это означает, что общие технические стандарты и протоколы продолжают внедряться в целях создания сети взаимосвязанных сетей, преодолевающих границы стран и регионов, а также то, что стандарты качества контента и сервисов находятся в соответствии с правами человека и принципом верховенства закона. Призыв к применению нормативно-правовой базы, приоритизирующей права и свободы пользователей наряду с инфраструктурной, сквозной согласованностью и через нее, нашел отражение в планах по разработке ГЦД.

Риск фрагментации является реальным и только растет. Необходимо решить проблему технической и коммерческой фрагментации, вызванной тем, что функционирование Интернета оказывается под воздействием произвольных и непроизвольных условий и практик ведения бизнеса. Фрагментация, обусловленная государственной политикой, влияющей на открытость и интероперабельность Интернета, также вызывает обеспокоенность.

Послания

Понимание существующих проблем

- **Глобальный цифровой договор предоставляет возможность для утверждения ценности Интернета как открытой инфраструктуры, состоящей из взаимосвязанных сетей, в целях соблюдения положений Устава ООН, достижения Целей устойчивого развития и реализации прав человека**. В рамках Интернет-сообщества существует общепринятое мнение о ценности глобального нефрагментированного Интернета как платформы для различных форм человеческой деятельности.

- **Вопросы, поднятые в ходе обсуждения фрагментации Интернета, отличаются своей многоаспектностью, причем разные заинтересованные стороны разными способами осмысляют и интерпретируют используемый термин**. Некоторые заинтересованные стороны особенно обеспокоены техническими и инфраструктурными аспектами Интернета, в то время как внимание других сосредоточено на вопросах государственной политики, в том числе касающихся доступа к Интернету, прав и форм влияния на пользовательский опыт. Данные вопросы рассматриваются в проекте документа, подготовленном Сетевой рабочей группой по вопросам фрагментации Интернета ФУИ. Уважение и понимание опыта различных людей и их представлений о фрагментации Интернета абсолютно необходимо, если мы стремимся к принятию эффективных и скоординированных мер.

- **Широкий спектр политических, экономических и технических факторов может способствовать фрагментации**. Однако не следует принимать за фрагментацию разнообразие и децентрализацию – глубоко положительные аспекты архитектуры и функционирования Интернета.

Устранение риска фрагментации

- **Эффективные механизмы управления, применяемые с участием многих заинтересованных сторон, играют ключевую роль в управлении глобальным нефрагментированным Интернетом**. Необходимо укреплять доверие к данным механизмам, обеспечивать их надежность и устойчивость, а также содействовать тому, чтобы действия структур управления, развивающихся и реагирующих на новые вызовы, были согласованными.

- **Необходимо проявлять бдительность по отношению к новым или формирующимся рискам фрагментации**. Глобальная кооперация и координация усилий будут крайне важны для обнаружения тревожных признаков на ранних этапах, оценки влияния политик и других разработок, а также подготовки к преодолению последствий подобных изменений. Подход с участием всех заинтересованных сторон наиболее эффективен в части оценки, измерения и отслеживания потенциальных непреднамеренных последствий мер, влияющих на функционирование Интернета, а также в части предложения действенных альтернатив, исключающих или снижающих риски фрагментации. Сетевая рабочая группа по вопросам фрагментации Интернета ФУИ является положительным примером использования описанного подхода.

- **Открытость Интернета играет важную роль в эффективной реализации прав интернет-пользователей, поощряя конкуренцию и равенство возможностей, а также сохраняя генеративный одноранговый характер Интернета**. В данном контексте споры о сетевом нейтралитете и недискриминационном управлении трафиком являются лишь частью более широкой дискуссии. Сетевой нейтралитет необходим, но недостаточен для обеспечения открытости Интернета. Интероперабельность инфраструктур и данных, нейтралитет платформ и устройств также необходимы.

