Тезисы выступления ответственного секретаря
Научно-консультативного совета при
Антитеррористическом центре
государств-участников СНГ Смирнова А.А.

Правовые основы и опыт государств-участников СНГ по противодействию дезинформации, исходящей от террористических и экстремистских организаций

Добрый день, уважаемые участники совещания экспертов! Меня зовут Смирнов Александр, я представляю Антитеррористический центр государств-участников Содружества Независимых Государств. Наш Центр является специализированным отраслевым органом СНГ и предназначен для обеспечения координации взаимодействия компетентных органов стран Содружества в области борьбы с международным терроризмом и иными проявлениями экстремизма. В состав Содружества Независимых Государств в настоящее время входит 11 государств: Азербайджан, Армения, Беларусь, Казахстан, Кыргызстан, Молдова, Россия, Таджикистан, Туркменистан, Узбекистан и Украина.

В начале своего выступления хотелось бы поблагодарить офис Представителя по вопросам свободы средств массовой информации ОБСЕ и персонально Андрея Рихтера за приглашение принять участие в таком представительном мероприятии. Для нас это прекрасная возможность услышать позиции европейских экспертов относительно противодействия информационным рискам и поделиться положительным опытом Содружества Независимых Государств в данной сфере.

Сегодня мы обсуждаем тему дезинформации и фейковых новостей. Сами эти угрозы никак нельзя считать новыми. Напротив, дезинформация всегда считалась классическим инструментом психологической войны. Например, Александром Македонским в целях оказания устрашающего воздействия на противника часто использовалась тактика, предполагавшая

распространение ложных слухов о превосходящей численности и мощи своего войска. Широко известна операция обмана с применением троянского коня, проведенная греками для завладения Троей. Все эти события происходили до нашей эры.

Однако в современных условиях угроза распространения ложной информации получила особую остроту. Этому есть несколько причин, но все они связаны с развитием новых информационно-коммуникационных технологий и их влиянием на общество.

Во-первых, развитие глобальных телерадиовещательных компаний и сети Интернет сделало реальным по-настоящему трансграничное распространение информации.

Во-вторых, развитие социальных интернет-технологий (Web 2.0) наделило пользователей возможностями трансляции информации на широкую аудиторию (то есть функционалом массмедиа), тем самым мультиплицировав количество источников массовой информации.

В-третьих, новые алгоритмы отслеживания поведения пользователей сделали возможным выстраивание персонализированной новостной ленты, показывающей ту информацию, которая соответствует их взглядам, и отсекающая противоречащие им сведения. Данное явление получило в науке название «пузыря фильтров».

В-четвертых, произошли серьезные изменения в социальной психологии аудитории массмедиа, маркированные учеными термином «постправда». В условиях постправды на формирование общественного мнения большее влияние оказывают сообщения, апеллирующие к эмоциям и личным убеждениям аудитории, нежели к истине и объективным фактам.

Указанные факторы обусловили широкое распространение фейков в новой цифровой среде. Новый потенциал для дезинформации создают технологии искусственного интеллекта, в частности позволяющие создавать так называемые «глубокие фейки» (deepfakes).

Поэтому обращение мировым сообществом пристального внимания на угрозу дезинформации считаем вполне обоснованным. Вместе с тем хотелось бы сделать несколько оговорок для правильного понимания предметного поля. Вначале отметим, что дезинформация – это не какой-то самостоятельный феномен, а широкая палитра видов коммуникации, в основе которых лежит целенаправленная передача ложной информации. Поэтому дезинформация должна, во-первых, рассматриваться наряду с другими видами деструктивной коммуникации в рамках общего предметного поля информационной безопасности; и во-вторых, изучаться в многообразии и многоликости форм своего проявления.

Дезинформация может проявиться в разных контекстах: как элемент информационной войны между государствами, как инструмент деструктивной пропаганды, как форма деструктивной межличностной коммуникации. Соответственно инструменты и методы борьбы с фейками должны быть гибкими и вариативными, особенно в отношении массмедиа. Здесь очень уместным будет предложенный Советом Европы «градуированный и дифференционный подход» к регулированию новых медиа.

