Секция «Криминалистика»

К вопросу о необходимости формирования групповой методики расследования преступлений, совершенных с использованием высоких информационных технологий

Романов Роман Владимирович

Студент (магистр)

Санкт-Петербургский государственный университет, Юридический факультет, Кафедра уголовного процесса и криминалистики, Санкт-Петербург, Россия

E-mail: rrv93@bk.ru

Современное общество позиционирует себя как информационное, что связано в том числе с использованием высоких информационных технологий во многих сферах жизнедеятельности. Научно-технический прогресс не стоит на месте и привносит в нашу жизнь различные позитивные моменты. Между тем, высокие информационные технологии находятся под пристальным вниманием преступников, для которых подобные технологии служат способом совершения их преступных посягательств. Наиболее важной информационной системой является международная сеть Интернет. О масштабах ее использования можно судить по статистическим данным, согласно которым на 2015 год 103 млн из 146 млн жителей России относятся к категории интернет-пользователей [8]. Ежегодно в сети Интернет совершается большое число преступлений, начиная от кибер-мошенничества, заканчивая получением личных данных пользователей социальных сетей. Многие из данных преступлений даже не выявляются.

Интерес злоумышленников наблюдается и к другим технологиям, позволяющим осуществить неправомерный доступ к локальным информационным системам государственных органов и коммерческих организаций с целью сбора информации, относящейся к категории государственной или коммерческой тайны. Следует отметить и то обстоятельство, что современный уровень высоких информационных технологий позволяет совершать преступления, связанные с уничтожением (повреждением) объектов военной и гражданской инфраструктуры, возникновением сбоев в работе государственных органов и оборонных предприятий и т. д. Речь идет о совершении террористических актов и диверсий с использованием высоких информационных технологий. Подобная возможность является актуальной в связи с возросшей напряженностью в международных отношениях и деятельностью террористических организаций. Таким образом, ущерб от этих преступлений может исчисляться миллиардами рублей, что подтверждает их большую общественную опасность [9].

Зачастую в период предварительной проверки и на начальном этапе расследования данных преступлений следователь не обладает объемом сведений, указывающему на конкретный состав преступления и позволяющему применять частную методику расследования. Кроме того, необходимые частные методики не всегда существуют. Соответственно, ему необходима некая типовая программа, которая бы учитывала широкий круг преступлений, выделенных на основе общих криминалистически значимых признаков, предоставляя следователю данные, необходимые для понимания им сути произошедшего события. Приведенные обстоятельства позволяют нам поставить вопрос о необходимости формирования групповой методики расследования преступлений, совершенных с использованием высоких информационных технологий.

Групповые методики - это система научных положений и разработанных на их основе рекомендаций по расследованию преступлений, охватываемых общими криминалистическими признаками, присущих целому классу (роду) преступлений [2, 6]. В качестве криминалистически значимых признаков, в нашем случае, выступают механизм следооб-

разования и способ совершения преступления.

Преступления, совершаемые с использованием высоких информационных технологий обладают рядом общих признаков, диктующих необходимость выделения их в отдельный род преступлений. К числу таковых следует отнести осуществление противоправной деятельности в виртуальной среде; такая деятельность носит транснациональный характер; деятельность осуществляется путем совершения действий, направленных на получение неправомерного доступа к информации, нарушение системы защиты информации и других форм противоправного вмешательства в информационные системы (технологии); операции производятся в отношении информации, внешнее распознавание и визуализация которой возможны только при условии использования специальной аппаратуры; в процессе совершения преступлений используются программное обеспечение и средства вычислительной техники, позволяющие осуществить незаконные операции с электронной информацией; преступники обладают специальными знаниями и навыками в данной сфере, а также имеют непосредственный доступ к интересующей информации или средства вычислительной техники и программное обеспечение, позволяющие получить его; мотивы преступников определяются целями осуществления операций с информацией [3].

Как уже отмечалось, криминалистически важным признаком является механизм следообразования. Ранее в криминалистике ученые выделяли два вида следов: материальные и идеальные [7]. Однако на сегодняшний день можно констатировать наличие третьего вида - виртуальные [1, 4]. Они существуют только в виртуальной среде, которая определяет следообразующие и следовоспринимающие факторы.

Надо отметить важность указания в групповой методике вопросов, связанных с взаимодействием правоохранительных органов на международном уровне. Часто киберпреступники оставляют следы противоправной деятельности в различных государствах (например, действуя в составе международной организованной группы). Следовательно, возникает потребность в обмене информацией (полученной в ходе цифрового розыска [5]), исполнении запросов о проведении оперативно-розыскных мероприятий, реализации совместных оперативно-розыскных и следственных мероприятий.

Полагаем, что данная групповая методика расследования может включать в себя криминалистическую характеристику; обстоятельства, подлежащие установлению; механизм следообразования и места возможного обнаружения доказательств; способы обнаружения и фиксации виртуальных следов и изъятия объектов, содержащих данные следы; типичные следственные ситуации; типичные общие и частные версии; планирование расследования; способы проверки выдвинутых версий; тактические особенности следственных действий и иных предусмотренных законом мер; использование специальных знаний; способы противодействия следствию; взаимодействие правоохранительных органов на международном уровне; особенности предупреждения данного рода преступлений.

Источники и литература

1) Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе. М., 2012.

2) Гармаев Ю. П., А. Ф. Лубин. Проблемы создания криминалистических методик расследования преступлений : Теория и практика. СПб., 2006.

3) Кушниренко С. П. Значение разработки групповых методик расследования в криминалистике // Криминалистика и судебная экспертиза: Наука, обучение, практика. Вильнюс, 2009. С. 84-93.

4) Мещеряков В. А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. 2013. № 5. С. 265-270.

5) Овчинский А. С. Правоохранительные инфотехнологии. М., 2009.

6) Шмонин А. В. Методология криминалистической методики. М., 2010.

7) Яблоков Н.П. Криминалистика: учебник для вузов. М., 2014.

8) Internet World Stats: http://www.internetworldstats.com

9) Norton: http://www.us.norton.com