- **Несмотря на то что в разных регионах мира будут использоваться разные правовые, регуляторные и программные подходы, активная координация действий, осуществляемая поверх международных границ, крайне важна для обеспечения того, чтобы фрагментированные подходы не угрожали глобальному охвату и функциональной совместимости Интернета**. Сохранение целостности глобальной сети требует международного регуляторного сотрудничества и консенсуса в отношении основных принципов.

- **На особенности использования Интернета в различных юрисдикциях влияет множество различных факторов, включая отличия социальных, демографических, экономических, культурных и политических условий, а также вопросы технического и инфраструктурного характера**. Стремление к некоторым формам цифрового управления на национальном уровне может повысить риск фрагментации Интернета на техническом уровне. Однако регуляторные базы должны учитывать требования, соответствующие различным условиям, и успевать за стремительными изменениями технологий и сервисов.

- **Необходим более широкий обмен знаниями и информацией между заинтересованными сторонами** для дальнейшего обсуждения вопросов кибердипломатии как развивающегося феномена, а также для рассмотрения возможности допустимых вмешательств. Органы по стандартизации должны продолжить поддержку заинтересованных сторон и взаимодействие с ними и улучшать взаимопонимание между политическим и техническим сообществами. Технические решения, влекущие за собой политические последствия, должны обсуждаться органами по стандартизации с прямым участием всех затрагиваемых заинтересованных сторон.

Управление данными и защита приватности

Тема

В эпоху цифровизации и глобализации данные являются ключевым ресурсом. Движение данных управляет экономикой, а анализ данных, включая аналитику больших данных, является фундаментом удивительных инноваций в самых разных областях – от финансов до здравоохранения и правоохранительной деятельности.

Однако сложные вопросы, связанные с широким использованием данных, их привычной трансграничной передачей и взаимозаменяемостью, по-прежнему не решены. Как международный коммерческий актив, потоки данных существуют в условиях слабой согласованности национальных правовых режимов и значительных трудностей правоприменения. Конфиденциальность персональных данных слишком часто приносится в жертву при обмене данными, их сборе, применении и хранении, что имеет глубокие последствия для поддержания доверия и обеспечения безопасности.

Чтобы задействовать значительный потенциал данных в экономических и исследовательских целях, необходимо возобновить дискуссии об управлении, целостности, а также о защите приватности.

Послания

Центральная роль данных

- **В эпоху растущей цифровизации данные стали критическим ресурсом**. Потоки данных играют важнейшую роль в международной кооперации во многих областях, включая научные исследования, правоприменение, национальную и глобальную безопасность. Данные, безопасность данных и защита данных являются ключевыми элементами устойчивого развития. Путем эффективного использования данных и обмена ими на глобальном уровне можно решить общие проблемы и устранить угрозы, связанные с целым рядом кризисных явлений, таких как пандемии и изменение климата.

- **Данные одновременно приносят прибыль и имеют серьезную общественную ценность**. Однако выгоды экономики, основанной на данных, до сих пор распределялись неравномерно. Многие люди обеспокоены тем, что становятся главным образом поставщиками данных, а не выгодоприобретателями.

- **Отношения между теми, кто производит данные, и теми, кто использует данные, крайне важны**. Недостаток данных является серьезной проблемой, которая проявляется особенно остро в локальных сообществах и среди уязвимых групп населения. Отсутствие конфиденциальности данных и их недостаточная защита подрывают доверие к механизмам управления данными. Важно развивать грамотность в использовании данных и навыки работы с ними на всех уровнях государственного управления, в рамках образовательных программ и среди широких слоев населения.

- **Управление данными в широком и узком смысле представляет собой сложную проблему национальной и международной политики**. Разработки, связанные с данными, включая

аналитику больших данных, инновации в области искусственного интеллекта и машинного обучения, инновации, охватывающие различные аспекты государственной политики и достижения ЦУР, сопряжены с необходимостью уделять должное внимание политическому, экономическому и социальному воздействию описанных разработок, а также осуществлять тонкое политическое вмешательство. Для внедрения эффективных национальных рамочных программ по управлению Интернетом правительству и органам регулирования необходимы соответствующие мощности и инфраструктура. Разработчики приложений обязаны обеспечить их этичное и безопасное устройство.