Кроме того, нельзя не отметить чрезвычайную политизированность темы дезинформации, которая существенно искажает восприятие картины проявления данной угрозы. Мы постоянно видим, как некоторые страны мира фокусируют внимание на одних ложных сообщениях, в упор не замечания других. Предпринимаются попытки повесить на определенные государства и массмедиа ярлык перманентного источника фейковых новостей. Такая политика контрпродуктивна и препятствует выработке общих подходов для реагирования на общую для мировых наций угрозу.

Когда мы рассматриваем угрозу дезинформации, исходящую от террористических и экстремистских организаций, то включаем сюда ряд аспектов.

Первым и наиболее очевидным из них является *заведомо ложное сообщение об акте терроризма*. Данное деяние признается преступлением в странах СНГ. Как правило, злоумышленник по телефону сообщает о заложенном взрывном устройстве и намерении привести его в действие. Такие действия часто совершают психически больные люди, а также подростки, которые пытаются таким образом «пошутить». Хотя субъектами ложных сообщений могут выступать и террористы, которые таким образом прощупывают готовность государственных структур либо отвлекают их внимание от истинных целей атак. Опасность этого преступления состоит в том, что наносит вред общественной безопасности, нарушает нормальную жизнь общества, вносит существенную дезорганизацию в работу государственных органов, предприятий, организаций, транспорта.

Однако в последние годы получила распространение *массовая (веерная) рассылка сообщений о ложных минированиях*. Так, в России только за несколько месяцев 2019 года поступили сообщения о более чем 16 тыс. якобы заминированных объектах социальной инфраструктуры, включавших школы, детские сады, больницы, объекты транспорта. Для их рассылки использовались сервисы защищенной электронной почты и сервисы интернет-телефонии с опциями анонимайзеров, что говорит об их профессионализме и целенаправленном характере подрывной деятельности. Схожие случаи имели место и в других странах Содружества, в частности в Республике Беларусь.

Следующий блок рисков дезинформации связан с пропагандистской и вербовочной деятельностью террористических и экстремистских организаций. При ведении своей пропаганды ненависти и вражды экстремисты зачастую используют *ложные нарративы*, искажающие смысл религиозных учений, священных писаний. Сложность нейтрализации нарративов экстремистской пропаганды состоит в том, что они зачастую базируются на мифологии, которую весьма затруднительно дезавуировать через рациональные аргументы. Среди радикалов распространены мифы религиозного характера (ими пронизана идеология джихадистов) и

конспирологические теории (например, миф о «глобальном еврейском заговоре» у неонацистов).

Приемы обмана и манипуляции сознанием активно используются *при вербовке* террористами новых участников. Вовлечение адептов осуществляется как при межличностном общении, так и в ходе групповой коммуникации в многочисленных виртуальных сообществах в социальных сетях и мессенджерах. Причем в этих закрытых виртуальных группах единомышленников радикальные идеи усиливаются посредством взаимного подкрепления (эффект эхо-камеры).

Антитеррористическим центром государств-участников СНГ изучается положительный опыт компетентных органов стран Содружества в области противодействия деструктивной информационной активности террористических и экстремистских организаций, включая дезинформацию.

Правовую основу деятельности правоохранительных органов в рассматриваемой области составляют международно-правовые акты и национальное законодательство в сфере борьбы с терроризмом и экстремизмом. В рамках Содружества Независимых Государств принят ряд важных документов в рассматриваемой области, включая Договор о сотрудничестве государств-участников СНГ в борьбе с терроризмом 1999 года, Концепцию сотрудничества государств-участников СНГ в борьбе с терроризмом и иными насильственными проявлениями экстремизма 2005 года, Соглашение о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности 2013 года, а также пакет модельных законов. Ряд значимых практических мероприятий по противодействию информационным угрозам экстремистского характера закреплен в межгосударственных программах СНГ по борьбе с терроризмом и иными насильственными проявлениями экстремизма. В настоящее время действует программа, рассчитанная на период 2020-2022 годов.

