*Примечание: этот перевод доступен благодаря добровольному взносу Алексея Марчука. IGF ему благодарен.*

**Тезисы IGF 2020**
**ДОВЕРИЕ**

**Какие структурные элементы необходимы для обеспечения функционирования, стабильности и отказоустойчивости Интернета и онлайн-мира в настоящее время, достаточно надежные, чтобы продолжать поддерживать эффективное взаимодействие в будущем, независимо от постоянно развивающихся условий и меняющегося характера угроз?**

COVID-19 переворачивает нашу жизнь с ног на голову, а ограничения по контролю над распространением пандемии ограничивают нас в нашей самой обычной повседневной деятельности. Электронные решения, которые позволяют нам продолжать работать или учиться из дома, требуют безопасного и стабильного подключения к надежному Интернету. Для надежного Интернета требуется наличие хорошо защищенной и укрепленной Интернет-инфраструктуры.

Страны, разработавшие национальный план действий в чрезвычайных ситуациях, имеют больше возможностей для более эффективного реагирования на бедствия во время кризиса. Стратегии реагирования обеспечивают координацию и согласованность действий на всех уровнях государственного управления. Партнеры на федеральном, местном, территориальном и других уровнях играют важную роль в разработке согласованных и конструктивных мер реагирования на национальные чрезвычайные ситуации, в том числе в случаях, когда инфраструктура не подвергается воздействию, как это было в случае с кризисом COVID-19.

Пандемия COVID-19 дает возможность выявить и оценить пробелы и узкие места в цифровой инфраструктуре, а также приступить к подготовке планов действий по обеспечению доступного и надежного подключения, обеспечению достаточной пропускной способности на каждом участке сети и расширению возможности подключения для тех, кто еще не подключен или еще не имеет хорошей связи.

Глобальный трансграничный характер Интернета бросает вызов пониманию суверенитета. Трансграничное сотрудничество становится новой нормой. Интернет был прямо предназначен для того, чтобы поощрять глобальную взаимосвязанность и забывать о международных границах. Одной из основных целей было и остается объединить как можно больше людей, устройств и сетей в глобальную «сеть сетей».

Большая часть сотрудников работает из дома, что является внезапной и непредвиденной мерой по борьбе с коронавирусом. Сотрудники подключаются к своим домашним сетям вместо хорошо защищенной корпоративной сети, что создает новые и увеличивает существующие риски безопасности. Это требует особых усилий для повышения их подготовленности к вопросам кибербезопасности. Совершенствование и постоянное наращивание потенциала, образование и обучение способствуют созданию культуры кибербезопасности.

Стремительные темпы роста домашних устройств Интернета вещей вызывают обеспокоенность по поводу последствий для безопасности и конфиденциальности их пользователей. Руководства, материалы и рекомендации необходимо публиковать в

удобном для пользователя формате и использовать язык с меньшим количеством жаргонных выражений и технической терминологии.

---

**Что могут сделать стейкхолдеры, начиная от моделей управления и заканчивая конкретными инициативами по созданию Интернета, который является безопасным и защищенным онлайн-пространством для всех, поддерживает уважение прав человека и защиту наших детей, минимизацию рисков и потенциального вреда для пользователей и искоренение дискриминации?**

Правительствам необходимо ускорить цифровую трансформацию и развивать онлайн-каналы, которые имеют решающее значение для коммуникации и обеспечения доступа граждан к важной информации в период кризиса.

Проверка фактов требует сотрудничества на местном и международном уровнях, а также навыков и ресурсов, необходимых для того, чтобы справиться с потоком информации, разнообразием источников и языковым разнообразием. Надлежащей проверке фактов препятствует политическое давление, а также финансовые и правовые угрозы.

Проверка фактов останется неэффективной, если не будут доверять средствам проверки фактов. Участие правительства в инициативах по проверке фактов может укрепить или подорвать это доверие.

Боты – важные инновационные и эффективные инструменты для автоматизации задач по борьбе с дезинформацией. Сэкономленные ресурсы можно сконцентрировать на задачах, требующих контроля со стороны человека. Транспарентность имеет решающее значение для недопущения того, чтобы боты ограничивали основные права, такие как свобода выражения мнений и доступ к информации. У транспарентности много уровней: внутренняя работа инструментария, используемые критерии и их воздействие, а также то, кто применяет инструмент и какова цель.

Производство и распространение незаконного и вредоносного контента – это две разные вещи, требующие особой бдительности. Алгоритмическое усиление рискует автоматизировать распространение такого контента.

Образование, медиаграмотность и общественный диалог, способствующие уважению к фактам и науке, содействуют борьбе с онлайн дезинформацией, а также восстановлению доверия к журналистике и повышению транспарентности в том, как социальные медиа-компании (и их алгоритмы) обрабатывают информацию. Обучение молодых людей навыкам критического мышления должно начинаться с раннего возраста.

