ИНТЕРНЕТ КАК СРЕДСТВО СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТКОЙ НАПРАВЛЕННОСТИ

Бетев Борис Тимурович

магистрант, Казанский (Приволжский) федеральный университет, РФ, г. Казань

Никитин Антон Евгеньевич

магистрант, Казанский (Приволжский) федеральный университет, РФ, г. Казань

Сундуров Федор Романович

научный руководитель, профессор, Казанский (Приволжский) федеральный университет, РФ, г. Казань

THE INTERNET AS A MEANS OF COMMITTING EXTREMIST CRIMES

Boris Betev

Master's student, Kazan (Volga region) Federal University, Russia, Kazan

Anton Nikitin

Master's student, Kazan (Volga region) Federal University, Russia, Kazan

Fedor Sundurov

Scientific adviser, Professor, Kazan (Volga region) Federal University, Russia, Kazan

Аннотация. Важно отметить, что преступления экстремистской направленности, совершаемые через Интернет, могут включать в себя различные действия, такие как распространение экстремистской пропаганды, призывы к насилию, угрозы, оскорбления и дискриминация на основе расы, религии, пола и т.д. Расследование таких преступлений требует сотрудничества различных органов правопорядка и специалистов в области кибербезопасности. Как правило, первоначальным шагом является фиксация и сохранение всех доступных важных данных, таких как IP-адреса, метаданные, содержимое сообщений и т.д. Это может быть осуществлено с помощью специальных программных средств, которые позволяют провести копирование и изъятие данных с носителей информации или сетей.

Abstract. It is important to note that extremist crimes committed via the Internet can include a variety of actions, such as the dissemination of extremist propaganda, calls for violence, threats, insults and discrimination based on race, religion, gender, etc. Investigating such crimes requires the cooperation of various law enforcement agencies and cybersecurity experts. Typically, the initial step is to capture and store all available important data such as IP addresses, metadata, message contents, etc. This can be done using special software that allows copying and retrieving data from storage media or networks.

Ключевые слова: Экстремистская деятельность, осмотр, сеть Интернет, способ, сокрытие информации.

Keywords: Extremist activity, inspection, Internet, method, concealment of information.

Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» не содержит понятия преступлений рассматриваемой категории [2]. В соответствии со ст. 1 данного документа экстремистской деятельностью (экстремизмом) является деятельность общественных и религиозных объединений, либо иных организаций, либо средств массовой информации, либо физических лиц по подготовке и совершению действий, направленных на насильственное изменение основ конституционного строя и нарушение целостности России, подрыв безопасности страны, захват или присвоение властных полномочий, создание незаконных вооруженных формирований и т. д. В соответствии с примечанием 2 к ст. 280 УК РФ под преступлениями экстремистской направленности понимаются преступления, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы, предусмотренные соответствующими статьями Особенной части УК РФ [1].

Однако, следует отметить, что данные ресурсы активно борются с размещением экстремистского контента и применяют меры для его удаления. ВКонтакте, например, имеет свою антиэкстремистскую службу, которая мониторит и блокирует подобный контент. Тем не менее, в связи с объемом информации, поступающей на эти платформы, задача полной фильтрации всех случаев экстремизма остается сложной. При этом важно заметить, что размещение экстремистского контента является нарушением закона во многих странах, включая Россию. Ведение экстремистской пропаганды и распространение экстремистской информации может привести к уголовной ответственности.

Кроме того, преступники могут использовать специальные программы и скрипты, которые автоматически размещают информацию на различных платформах и форумах. Это позволяет им быстро достичь большой аудитории и увеличить вероятность того, что их сообщение будет замечено и принято к исполнению. Преступники также могут использовать различные техники манипулирования, чтобы убедить людей выполнить определенные действия. Например, они могут создать поддельные аккаунты или сайты, которые выглядят аутентично, чтобы убедить пользователей предоставить личную информацию или выполнить определенные действия.

Преступники часто используют техники социальной инженерии, чтобы обмануть людей и получить доступ к их информации или системам. Они могут представляться важными или доверенными лицами, чтобы убедить жертву предоставить доступ или отправить деньги. Для борьбы с такими способами размещения данных применяются различные меры безопасности. К ним относятся обучение людей основам кибербезопасности, использование антивирусных программ и фаерволов, регулярное обновление программного обеспечения, осторожность при открытии подозрительных ссылок и вложений, использование сложных паролей, многофакторной аутентификации и шифрования данных.

Возможность общаться в зашифрованном виде также усложняет работу правоохранительных органов, потому что они не могут просто перехватывать и прочитывать сообщения для получения информации о планируемых преступлениях. Это требует отслеживания и дешифрования сообщений, что может быть сложным и требовать специальных технологических возможностей и навыков. Однако, такие компании, как Telegram, активно сотрудничают с правоохранительными органами, предоставляя необходимую информацию и содействуя в расследованиях экстремистских действий [4].

Длительность процесса получения информации с защищенных сайтов и их блокировки является одной из основных проблем для следственных органов. Защищенные сайты

обеспечивают анонимность и шифрование данных, что затрудняет доступ к ним для правоохранительных органов. В таких случаях необходимо проводить сложные технические операции, чтобы проникнуть в защищенные системы и получить информацию, что требует дополнительного времени и ресурсов.

Местом совершения таких преступлений может служить любое место с доступом к сети Интернет. Преступники могут находиться в любой точке мира и использовать анонимные сети или виртуальные частные сети для скрытия своей личности и местоположения. Это делает обнаружение и пресечение таких преступлений более сложными задачами для правоохранительных органов.

Особое внимание следователю необходимо уделять взаимодействию с оперативными подразделениями органов внутренних дел, так как некоторые аспекты совершенного преступления невозможно установить без их помощи [3, с. 393].

Таким образом, развитие технологий и новые методы шифрования требуют постоянного обновления навыков и компетенций правоохранительных органов. Это может включать в себя повышение квалификации сотрудников, сотрудничество с компаниями-разработчиками и внедрение новых технологических инструментов для эффективной борьбы с преступлениями экстремистского характера в современной информационно-коммуникационной среде.

Список литературы:

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 04.08.2023) // Собрание законодательства РФ. – 1996. - №25. – Ст.2954.

2. Федеральный закон от 25.07.2002 №114-ФЗ (ред. от 28.12.2022) «О противодействии экстремистской деятельности» // Собрание законодательства РФ. – 2002. - №30. - Ст. 3031

3. Герасименко Н. И. Особенности использования сети Интернет в расследовании преступлений экстремистской направленности // Пенитенциарная наука. – 2020. – Т. 14. – №. 3. – С. 388-393.

4. Telegram согласился передавать спецслужбам данные пользователей [Электронный режим]. – Режим доступа: https://www.rbc.ru/technology_and_media/28/08/2018/5b8527749a7947318f857b0f (дата обращения: 13.11.2023)