Конфиденциальность данных и справедливость на основе данных

- **Конфиденциальность данных – это не вопрос удобства или внедрения эффективной практики, а вопрос соблюдения прав человека**. С ней связано не только обеспечение тайны частной жизни, равного отношения и недискриминации, но и других прав человека, в том числе прав на охрану здоровья, образование, получение государственных услуг, а также демократических прав, таких как право на свободу выражения мнения и право объединения с другими. Законы о приватности должны быть содержательными, основанными на фактических данных, осуществимыми, а также доступными для понимания теми, кто подпадает под их действие.

- **Потоки данных и обмен данными должны существовать без ущерба для конфиденциальности данных.** Конфиденциальность персональных данных зачастую приносится в жертву в процессе обмена данными – начиная со сбора информации и заканчивая ее использованием, – с чем связано появление преднамеренных и непреднамеренных угроз доверию и безопасности. Доступ в Интернет и использование Интернета не должны находиться в зависимости от отслеживания данных: пользователи должны иметь право выбирать, каким объемом информации они делятся, в том числе информации, связанной с их действиями в Интернете. Персональные данные не должны экспортироваться в юрисдикции, не предоставляющие надлежащих гарантий.

- **Правовые меры должны быть направлены не только на защиту данных, но и на обеспечение справедливости на основе данных, то есть обеспечение таких условий, при которых человек может выбрать, каким образом будут использованы персональные данные, и получить свою долю доходов и выгод от инноваций**, основанных на наборах данных, которые получены с помощью данных, предоставленных человеком. Таким образом, меры по защите приватности должны способствовать повышению безопасности и процветанию цифровой экономики.

- **Правительства и регуляторы должны обеспечить защиту персональных данных**, определив степень дифференцированной ответственности различных заинтересованных сторон и не возлагая чрезмерную нагрузку или ответственность на отдельных пользователей. Политика управления данными должна разрабатываться при содействии многих заинтересованных сторон, чтобы сложности, связанные с ее внедрением, были приняты в расчет.

- **Вопросы приватности и защиты данных имеют особое значение для управления искусственным интеллектом и машинного обучения**. Все заинтересованные стороны, участвующие в цепочке поставок ИИ, должны сыграть свою роль в поддержке права на неприкосновенность частной жизни.

- **Необходимо участие независимых надзорных органов, имеющих надлежащие ресурсы**. Службы по защите данных должны иметь полномочия по управлению регистрацией данных, предоставлению указаний, проведению расследований и рассмотрению жалоб субъектов данных.

Управление данными

- **Вопросы, связанные с управлением данными, не должны решаться изолированно или без учета их влияния**. Текущий ландшафт в области управления данными представляет собой раздробленный набор национальных, региональных и международных правил, определяющих ответственность национальных правительств, предприятий частного сектора и отдельных лиц.

- **Для формирования сбалансированного подхода, обеспечивающего использование данных в интересах людей и планеты, необходима бóльшая согласованность действий на глобальном уровне**. Законодательство и нормативно-правовые базы, действующие на национальном, региональном и международном уровнях, зачастую оказываются недостаточными, не поспевают за изменениями в технологиях, приложениях и должны стремиться к тому, чтобы обеспечить соблюдение высоких стандартов безопасности компаниями и другими организациями, ответственными за хранение данных.

- **Различия в условиях и вызовах, истории, культуре, правовой традиции и регуляторных структурах означают, что не может существовать единого, жесткого свода правил, подходящего для всех**. Различные лица и организации видят в широком смысле схожие подходы по-разному. Однако, хотя государства и регионы должны разработать свои собственные подходы к управлению данными, необходимо также обеспечить согласованность и интероперабельность, чтобы упростить передачу данных и предоставить всем равные условия.

