Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

Финансирование экстремистской деятельности с использованием сети Интернет: угроза финансовой безопасности Российской Федерации

Научный руководитель – Каменева Анна Николаевна

Колоколова Марина Владиславовна
Студент (бакалавр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия
E-mail: kolokolova.marin@gmail.com

В современном мире главным и самым опасным источником угрозы национальной безопасности государства считается деятельность экстремистских организаций. «Опасность» их деятельности обуславливается, прежде всего, антиконституционным характером совершаемых ими деяний, а также масштабом последствий и распространенностью «вовлечения» в экстремистские сообщества граждан. Концентрация экстремистских организаций и их деятельности напрямую зависит от уровня их финансирования и материально-технической оснащенности. В связи с этим, перекрытие каналов финансирования экстремистских организаций и заморозка активов - одно из условий эффективной борьбы с экстремизмом.

К основным причинам, по которым финансирование экстремистских организаций успешно развивается можно отнести: отсутствие эффективного государственного контроля за финансовым и экономическим секторами в силу существующих пробелов в законодательстве; незначительный объем практики расследования уголовных дел о финансировании экстремистской деятельности; нестабильность в обществе, как политическая, так и экономическая; коррупция.

Экстремистские организации получают финансирование из широкого круга абсолютно разнообразных источников. Новые организации ищут «легко маскирующиеся» источники финансирования для того, чтобы органам государственной власти было невозможно отследить источник поступлений доходов на счета организации.

В современном мире интернет выполняет одну из самых важных функций - служит универсальным средством общения, позволяющим мгновенно обмениваться информацией с множеством лиц, находящихся в различных «уголках планеты». Однако возможности интернета также позволяют использовать его в целях ведения противоправной деятельности. Действительно, в течение последних десяти лет экстремистские организации активно ведут свою деятельность в киберпространстве, где, на сегодняшний день, насчитывается до десяти тысяч экстремистских электронных площадок, более 5% из которых являются русскоязычными. [1]

Стоит обратить внимание на такой канал финансирования экстремистской деятельности как использование социальных сетей для сбора средств. Совершенно ясно, что «жертвователи» зачастую находятся в неведении истинных целей сбора средств. [2] Помимо социальных сетей, экстремистскими организациями также используются как обычные чаты по привлечению жертвователей, такие как WhatsApp, Facebook, Viber, Twitter, так и «даркнет» - защищенная сеть связи, способствующая скрыть преступный умысел.

Как показывает практический опыт правоохранительной деятельности и финансовой разведки, высокая степень риска использования социальных сетей и сети Интернет в целях финансирования экстремисткой деятельности обусловлена статистическими данными обнаружения данных фактов при расследовании смежных преступлений.

При этом, социальные сети и сеть Интернет привлекают экстремистские группировки возможностью удаленного доступа - вовлечение в финансирование людей со всего мира, а также управления процессами из любой точки доступа, что затрудняет работу следственных органов по привлечению к ответственности и идентификации самой экстремистской организации, организовавшую сбор средств на осуществление своей деятельности.

Несмотря на высокий уровень угрозы и при этом сложность раскрытия сбора средств через Интернет для целей финансирования экстремистской деятельности, предлагается ряд мер, которые могут снизить данные риски. [4]

Во-первых, исключение использования неидентифицированных, обезличенных платежей с использованием электронных средств, онлайн переводов и безналичных денежных средств.

Во-вторых, создание механизма (судебного и внесудебного) блокирования страниц (личных, групповых) и всех собранных средств в социальных сетях и сети Интернет, публикующих (организующих) частые сомнительные сборы средств без дальнейшего отчета об их использовании.

На сегодняшний день, согласно разъяснениям Верховного Суда РФ, в случае выявления банком подозрительной операции (*прим.:* перевода денежных средств), последний имеет право заблокировать банковскую карту и отказаться проведении операций по счету. Также банки обязаны осуществлять постоянный внутренний контроль за сделками клиентов, вне зависимости от их суммы, с целью выявления клиентов, чьи операции и деятельность может быть связана с финансированием или осуществлением экстремистской деятельности. [3]

Исходя из вышесказанного, можно сделать вывод о том, что наиболее актуальным из применяемых способов привлечения средств для финансирования экстремистской деятельности является осуществления такой деятельности в сети Интернет. На современном этапе у правоохранительных структур и финансовой разведки имеются разработанные меры, направленные на минимизацию рисков финансирования экстремистской деятельности с использованием информационных технологий. Применение данных мер также позволит снизить уязвимость финансовой и экономической безопасности Российской Федерации от внешнего воздействия, оказываемого экстремистскими организациями.

Источники и литература

1) Жаворонкова Т.В. Использование сети интернет террористическими и экстремистскими организациями // ВЕСТНИК Оренбургского государственного университета. 2015. №3 (178). С.78-93

2) Мелкумян К.С. Финансирование терроризма: тренды XXI в. с сирийским акцентом // Вопросы безопасности. 2018. №3

3) Определение Судебной коллегии по гражданским делам ВС РФ от 24 октября 2017 года №11-КГ17-23

4) FATF (2019), Terrorist-Financing-Risk-Assessment-Guidance, FATF, Paris, France – июль 2019 - https://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-Risk-Assessment-Guidance.pdf