Секция «Цифровая Криминалистика»

"Кибервымогательство" как новый этап в развитии преступности: криминалистический аспект

Научный руководитель – Абдулаев Абдула Арсланалиевич

Кимпаев Камал Мурадович
Студент (специалист)
Российская правовая академия МЮ РФ, Северо-Кавказский филиал, Юридический факультет, Кафедра теории государства и права, Махачкала, Россия
E-mail: kimpaev.kamal@gmail.com

Компьютерные технологии, которые бесспорно принесли огромную пользу для всего человечества, в тоже время создали предпосылки для новых появлений криминальной активности. Так, согласно официальной статистике МВД России количество совершенных компьютерных преступлений в 2017 году составило свыше 95 тыс. По оценкам российских и иностранных специалистов ежесекундно в мире от действий криберпреступников страдают порядка двадцати человек. Но это всего лишь верхушка айсберга, так как ежедневно количество преступлений в кибер сфере стремительно растет, а вместе с ним и растет уровень латентности, составляющий на сегодняшний день 90%. Приведенные статистические данные, характеризующие состояние борьбы с кибер преступностью в целом и кибер вымогательства в частности, показывают, насколько злободневной является задача по повышению эффективности борьбы с рассматриваемой категории преступлений. Сама по себе компьютерная преступность это широкий термин, который обозначает достаточно разные правонарушения. С одной стороны, это преступления, направленные против информационных систем, то есть действия хакеров. С другой стороны, киберпреступлением считается такое правонарушения, в котором вычислительная техника присутствует как средство достижения преступных целей. Таким образом, под киберпреступлениями понимается очень много деяний , начиная от банального взлома компьютера, и заканчивая мошенничеством.

Среди подобного рода преступлений особое место занимают - вымогательства совершаемое посредством создания и распространения вредоносных программ, (вирусное вымогательство). Принцип их действия строится на так называемом " троянском коне". Программа как правило скрывается внутри или под видом вложения в электронное письмо, рабочую программу, баннер и другие файлы либо просто загружается с инфицированного сайта. Попав на компьютер, вирус активируется и блокирует нормальную работу операционной системы как в целом, так и отдельных программ шифруя файлы требуя при этом выкуп. Ярким примером таких преступлений является атака вируса -шифровальщика "wannacry" которая стала одной из самых масштабных за всю историю человечества. Wannacry на протяжении нескольких лет атаковала компьютеры с устаревшими версиями windows, блокируя их систему и требуя денежный выкуп в размере 300\.150.1.., , . – . – , , .

Эффективность предварительного расследования по уголовным делам о кибер вымогательстве невозможно без определения факторов, которые способны оказывать заметное негативное влияние на качество процедуры расследования уголовного дела. Во первых, это касается несовершенства норм уголовного права, предусматривающих ответственность за кибер вымогательство. Данная проблема предопределяет неизбежное возникновение у правоприменителей сложностей в грамотной квалификации рассматриваемой разновидности вымогательства. [2]

Во вторых отсутствует в полной мере адекватное сложившиеся криминогенной ситуации криминалистическое обеспечение процедуры расследования этой категории уголовных дел. В третьих степень профессиональной квалификации субъектов расследования не

всегда в полной мере соответствует современным требованиям, что безусловно не может не сказаться на качестве предварительного расследования по уголовным делам о кибервымогателстве. В четвёртых негативное воздействие оказывает недостаточная координация совместных усилий правоохранительных органов с государственными и не государственными структурами, специализирующимися на обеспечение безопасности в сфере телекоммуникации и компьютерной информации.[1]

Еще одной немаловажной проблемой является проведение ОМП и выемка доказательств. Многие сотрудники отмечали, что даже не проводили ОМП. Вы спросите почему? Ответ этому простой, оно отсутствует. Это означает, что распознание места совершения киберпреступления неосуществимо без определения обстановки совершения преступления, которая определяется системой киберпространства. Что же касается экспертизы, то из-за высокой перезагруженности государственных судебно-экспертных учреждений, несвоевременность выполнения экспертиз возросло вдвое. Согласно официальным данным СК РФ, В 58% случаев проведение экспертизы поручали государственно-экспертным учреждениям и лишь в 5% - не государственным.

Это частично обусловлено отсутствием системных обобщений материалов следственной и судебной практики, нехваткой методических рекомендаций по организации расследования данного вида преступлений, небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов, а также недостаточно высоким уровнем подготовки специалистов по соответствующей специализации в высших учебных заведениях. Около 86% респондентов считают необходимой разработку криминалистических рекомендаций по выявлению и расследованию киберпреступлений.

Как показали исследование научной литературы и опрос следователей (дознавателей), для решения приведенных проблем и повышения эффективности расследования киберпреступлений необходимо:

- повысить уровень мониторинга данного вида преступлений;
- разработать программы повышения квалификации следователей (дознавателей) по расследованию данной категории дел;
- увеличить объем научно-методической литературы, посвященной прикладным аспектам расследования киберпреступлений.

С технической стороны существует несколько основных способов защиты от преступного посягательства:

- Использование систем фильтрации электронной почты;
- Использование систем контентной фильтрации веб-трафика;
- Обеспечение контроля доступа к корпоративной сети.

Источники и литература

1) Гладких В.И. Компьютерное мошенничество: а были ли основания для криминализации? // Рос. следователь. – 2014. – № 22. – С. 25–31.

2) VIII Всероссийская научная конференция, Санкт-Петербург, 22 апреля 2017 года : материалы / под ред. А. А. Сапожкова. Ч. 2.

3) Корноухов В. Е. Методика расследования преступлений: теоретические основы. М., 2008. С. 340. Тищенко В. В. О современных направлениях развития криминалистической методики расследования преступлений. С. 247.