- **Прозрачность, участие и ответственность являются важными факторами качественного управления данными**. Управление данными включает в себя следующие значимые аспекты, не ограничиваясь ими: стандарты в области данных и классификацию данных; обмен данными, их совместное использование и интероперабельность; безопасность и конфиденциальность данных; инфраструктуру данных; данные и цифровую идентичность; справедливость и беспристрастность на основе данных; прослеживаемость, прозрачность и объяснимость данных; минимизацию и ограничение данных; точность и качество данных; предвзятость, маргинализацию и дискриминацию данных; жизненный цикл, специфичность и хранение данных; ответственное использование данных и этику обращения с данными; ущерб от использования данных, безопасность и защиту данных.

- **Многие заинтересованные стороны, в том числе регуляторы, исследователи, организации по стандартизации, потребительские организации и конечные пользователи, играют определенные роли в текущем процессе и должны использовать свою власть и влияние для содействия эффективному управлению данными**. Политика управления данными должна быть разработана при содействии сообщества всех заинтересованных сторон, обладающих как опытом участия в юридической полемике вокруг приватности, так и опытом преодоления «реальных» трудностей, связанных с внедрением эффективных решений в области конфиденциальности данных.

- **Развивающимся экономикам необходимо расширять свои институциональные возможности управления данными, их использования и обработки комплексными, объективными, доказательными методами, в том числе путем региональной и глобальной кооперации**. Для этого требуется сформировать более глубокое представление об институциональном потенциале чиновников и заинтересованных сторон.

Трансграничная передача данных

- **Трансграничная передача данных необходима для осуществления различных процедур, связанных с электронной коммерцией и цифровой торговлей.** Эффективность внутрирегиональной торговли и управления цепочками поставок зависит от бесперебойности движения потоков данных, а также товаров, услуг и капитала. Однако в этой связи требуется разработка комплексных межсекторальных требований, направленных на сближение регуляторных практик, гармонизацию нормативно-правовой базы, управление Интернетом, реформирование политики в области информационно-коммуникационных технологий, а также стратегическое внедрение региональной инфраструктуры.

- **Действующих многосторонних, региональных и двусторонних торговых соглашений недостаточно для обеспечения текущей и будущей трансграничной передачи данных.** Сегодня передача данных осуществляется в почти не регулируемой среде, в условиях слабой согласованности национальных правовых режимов. Используемые подходы различаются и носят контекстуальный характер, что создает торговые барьеры, причем у многих стран сегодня отсутствует соответствующее законодательство или правоприменительный потенциал. Возрастает необходимость разработки и гармонизации мер, направленных на управление трансграничной передачей данных, а также содействующих развитию и извлечению экономической ценности, в зависимости от контекста, и вместе с тем соблюдающих национальный суверенитет и приватность пользователей.

Обеспечение безопасности, защиты и ответственности

Тема

Безопасность Интернета находится под угрозой по нескольким причинам. Кибербезопасность традиционно представляет собой защиту сетей, устройств и данных от неавторизованного доступа или использования в преступных целях. С этим связана текущая проблема кибератак, которые могут осуществляться отдельными лицами или быть санкционированными государством и целью которых являются гражданские, коммерческие или правительственные объекты. Ряд факторов, включая отсутствие широких юридически обязывающих соглашений в области кибербезопасности и недостаточная защищенность сетей, способствует утрате возможностей, связанных с использованием экономических выгод цифровых технологий, особенно в развивающихся странах.

Вопросы безопасности, защиты и ответственности многоаспектны и в числе прочего охватывают темы, связанные с инфраструктурой, сервисами, контентом и другими сторонами функционирования Интернета. Так, наше сегодняшнее представление о безопасности и защите включает в себя подходы к сохраняющимся проблемам дезинформации и появления недостоверной информации в Интернете. В последние годы эти проблемы усугубляли последствия пандемии COVID-19 и создавали значительную угрозу электоральным процессам по всему миру. В данном контексте стала очевидной необходимость введения мер ответственности за действия, связанные с недостоверным контентом, и формирования четких критериев его определения.

