КОНЦЕПТУАЛЬНАЯ ЗАПИСКА

Противодействие использованию информационно-коммуникационных технологий в террористических и экстремистских целях

Мандату Спецкомитета ООН по разработке универсальной конвенции о противодействии использованию информационно-коммуникационных технологий (ИКТ) в преступных целях соответствует создание всеобъемлющего документа. Российская Федерация выступает за включение в будущий международный договор положений о сотрудничестве между государствами-членами ООН в части противодействия использованию ИКТ в террористических и экстремистских целях. При этом в законодательстве стран, выступающих против международного регулирования борьбы с терроризмом и экстремизмом в информационной сфере, данная тематика подробно закрепляется на национальном уровне. Эти вопросы также нашли детальное отражение и в региональных конвенциях о борьбе с ИКТ-преступностью.

Национальное законодательство

США

«Патриотический акт» США 2001 г. в части, касающейся «Процедур усиленного наблюдения», предоставляет американским правоохранительным органам и спецслужбам полномочия по перехвату проводных, устных и электронных сообщений, касающихся терроризма (статья 201) и компьютерного мошенничества и злоупотреблений (статья 202). Это нормативный акт позволяет также собирать информацию о всех видах преступлений, связанных с терроризмом (использование химического оружия, оружия массового уничтожения, против американских граждан за границей, финансирование терроризма и пр.), а также вести полноформатное электронное наблюдение за террористами. Приравнял злоумышленников в информационном пространстве с преступниками, причиняющими физический вред. Документ также содержит положения о необходимости пресечения кибертерроризма (статья 814).

Великобритания

Закон о борьбе с терроризмом 2006 г. Великобритании в статье 3 «Применение к действиям в Интернете» фиксирует, что к преступлениям, предусмотренным статьей 1 («Поощрение терроризма») и статье 2 («Распространение террористических публикаций»), относятся публикации и материалы в Интернете, а также на других электронных сервисах.

Франция

Уголовный кодекс Франции распространяет действие статьи 421-1 (террористические акты) на компьютерные преступления, в т.ч. атаки на автоматизированные системы обработки данных (статьи с 323-1 по 323-8).

Европейский Союз

15 марта 2017 г. принята директива № 2017/541 по вопросам противодействия терроризму. В ней отмечается, что террористические угрозы существенно эволюционировали. Отдельно прописано, что преступное поведение должно подлежать наказанию, если оно совершается через Интернет, включая социальные сети (п.6). **Провокация совершения террористического акта, включая прославление и оправдание терроризма, а также распространение сообщений или изображений в Интернете также должны наказываться, когда имеются основания полагать, что совершение теракта возможно** (п.10) — в целях предупреждения и пресечения. Самостоятельное обучение, в том числе через Интернет или изучение других учебных материалов, также следует рассматривать как подготовку к террористической деятельности, если оно является результатом активного поведения и осуществляется с намерением совершить или способствовать совершению теракта (п.11).

В целях эффективного расследования преступлений, связанных с террористической деятельностью, и судебного преследования виновных лиц соответствующим правоохранительным органам предписано иметь

возможность использовать эффективные следственные инструменты, аналогичные тем, которые используются в борьбе с организованной преступностью или другими тяжкими преступлениями. Эти инструменты включают перехват сообщений, скрытое наблюдение, включая электронное наблюдение, съемку и хранение аудиозаписей в частных или общественных транспортных средствах и местах, а также изображения людей в общественных транспортных средствах и местах, проведение финансовых расследований (п.21).

Эффективным средством борьбы с терроризмом в Интернете рассматривается удаление онлайн-контента, представляющего собой публичную провокацию к совершению террористического акта (п.22).

Пункт 31 директивы касается противодействия радикализации и вербовки в террористические организации, включая радикализацию в Интернете.

«ДИРЕКТИВА ЕС № 2017/541:

Глава 3

Преступления, связанные с террористической деятельностью

Статья 5. Публичная провокация с целью совершения преступления, связанного с террористической деятельностью

Государства-члены ЕС принимают необходимые меры для признания в качестве уголовного преступления, если оно совершается умышленно, распространение сообщения или предоставление доступа к нему любым способом, онлайн или оффлайн, с намерением совершить подстрекательство к совершению одного из преступлений, перечисленных в пунктах (a) - (i) статьи 3(1):

- преступления, связанные с террористической деятельностью, включая разрушение информационной системы;
- производство, владение, приобретение, транспортировка, поставка или использование взрывчатых веществ или оружия, в т.ч. химического, биологического, радиологического или ядерного;
- незаконное вмешательство в систему и пр.,

если такое поведение, прямо или косвенно, например, путем прославления террористических актов, способствует совершению преступлений, связанных с террористической деятельностью, тем самым создавая опасность совершения одного или нескольких таких преступлений.»

