

ОСОБЕННОСТИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ МЕТОДИКИ РАССЛЕДОВАНИЯ МЕЖДУНАРОДНЫХ КИБЕРПРЕСТУПЛЕНИЙ

Научный руководитель – Зайнуллин Руслан Ильдарович

Гареева Екатерина Радиковна

Студент (бакалавр)

Башкирский государственный университет, Институт права, Кафедра криминалистики,
Уфа, Россия

E-mail: hatikusan893@icloud.com

Одной из основных специфических черт киберпреступности является её интернациональность. Совершение преступления в интернет-пространстве не ограничивается местонахождением преступника, что существенно затрудняет расследование подобных преступлений. Нахождение преступника никак не влияет на объект кибератаки: свободный выход допускает совершение преступного деяния из любой точки выхода в Интернет. В данном случае исключение могут составлять только те страны, которые устанавливают занавес внешней сети (Китай, Сирия, Иран, Куба и т.д.) [/rus/event/request/70530/report/edit#_ftn1](#).

Одной из основных проблем при расследовании интернациональных киберпреступлений можно считать разрешение вопроса о том, кем будет расследоваться данное дело. Если изначально, заявление от потерпевшего лица будет принято по месту причинения вреда, то в случае, если речь идет о ряде кибератак, а также совершению преступления группой лиц, когда соучастники преступления находятся в различных странах. Расследование преступлений в таком случае существенно осложняется не только дальностью, но и различными правовыми системами, предусматривающие разные институты осуществления уголовного судопроизводства. Собираание следов и накопление доказательной базы существенно осложняется предусмотренными в различных странах различных по своей сущности и форме следственных действиях и оперативно-розыскных мероприятиях.

При расследовании интернациональной киберпреступности наиболее важное значение занимает сотрудничество с такими международными организациями как Интерпол, Европол. Однако, на сегодняшний день такое сотрудничество чаще всего считают наиболее медленным, в связи с чем неэффективным. Таким образом, ответы на запросы на получение информации либо проведение тех или иных следственных действий в другой стране, следственные органы могут ожидать на протяжении нескольких недель, а то и месяцев, что негативно отражается при производстве расследования.

Подводя итог, следует сказать, что на наш взгляд наиболее эффективным выходом из данной ситуации было бы создание единого правового поля в области расследования киберпреступлений. Гармонизация либо даже унификация процессуальных норм в данном вопросе, на наш взгляд, путем создания единого договора (конвенции) о методике расследования киберпреступлений на межнациональном уровне, с одной стороны существенно бы упростила проведение такого расследования. Следует помнить, что киберпреступность обладает рядом специфических признаков, что существенно отличает её от обычных преступлений, а значит и расследование по данным делам, производство следственных действий и оперативно-розыскных мероприятий должно быть иным: выполняться частично в Интернет-пространстве.

Вторым этапом в данном случае, на наш взгляд, было бы эффективным создание отдельной организации на межнациональном уровне, специализирующейся на расследовании интернациональной киберпреступности. В частности, это объединило бы специалистов в области компьютерной информации, задачей которых стояло бы непосредственно определение механизма совершения кибератак, а также местонахождение преступника. Несмотря на то, что с одной стороны, организация была бы достаточно серьезно загружена, качество работы на наш взгляд можно было бы считать более эффективным, так как подобные специалисты, служащие в современных ЭКЦ МВД России занимаются совершенно разными задачами при выполнении компьютерных экспертиз. Специализация непосредственно на двух названных выше задачах существенно увеличило бы качество работы.

Функционирование такой организации предполагает сотрудничество на национальном уровне: осуществление следственных действий, не терпящих отлагательств, как то обыск, выемка, задержание и др. Однако в виду специфики, необходимости использования специальных (компьютерных) знаний при расследовании киберпреступлений, осуществление ключевых следственных действий: допрос, производство экспертиз, опознание и т.д. должно проводиться в рамках подобной организации.

Как было сказано выше, кибератаки не привязаны к местонахождению, правовой системе или определенному государству, в связи с чем расследование подобной категории уголовных дел также будет более эффективным в отсутствие подобных рамок и границ. Противодействие преступлениям в Интернет-пространстве должно быть более эффективным, чем осуществление традиционного расследования, однако возможность такого противодействия появится лишь в случае привлечения специалистов такого же уровня в сфере компьютерных технологий, что и сами киберпреступники.

[/rus/event/request/70530/report/edit#_ftnref1](#) Линников А.С. Экономические последствия расширения масштабов киберпреступности в России и мире // Банковское право. 2017. № 5. С. 19 - 29.

Источники и литература

- 1) Чекунов И.Г., Шумов Р.Н. Современное состояние киберпреступности в Российской Федерации // Российский следователь. 2016. № 10. С. 44 - 47
- 2) Шайхаттарова С.В. Россия и международные стандарты по борьбе с киберпреступностью // Международное уголовное право и международная юстиция. 2016. № 4. С. 26 - 29.
- 3) Линников А.С. Экономические последствия расширения масштабов киберпреступности в России и мире // Банковское право. 2017. № 5. С. 19 - 29.