Понятие «безопасность» может быть расширено и в таком случае включает в себя экологическую безопасность, в том числе усилия по «озеленению» Интернета и сокращению выбросов углекислого газа, причиной которых является потребление цифрового контента. Необходимость решения проблем, вызванных влиянием цифровизации на окружающую среду, становится все более важной темой для обсуждений, проходящих в рамках ФУИ.

Послания

Роль ответственных лиц и инстанций, реализующих соответствующую политику

- **Кибербезопасность следует рассматривать как центральную проблему интернет-политики.** Соображения, касающиеся доверия и защиты, в том числе уважения к правам человека, открытости и прозрачности принятия политических решений, должны стать неотъемлемой частью процессов обеспечения безопасного, защищенного доступа и разработки подхода с участием всех заинтересованных сторон, отвечающего интересам конечных пользователей.

- **Обеспечение кибербезопасности и предотвращение киберпреступлений являются важными направлениями политики, требующими серьезного внимания и развития соответствующих знаний**. Однако данные направления имеют разные цели и потому требуют разного подхода. Подход, доказывающий свою эффективность при реализации одного направления, не будет эффективным при реализации другого без должной корректировки и пересмотра.

- **Проблемы кибербезопасности и киберпреступности выходят за пределы отдельных организаций или стран. Их решение требует:**

a) **применения общегосударственного и общесоциального подходов**, предполагающих создание крепких партнерских отношений и осуществление скоординированных усилий со стороны парламентов, регуляторов и других релевантных органов власти и государственных учреждений, а также частного сектора, технического сообщества, научного сообщества и гражданского общества;
b) **эффективной и результативной региональной и международной кооперации**, которая носила бы межправительственный, многосторонний характер и осуществлялась при участии всех заинтересованных сторон.

- **Правительства, частный сектор и техническое сообщество не должны допускать принятия таких законов и установления таких стандартов в области киберпреступности, которые могли бы негативно отразиться на деятельности сторон, обеспечивающих кибербезопасность.** Следует пригласить к разработке политик все заинтересованные стороны, а также способствовать взаимодействию и обмену опытом и знаниями между различными заинтересованными сообществами.

- **Гражданское общество должно принимать участие в обсуждении как вопросов киберпреступности, так и вопросов кибербезопасности.** Для эффективной работы заинтересованные стороны, представляющие гражданское общество, должны расширять круг своих знаний в области различных релевантных подходов и проблем, а также взаимодействовать с другими заинтересованными сторонами в целях сбора информации и ресурсов, необходимых для полноценного участия в разработке политики.

Кибербезопасность

- **Международное сообщество должно искать практические пути интеграции усилий по укреплению потенциала, связанного с обеспечением кибербезопасности, в более широкий спектр мер, направленных на цифровое развитие**. Некоторые противоречия между стремлением содействовать цифровизации и необходимостью обеспечивать эффективную работу механизмов кибербезопасности препятствуют формированию безопасной, защищенной онлайн-среды и достижению Целей устойчивого развития. Меры по повышению устойчивости цифровой инфраструктуры необходимы, но их недостаточно. Давно созрела необходимость использовать действующие международные соглашения для реализации практически осуществимых мер.

- **Стандарты, направленные на обеспечение кибербезопасности, крайне важны для формирования открытого, защищенного и устойчивого Интернета, способствующего социальному прогрессу и экономическому росту, а также играют особую роль в защите тех, кто еще не подключен к Интернету**. Такие стандарты уже разработаны, но для достижения максимальной эффективности необходимо значительно расширить их использование. Организация Объединенных Наций могла бы ускорить глобальное внедрение ключевых стандартов, включив рекомендации по их применению в Глобальный цифровой договор, поддерживая их защиту и укрепление потенциала, а также содействуя инициативам по проверке и контролю их реализации. Повышение осведомленности и укрепление потенциала в области стандартов должны входить в круг приоритетных направлений и в тех регионах, где многие люди еще не подключены к Интернету и происходит расширение использования Интернета.

