

# Вебинар: Использование интернета террористами и пробелы в нормативно-правовой базе



12 марта, 11:00 - 12:30 CET

## ИТОГОВЫЙ ДОКУМЕНТ

Данное онлайн-мероприятие было организовано **Антитеррористическим подразделением** Департамента по противодействию транснациональным угрозам (ДПТУ) Секретариата ОБСЕ, при поддержке албанского председательства Группы азиатских партнеров ОБСЕ по сотрудничеству, и Секции внешнего сотрудничества ОБСЕ. В мероприятии приняли участие более 180 человек (72 женщины и 110 мужчин), в том числе эксперты и высокопоставленные должностные лица **государств-участников ОБСЕ и других регионов**.

Мероприятие стало продолжением обсуждений в рамках круглого стола ОБСЕ на тему ["Использование инноваций и технологий для решения вызовов и кризисов в области безопасности в XXI веке в рамках ОБСЕ и азиатских партнеров по сотрудничеству"](#), состоявшегося в ноябре 2020 года в онлайн-режиме.

Состоявшийся 12 марта вебинар предоставил участникам возможность рассмотреть **текущие и зарождающиеся тенденции**, а также ключевые вопросы, связанные с национальными нормативно-правовыми основами по выявлению незаконного контента в интернете, а также по вопросам того как онлайн-платформы решают эти проблемы при помощи своих "договоров на предоставление услуг". В ходе экспертных обсуждений особое внимание было уделено тому, каким образом инициативы по

борьбе с различными проявлениями насильственного экстремистского и террористического контента в интернете могут негативно влиять на соблюдение прав человека в соответствии с международными стандартами.

Среди участников вебинара были представители различных исполнительных структур ОБСЕ, а также исследователи и практикующие специалисты из Канады, Италии и Японии. Состоявшиеся обсуждения отразили растущую озабоченность по поводу того, как **ответные меры государств могут непреднамеренно ограничить свободу выражения мнений**. Хотя эффективность в уменьшении доступности незаконного контента имеет решающее значение, стратегии, принимаемые государствами, технологическими компаниями и гражданским обществом, должны также обеспечивать соблюдение прав человека.

В целях дополнения мер государственного регулирования и удаления контента превентивными мерами, государства несут основную ответственность за **повышение цифровой грамотности и осведомленности своих граждан**, основываясь на подходе здравоохранения, который сфокусирован на защитных факторах по принципу «не навреди». Один из главных посылов мероприятия состоял в том, что насильственный экстремистский и террористический контент в интернете можно эффективно обуздать только путем сочетания ответных и превентивных мер.

В своих выступлениях **послы Игли Хасани** (Постоянный представитель Албании при ОБСЕ, Председатель Группы азиатских партнеров ОБСЕ по сотрудничеству) и **Алена Купчина** (Координатор деятельности ОБСЕ по противодействию транснациональным угрозам) подчеркнули факт эскалации угроз, связанных с террористическим и насильственным экстремистским контентом, а также с другими вредоносными явлениями в интернете. Они отметили то, каким образом цифровая трансформация усугубляет эти угрозы и что государства пытаются реагировать на них методами, соответствующими международным стандартам в области прав человека.

**Представитель ОБСЕ по вопросам свободы средств массовой информации Тереза Рибейро** подчеркнула далеко идущие последствия контртеррористических и анти-«экстремистских» подходов для свободы средств массовой информации во всем регионе ОБСЕ. Она заявила, что законы о борьбе с "экстремизмом", в частности, используются для преследования журналистов и других лиц за сообщения или выступления по вопросам, представляющим общественный интерес.

**Д-р Эдуардо Селест из Факультета права и управления Дублинского городского университета** подчеркнул двойственный характер социальных сетей как инструмента, который может как увеличить возможности для реализации прав человека, так и использоваться для ущемления этих же прав.