Австралия

Уголовный кодекс 1995 г. Австралии в части 5.3, касающейся борьбы с терроризмом, в статье 100.4 «Применение положений» *(данная часть обычно применяется ко всем террористическим актам и подготовительным действиям)* предусматривает, что действие [теракт] предполагает использование электронных средств связи (пп. «h») или угроза [совершения теракта] осуществляется с использованием электронного сообщения (пп. «i»).

Новая Зеландия

Закон о пресечении терроризма 2002 г. Новой Зеландии в приложении 4D закрепляет полный текст резолюции Совета Безопасности ООН **2178 (2014)**, в котором отмечается, что государства-члены выражают озабоченность по поводу активизации использования террористами и их сторонниками коммуникационных технологий для целей доведения радикализации до уровня, порождающего терроризм, вербовки и подстрекательства других к совершению террористических актов, в том числе с использованием Интернета. Подчеркивается необходимость совместных действий государств-членов, направленных на недопущение использования террористами технологий, средств коммуникации и ресурсов для мобилизации поддержки террористических актов. Осуждается насильственный экстремизм, который может стать питательной средой для терроризма. К тому же в документе прямо прописан призыв к государствам-членам сотрудничать при принятии национальных мер, призванных воспрепятствовать использованию террористами технологий, средств связи и ресурсов для подстрекательства к поддержке террористических актов.

Региональные документы

Африканский Союз

Пункт 3 Статьи 29 «Преступления, связанные с контентом» Конвенции Африканского Союза о кибербезопасности и защите персональных данных 2014 г. предписывает Государствам-участникам установить уголовную ответственность за **создание и распространение расистских и ксенофобских идей** через компьютерную систему (пп. «e»), угрозу совершения через компьютерную систему уголовных преступлений против лица по признаку расы, цвета кожи, гражданской и этнической принадлежности или религии (пп. «f»), **намеренное отрицание, одобрение или оправдание действий, представляющих собой геноцид или преступление против человечности с помощью компьютерной системы** (пп. «h»).

Пункт 1 Статья 30 «Некоторые преступления, связанные с использованием информационных и коммуникационных технологий» предусматривает, что Государства-участники принимают необходимые законодательные и/или нормативные меры для рассмотрения в качестве отягчающих обстоятельств использования информационных и коммуникационных технологий для совершения таких преступлений, как кража, мошенничество, обращение с украденным имуществом, злоупотребление доверием, вымогательство средств, **терроризм** и отмывание денег.

Лига Арабских Государства

Статья 15 Конвенции Лиги арабских государств о противодействии преступлениям, совершенным с использованием информационных технологий 2010 г. квалифицирует в качестве преступлений, связанных **с терроризмом и совершаемых с использованием информационных технологий**:

а) распространение и пропаганду идей и принципов террористических групп;

б) финансирование и подготовку террористических операций, а также содействие связям между террористическими организациями;

в) распространение способов изготовления взрывчатых веществ, особенно для использования в террористических операциях;

г) распространение религиозного фанатизма, а также нападки на религии и убеждения.

Кроме того, статья 16 Конвенции также **криминализует незаконный оборот оружия**.

Очевидно, что тематика противодействия использованию ИКТ в террористических и экстремистских целях уже детально проработана на региональном и национальном уровнях. Однако существующая фрагментация в регулировании этих вопросов затрудняет комплексное взаимодействие между государствами для эффективной борьбы со злоумышленниками. Российская Федерация вновь призывает к закреплению в тексте разрабатываемой универсальной конвенции положений о противодействии терроризму и экстремизму. Это будет отвечать интересам международного сообщества и способствовать эффективному международному сотрудничеству по борьбе с преступностью.

В резолюции ГА ООН 74/247 отмечается, что Спецкомитету необходимо «в полной мере учитывать существующие международные документы и предпринимаемые на национальном, региональном и международном уровнях усилия по борьбе с использованием ИКТ в преступных целях».