- **Необходимо прилагать дополнительные усилия по повышению осведомленности лиц и органов, принимающих политические решения на национальном уровне и других заинтересованных лиц о проблемах в области кибербезопасности, международных норм и принципов**. Данные усилия должны включать в себя действия по повышению осведомленности и укреплению потенциала в области связи между устойчивым развитием и кибербезопасностью, а также по объединению различных заинтересованных сторон для содействия эффективному, устойчивому и инклюзивному руководству международной кооперацией в целях обеспечения киберустойчивости. Для поддержки данного процесса уже был разработан ряд международных инициатив. Финансирующие учреждения и другие заинтересованные стороны также должны рассмотреть возможности финансирования проектов по достижению киберустойчивости.

- **Нормы кибербезопасности должны качественно изменить прошлый, текущий и будущий опыт интернет-пользователей**. В этой связи, особенно при разработке новых норм, необходимо прислушиваться к опыту отдельных лиц и организаций, ставших жертвами кибератак, а также тех, кто первым реагировал на них и принимал соответствующие меры противодействия.

Киберпреступность

- **Киберпреступность представляет собой растущую угрозу для многих пользователей Интернета**. Положения, связанные с противодействием киберпреступности, должны учитывать размеры, возможности и ресурсы платформ. При введении юридических обязательств необходимо принимать во внимание многообразие субъектов технического сектора и исходить из потребностей и обстоятельств функционирования малого бизнеса при выполнении юридических обязательств, например при противодействии террористическому или насильственному экстремистскому использованию услуг бизнеса.

- **Правительства и политики должны обеспечить, чтобы правовые меры в ответ на преступное или террористическое использование Интернета находились в согласии с принципом верховенства закона и правами человека**, а также в полной мере учитывать право на свободу выражения мнения и обеспечивать прозрачность и подотчетность при реализации мер по борьбе с киберпреступностью.

Контент и дезинформация

- **Проблему дезинформации можно и следует решать с помощью механизмов управления рисками, а именно рисками, с которыми сталкиваются общества и отдельные лица, защищая свободу выражения мнения, плюрализм и демократический процесс**. Поддержка профессиональной журналистики и медиа, включающая в себя приверженность существующим принципам журналистики, играет важную роль при решении проблемы дезинформации.

- **Навыки в области медиа и цифровой грамотности позволяют гражданам более критически относиться к контенту или обнаруживаемой информации и помогают им выявлять дезинформацию и недостоверную информацию, а также расширять демократическое**

участие. Развитие цифровой грамотности может повысить осведомленность в области безопасности в Интернете, особенно среди наиболее уязвимых лиц и сообществ. Соответствующие инициативы должны учитывать потребности и риски, связанные с особенностями различных групп населения. Так, разные подходы в отношении представителей молодежи и более старших поколений должны отвечать различиям в навыках пользования.

- **Дисциплины по развитию цифровых навыков должны быть включены в образовательные программы для обеспечения безопасности детей в онлайн-пространстве.** Соответствующие инициативы должны осуществляться с участием родителей, учителей и опекунов. Законодатели и цифровые платформы должны принять на себя ответственность за обеспечение безопасности детей в рамках нормативной базы по реализации прав детей в цифровом пространстве, соответствующей международным соглашениям в области прав человека, в том числе Конвенции ООН о правах ребенка.

- **В данном контексте система доменных имен имеет ограниченный технический потенциал.** Для определения того, когда и каким образом она должна быть использована для устранения определенных проблем, связанных с контентом, и укрепления процессуальных норм, необходимо продолжать диалог заинтересованных сторон.

- **Шифрование играет важную роль в формировании открытого, безопасного и демократичного Интернета**, способствуя достижению безопасности, приватности пользователей и их свободы выражения мнений. Необходимо решать вопросы, связанные с правоприменением и способностью пользователей управлять доступом для защиты детей и в иных целях.