Центральная Азия была упомянута одним из выступавших в качестве примера региона с растущей цифровой экономикой, где в настоящее время более половины населения имеет доступ к интернету. Опираясь на исследование, проведенное [SecDev Group](#), **Рафал Рохозински** (генеральный директор SecDev Group) отметил, что необходимо оценить риски, связанные с использованием интернета террористами и насильственными экстремистами в Центральной Азии. По словам г-на Рохозински, террористические и насильственные экстремистские экосистемы в регионе невелики, но действенны. Несмотря на сравнительно низкую привлекательность, эти системы оказались устойчивыми по отношению к мерам, применяемым государствами по ограничению доступа к ним. Террористические онлайн сети адаптируются и расширяют свой охват с помощью т.н. “сетей амплификаторов”<sup>1</sup>.

**Д-р Мотохиро Цучия из Университета Кэйо в Японии**, описав существующую ситуацию в Японии, имеющую относительно низкий уровень риска террористических атак, поделился, что в Японии непосредственная угроза в данном направлении связана с предполагаемой возможностью кибератак на предстоящих Олимпийских играх. Он подчеркнул важность нахождения правильного баланса между государственной политикой, образованием, вовлечением и охраной правопорядка при решении рисков и проблем во все более взаимосвязанном и взаимосвязанном цифровом мире. Вместе с тем, д-р Цучия подчеркнул необходимость дальнейшего обсуждения правовых рамок, приемлемых на международном уровне, в свете того факта, что Будапештская конвенция о киберпреступности не была принята так широко, как того хотелось бы.

В ходе обсуждений был высказан ряд общих замечаний:

**Во-первых, отсутствие общепринятого определения терроризма и насильственного экстремизма имеет свои последствия.** Несмотря на то, что существует универсальное понимание параметров того, что является террористическим преступлением, социальные медиа-платформы вынуждены были разработать свои собственные (отличающиеся друг от друга) определения. Как следствие, они продолжают сталкиваться со сложными вопросами касательно того, где провести грань между законным и незаконным контентом. Модерация контента является тяжело решаемой проблемой для людей-модераторов, не говоря уже об инструментах искусственного интеллекта (ИИ), которые широко используются с этой целью.

**Во-вторых, государственные законы и соответствующие меры могут способствовать формированию прогрессивных подходов к определению того, что является, а что не является контентом террористического/насильственно-**

---

<sup>1</sup> Амплификация в онлайн сетях - это подход, при котором онлайн сообщениям придаётся позитивная окраска, и происходит их дальнейшее продвижение и распространение в более крупных по масштабам группах в социальных сетях.

**экстремистского характера.** Что касается задач по дефинициям, то государства не должны перекладывать ответственность на компании социальных сетей. Вместо этого, работая совместно с гражданским обществом, они смогут разработать минимальные стандарты для онлайн-платформ. Соответствующие определения групп и контента, а также соответствующих стратегий по их сдерживанию должны быть сбалансированы мерами профилактики преступлений и поощрением соблюдения прав человека. Участники отметили, что суды проявляют понимание в этом отношении, однако решающее значение имеют более четкие определения и руководящие принципы на уровне платформ в отношении соблюдения "надлежащих технологических процедур" и верховенства права.

**В-третьих, гражданское общество должно играть ключевую роль в отстаивании прав человека и сведении к минимуму последствий онлайн контента террористического/насильственно-экстремистского характера.** Гражданское общество играет ключевую роль в обеспечении подотчетности и прозрачности, а также в поддержке нормативно-правовой ясности в вопросах регулирования. Кроме того, поскольку законодательство часто отстает от развития технологий и общества, гражданское общество является источником инноваций. Оно играет основополагающую роль в предотвращении насильственного экстремизма и терроризма, в том числе путем продвижения цифровой грамотности, цифровой гигиены, наставничества и содействия уменьшению вредного воздействия онлайн контента.

**В-четвертых, существуют сложные проблемы, связанные с предотвращением и противодействием насильственному экстремизму и терроризму в интернете, при одновременном обеспечении уважения прав человека.** В Центральной Азии, как и в других регионах, существует реальная опасность того, что государства могут чрезмерно расширять применение мер по удалению нелегального контента, что приведет к тревожным последствиям, включая посягательство на независимость СМИ (например, права журналистов на сохранение конфиденциальности источников информации, а также попытки ограничить использование шифрования), массовая слежка и другие действия, когда происходит злоупотребление антитеррористическим законодательством приводящее к ограничению прав человека. Государствам следует рассмотреть вопрос о создании механизмов подотчетности для согласования противоречащих подходов, в том числе в партнерстве с гражданским обществом.