Стейкхолдеры, исследователи и разработчики должны сотрудничать с целью разработки технических инструментов и применения методов искусственного интеллекта и машинного обучения, чтобы распознавать и устранять проблемы, связанные с высказываниями, разжигающими ненависть, а также распространением дезинформации и фальшивых новостей в сети.

Обсуждения и повышение осведомленности о борьбе с дезинформацией и языком вражды нельзя откладывать, их необходимо усилить. Борьба с фальшивыми новостями является общей и личной ответственностью. Пользователи должны проявлять бдительность и нести ответственность за то, чем они делятся в Интернете, а не прятаться за технологиями или перекладывать всю ответственность на платформы социальных сетей.

Технологии как решают проблемы, так и создают их. Цифровой мир полон возможностей для детей учиться, играть, развивать свой потенциал и защищать свои права, но он также

изобилует опасностями, которые могут нанести вред или ущемить их права. Ученые и специалисты в области поведенческих наук и психического здоровья должны активизировать свои исследования относительно положительного и отрицательного воздействия онлайн-активности, включая влияние игр на развитие и благополучие детей, чтобы их выводы могли служить ориентиром при разработке политики и отраслевой практики. Дети, родители, педагоги, представители отрасли и лица, ответственные за разработку политики, должны быть вовлечены в разработку сбалансированного подхода, который управляет рисками при максимальном использовании возможностей.

---

**Как создать среду, способствующую диалогу между стейкхолдерами, в которой недоверие, страх и непонимание уступают место взаимному доверию и признанию роли друг друга, а игроки сотрудничают в выработке комплексных ответов на вызовы безопасности в онлайн-мире?**

Деловые круги, правительство, техническое сообщество и многосторонние организации должны сотрудничать для выработки адекватных ответов на вызовы на национальном, международном и глобальном уровнях, возникающие в результате таких кризисов, как COVID-19.

Пандемия показала, как технологии и социальные сети могут стать спасательным кругом для поддержания связи с друзьями и семьей, продолжения экономической деятельности и сбора информации. IGF должен способствовать диалогу о совместной ответственности и действиях стейкхолдеров, в том числе, при необходимости, о регулировании, с тем чтобы пользователи всегда могли взаимодействовать и общаться в безопасной онлайн-среде.

Инициативы по учету мнений и взглядов различных стейкхолдеров в диалогах ООН по вопросам кибербезопасности получили положительную оценку, однако необходимо приложить больше усилий для того, чтобы сделать эти диалоги и возможности для внесения своего вклада более наглядными, включая поддержку и наращивание потенциала для вовлечения стран и сообществ в процесс преодоления цифрового разрыва. Инициативы по наращиванию потенциала правительств развивающихся стран должны подготовить их к участию в международных и глобальных дискуссиях и инициативах, касающихся кибербезопасности, и отразить точку зрения и интересы местных сообществ и государств.

Защита детей в сети, в том числе в онлайн-играх, является новой и быстро развивающейся областью политики и неотъемлемой частью глобального управления Интернетом. Все стейкхолдеры должны взять на себя ответственность, укреплять сотрудничество и координировать адекватное сочетание государственных, частных, правовых и добровольных мер на национальном и международном уровнях. В качестве стандартной практики стейкхолдеры должны консультироваться с детьми по вопросам, которые влияют на их жизнь, включая их жизнь в сети.

Различия между регионами (географические, экономические, политические, культурные) могут быть значительными, и это приводит к тому, что передовая практика не применима напрямую к каждому региону. Привлечение множества партнеров благоприятно сказывается на устойчивом наращивании кибернетического потенциала. Сотрудничество и обмен передовым опытом между более и менее развитыми регионами и странами так же важны, как и межрегиональный обмен между одинаково развитыми регионами-партнерами. Доверие между стейкхолдерами внутри и между регионов будет способствовать обмену передовой практикой. Доверие, легитимность и участие всех соответствующих стейкхолдеров являются основой любого значимого проекта по наращиванию потенциала.

Механизмы доверия в киберпространстве, основанные на принципах ответственности, транспарентности, уважения, взаимных консультаций и взаимопонимания, должны

устанавливать открытое сотрудничество между сторонами, включая правительства, международные организации, предприятия, технические сообщества, научно-исследовательские учреждения и отдельных лиц, и изучать широкий спектр таких инструментов, как законы и правила, потенциал ИТ, социальная ответственность, этика, надзор и самодисциплина, а также нормы и стандарты.

Обеспечение безопасности и конфиденциальности имеет важное значение для процветания экосистемы Интернета вещей, в то время как руководящие принципы и соответствующий процесс принятия решений должны вовлекать различные заинтересованные стороны, включая гражданское общество и лиц, ответственных за разработку политики. Присутствует недостаточная осведомленность о рисках, связанных с Интернетом вещей, и необходимость принятия мер по наращиванию потенциала для представления передовых практик и предотвращения угроз. IGF располагает всеми возможностями для промежуточного этапа такого процесса.