- **Недостатки перевода создают значительные трудности, которые могут препятствовать полноценному ознакомлению конечных пользователей со стандартами и политиками платформ.** Некачественный перевод ключевых терминов приводит к их неоднозначному толкованию. Взаимодействие различных языковых сообществ в целях повышения точности и уместности перевода, в том числе при передаче понятий, не имеющих прямого эквивалента в языках перевода, имеет особое значение, поскольку позволяет платформам и пользователям понять, что от них требуется.

Передовые технологии, включая искусственный интеллект (ИИ)

Тема

Передовые технологии все больше меняют экономику и общество. В число таких технологий входят системы искусственного интеллекта (ИИ), которые управляют нашим опытом пользования Интернетом, обеспечивают работу умных устройств и влияют как на наши решения, так и на решения, принимаемые другими в отношении нас, а также робототехника и приложения Интернета вещей, используемые в самых разнообразных сферах, например в промышленном производстве, здравоохранении и сельском хозяйстве. Однако помимо потенциала у таких технологий есть и серьезные недостатки. Так, использование алгоритмических систем принятия решений может привести к предвзятости, дискриминации, стереотипизации и усилению социального неравенства, а системы на основе ИИ могут поставить под угрозу безопасность человека и соблюдение его прав. Применение устройств Интернета вещей связано с проблемами в области кибербезопасности и защиты приватности. Использование технологий дополненной и виртуальной реальности сопряжено с вопросами в области общественной безопасности, защиты данных и защиты прав потребителей.

Извлечение выгод из возможностей, предоставляемых передовыми технологиями, и одновременное решение сопутствующих проблем и устранение рисков – это задача, к решению которой ни один актор не может приступить изолированно. Диалог и кооперация всех заинтересованных сторон, в том числе правительств, межправительственных организаций, технологических компаний, гражданского общества и других, необходимы, чтобы обеспечить такое развитие и применение обозначенных технологий, которое ориентировано на интересы человека и соблюдение его прав.

Послания

Управление

- **При разработке передовых технологий, включая искусственный интеллект, должны быть учтены принцип верховенства закона, права человека, демократические ценности и принцип многообразия, а также подготовлены соответствующие меры безопасности.** Передовые технологии должны использоваться на благо людей и планеты, способствуя инклюзивному росту, устойчивому развитию и процветанию. Механизмы надзора и правоприменения должны функционировать в соответствии с определенными принципами и нормами, причем акторы ИИ должны нести ответственность за любой причиненный ущерб.

- **Предположение, что использование технологий всегда способствует достижению равенства, ложно**. Те, кто разрабатывает технологии машинного обучения или подбирает данные, необходимые для обучения программ искусственного интеллекта, зачастую являются нерепрезентативными членами своего сообщества. Технологии могут усилить существующее неравенство и причинить ущерб, в особенности уязвимым и маргинализированным группам населения.

- **Обществам нужно адаптироваться к трансформации, которую повлечет за собой применение ИИ, посредством преобразования рамочных программ по сотрудничеству и**

изменения модели управления. Формирование интеллектуального общества, ориентированного на человека, требует полноценной кооперации правительств, предприятий, общественных организаций и научного сообщества. Постоянный человеческий контроль по-прежнему необходим для недопущения нежелательных или неконтролируемых последствий использования алгоритмов. В этой связи одним из ключевых аспектов является устранение барьеров между инженерами и экспертами в области политики.

- **Глобальное соглашение по вопросам установления норм в области ИИ не может быть достигнуто в результате простой разовой процедуры**. Сегодня уже действуют некоторые нормы, однако они представлены главным образом не обязывающими принципами, а нормами «мягкого» права. Разработка полноценных глобальных стандартов потребует эффективного участия всех стран, включая развитые и развивающиеся, а также региональных инициатив и вовлеченности всех заинтересованных сторон.