**В-пятых, необходимы эмпирически обоснованные обсуждения для изучения соразмерности вмешательств, направленных на регулирование онлайн контента террористического/насильственно-экстремистского характера.** Чрезмерное удаление контента может привести к подавлению свободы слова и к самоцензуре. Более того, автоматическое удаление контента с помощью ИИ может возложить на

компании принятие важных решений в отношении свободы слова, тогда как их принятие было бы более целесообразным со стороны государственных органов. При введении правил, касающихся установления сроков удаления контента, государствам следует иметь ввиду такие сроки, при которых исполнение такого рода процедур реально выполнимо и для небольших поставщиков услуг, с тем чтобы последним не пришлось выплачивать финансовые штрафы. Кроме того, необходима система надлежащего надзора, обеспечивающая соблюдение норм и правил в соответствии с обеспечением прав человека. Принципы необходимости и соразмерности являются ключевыми, и государства должны работать над применением наименее ограничительных мер и обеспечивать, чтобы эти меры подлежали надзору.

**Наконец, разрабатываемые подходы должны быть не только регулятивными и соблюдающими правозащитные аспекты, но и должны быть основаны на передовой практике и извлеченных уроках.** Имеются данные, свидетельствующие о том, что чрезмерно агрессивное удаление онлайн контента террористического/насильственно-экстремистского характера часто не срабатывает, и фактически даже может ухудшить ситуацию. Кроме того, у государств, компаний социальных сетей, и гражданского общества имеется растущая база данных о передовой практике по реально действенным мерам, включая просветительскую деятельность, кампании по обеспечению цифровой безопасности, переориентацию вмешательства и другие стратегии "перенаправления".

В заключение эксперты вебинара подчеркнули, что для устранения существующих и растущих угроз, создаваемых насильственным экстремизмом и терроризмом в интернете, важнейшее значение имеют многосторонние подходы. Ключевое значение для достижения результатов имеет подход с участием многих заинтересованных сторон, основанный на правах человека, передовом опыте и извлеченных уроках, а также опирающийся на более четкие определения того, что представляет собой контент террористического/насильственно-экстремистского характера. Основная роль в формировании норм и мер вмешательства принадлежит государствам, однако они должны быть осторожны, чтоб не выйти за допустимые пределы.

*Доклад подготовил  
доктор Роберт Мугга  
директор SecDev Group*

## ПРОГРАММА ВЕБИНАРА

### 11:00 – 11:10 ПРИВЕТСТВИЕ

- **посол Игли ХАСАНИ**, Постоянный представитель Албании, Председатель Группы азиатских партнеров ОБСЕ по сотрудничеству
- **посол Алена КУПЧИНА**, Координатор деятельности по противодействию транснациональным угрозам, Секретариат ОБСЕ

### 11:10 – 12:00 ПРЕЗЕНТАЦИИ ЭКСПЕРТОВ

- **Д-р Тереза РИБЕЙРО**, Представитель ОБСЕ по вопросам свободы СМИ
- **Д-р Эдоардо СЕЛЕСТЕ**, доцент кафедры права, технологий и инноваций, Факультет права и государственного управления, Дублинский городской университет
- **Г-н Рафал РОХОЗИНСКИ**, генеральный директор, SecDev Group
- **Д-р Мотохиро ЦУЧИЯ**, декан и профессор факультета политического управления, Университет Кейо, Японии

**Модератор:** г-жа **Джорджия ХОЛМЕР**, Глава Антитеррористического подразделения, Департамент по противодействию транснациональным угрозам, Секретариат ОБСЕ

### 12:00 – 12:10 ВЫСТУПЛЕНИЕ ДОКЛАДЧИКА

**Д-р Роберт МУГГА**, соучредитель Института Игарапе и директор SecDev Group

### 12:10 – 12:30 ВОПРОСЫ И ОТВЕТЫ