Противодействие использованию дезинформации в деятельности террористических и экстремистских акторов ведется в странах Содружества в рамках следующих основных направлений:

1. *Криминализация наиболее опасных форм дезинформации и привлечение к юридической ответственности виновных лиц*: означает установление уголовной и административной ответственности за распространение дезинформации определенных типов. Как правило обязательным признаком составов таких правонарушений выступают общественные опасные последствия, наступающие в результате такой дезинформации. Выше мы говорили о криминализации заведомо ложного сообщения об акте терроризма. В 2019 году в России была закреплена административная ответственность за распространение фейковой информации в СМИ и информационно-телекоммуникационных сетях. При этом нормативно зафиксировали определение фейков как заведомо недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, создающей угрозу жизни или здоровью граждан, имуществу, общественному порядку и общественной безопасности. В качестве наказания предусмотрен штраф для физических и юридических лиц, размер которого зависит от тяжести последствий.

2. *Закрепление правовых запретов и ограничений на распространение ложной информации в массмедиа и сети Интернет*: признавая принцип свободы массовой информации, национальное законодательство стран Содружества устанавливает определенные пределы и ограничения. В частности, в российском законе о средствах массовой информации установлена недопустимость злоупотребления свободой массовой информации. К числу форм такого злоупотребления отнесено распространение материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, иной запрещенной законами информации. Под последнюю категорию подпадают

фейки. Схожий запрет закреплен в российском законе «Об информации, информационных технологиях и о защите информации». Соблюдение правовых ограничений контролируется специальным органом – Роскомнадзором.

3. *Ограничение доступа к экстремистскому контенту и ложным сообщениям в сети Интернет*: в странах Содружества установлены правовые алгоритмы, обеспечивающие ограничение доступа к противоправному контенту, включая экстремистские материалы. В последние годы предпринимаются попытки включить в поле работы данных алгоритмов фейковые сообщения. Это уже сделано в Российской Федерации, такая инициатива обсуждается в Республике Беларусь. Решение об ограничении доступа к незаконному контенту может приниматься как судебными органами, так и административными с возможностью судебного обжалования решения последних. Данные механизмы успешно работают, хотя конечно не обеспечивают создание стерильной цифровой среды.

4. *Разъяснительная и контрпропагандистская работа в офлайне и цифровой среде*: в правоохранительных органах стран Содружества сформировалось четкое понимание невозможности побороть деструктивную информационную активность экстремистов исключительно запретительными мерами. В этой связи ими во взаимодействии с иными государственными структурами и институтами гражданского общества проводится большая работа по разъяснению общественной опасности терроризма и экстремизма, возможных форм их проявления в цифровой среде, разоблачению лживых идеологических нарративов экстремистов и предложению альтернативных позитивных идей. Особое значение разъяснительная работа приобретает для борьбы с фейками, поскольку они распространяются в социальных сетях и мессенджерах со скоростью лесного пожара. Поэтому быстрое и оперативное реагирование на них критически важно. Причем в отличие от широких профилактических антиэкстремистских мероприятий, где ключевую роль играют общественные институты, нейтрализация фейков требует быстрой и

четкой реакции пресс-служб государственных органов и доведению ими информации через СМИ и иные доступные каналы.

5. *Повышение медиаграмотности и культуры кибербезопасности*: никакие внешние фильтры и самая эффективная работа публичных институтов не способны полностью нейтрализовать поток фейковых сведений и иного негативного контента. В этой связи важное значение приобретает формирование критического мышления и иных компетенций медиаграмотности конечного звена информационной цепочки – потребителя сведений. Это универсальный инструмент защиты от любых информационных угроз, ценность которого трудно переоценить. Помимо широкого комплекса обучающих мероприятий, в странах Содружества соответствующие тематические модули вводятся в программу школьного образования. Просветительские мероприятия по формированию культуры кибербезопасности проводятся и крупными компаниями IT-отрасли, такими как Яндекс и Лаборатория Касперского.

Завершая свое выступление хотелось бы отметить следующее. Цифровая среда по мере своего развития будет продолжать генерировать новые риски и модифицировать существующие угрозы. Для ответа на них требуется выработка согласованных подходов и совместных усилий, которые бы позволили эффективно противодействовать киберугрозам при соблюдении основополагающих прав человека. Локальные меры в условиях глобального информационного пространства будут заведомо недостаточными. В этой связи представляется важным реализация предложенных Российской Федерацией и поддержанных многими странами мирового сообщества инициатив по принятию универсальных международных договоров в области международной информационной безопасности, борьбы с преступностью и терроризмом в информационной среде.