- **Укрепление потенциала крайне важно в рамках усилий по решению вопросов, касающихся передовых технологий**. Политика, направленная на повышение грамотности в области ИИ, развитие соответствующих навыков и обеспечение языковых ресурсов для миноритарных языков, необходима для формирования подлинно глобального подхода к применению передовых технологий.

Доверие, безопасность и приватность

- **Нормативно-правовые базы должны включать в себя принципы, дающие социальным медиа и другим платформам возможность соблюдать обязательства, связанные с проявлением должной осмотрительности в отношении управления контентом, который может причинить ущерб демократии и нарушить права человека**. Рамочные программы должны способствовать глобальному диалогу на тему модерации интернет-контента в интересах пользователей, включая представителей наиболее уязвимых групп и носителей миноритарных языков. Аффективные (эмоциональные) вычисления и другие новейшие технологии, связанные с распознаванием, интерпретацией и симулированием человеческих эмоций компьютером, требуют многомерной этической оценки.

- **Обеспечение прозрачного функционирования и отчетности алгоритмических систем абсолютно необходимо для соблюдения прав человека**. ИИ упрощает непрерывный контроль и анализ данных для персонализации и таргетирования контента и рекламы. Вследствие соответствующей персонализации опыта пользования Интернетом возникает риск разделения информационных онлайн-пространств и ограничения доступа отдельных лиц к информации во всем ее многообразии. Отсутствие информационного плюрализма может способствовать манипуляции и обману, тем самым усиливая неравенство, препятствуя демократической дискуссии и потенциально содействуя цифровому авторитаризму, насилию и разжиганию ненависти.

- **Заинтересованные стороны, относящиеся к техническому и другим сообществам, должны делиться знаниями и взаимодействовать в целях разработки принципов, указаний и стандартов**, которые были бы достаточно гибкими для использования в различных условиях и укрепляли доверие по отношению к системам ИИ.

- **Важно учитывать и уважать различный институциональный и культурный опыт стран и сообществ**, а также способствовать инклюзивности и содействовать международной кооперации в области ИИ.

Права и модерация контента

- **Абсолютно необходимо, чтобы политики управления контентом онлайн-платформами и применение данных политик соответствовали международным стандартам в области прав человека**. Технологии искусственного интеллекта и машинного обучения уже используются для принятия решений о том, какой контент стоит публиковать, удалять, приоритизировать, а также о том, среди каких пользователей его следует распространять. Данные инструменты играют важную роль в формировании политического и общественного дискурса и оказывают влияние на реализацию индивидуальных и коллективных прав человека, включая социальные, экономические, культурные права и права, связанные с обеспечением международного мира и безопасности. При этом прозрачность применения таких инструментов, сопряженная с этим ответственность и общественный контроль зачастую оказываются слабыми или полностью отсутствуют. Описанная ситуация должна быть исправлена.

- **Технологии, которые могут применяться для реализации прав человека, также могут быть использованы для слежки, пропаганды насильственных мер и в других целях, нарушающих вышеупомянутые права**. Непреднамеренные последствия автоматизированного управления контентом могут быть особенно пагубными в условиях конфликтов или кризисов, поскольку способны заглушить критические высказывания в ту пору, когда они особенно важны.

- **Технические стандарты являются значимым фактором, способствующим развитию и повышающим ценность цифровых технологий, связанных с ними инфраструктур, сервисов, протоколов, приложений и устройств**. Такие стандарты также оказывают серьезное влияние на реализацию прав человека. В то же время процессы разработки технических стандартов, осуществляемые в рамках организаций по стандартизации, не учитывают соображения, касающиеся прав человека, в полной мере. Зачастую данные процессы характеризуются отсутствием прозрачности, сложностью и значительной ресурсоемкостью. По этой причине гражданскому обществу и другим заинтересованным сторонам сложно получать к ним доступ и осуществлять контроль на регулярной основе. Данная проблема должна быть решена.