Секция «Криминалистика»

Проблемы проведений следственных действий при расследовании «киберпреступлений»

Научный руководитель – Таркинский Абумуслим Исрапилович

Кимпаев К.М.[1]*, Алиев М.М.*[2]

1 - Российская правовая академия МЮ РФ, Северо-Кавказский филиал, Юридический факультет, Кафедра теории государства и права, Махачкала, Россия; 2 - Северо-западный филиал Российской правовой академии Министерства юстиции Российской Федерации, Юридический факультет, Санкт-Петербург, Россия

В современном мире мы являемся свидетелями того, что одной из самых актуальных проблем, как в России, так и во всем мире, является проблема "киберпреступности" охватившая сегодня практически все сферы человеческой жизни. Так, согласно официальной статистике МВД России количество совершенных компьютерных преступлений за 2015-2016 годы составила 47,5 %(13.000 23.000) из которых порядка 9,5 процентов приходится на Республику Дагестан.[1] Но это всего лишь верхушка айсберга, так как ежедневно количество преступлений в кибер сфере в РФ быстро растет, а вместе с ним и растет уровень латентности, составляющий на сегодняшний день 90% процентов.

Процесс компьютеризации в России, по нашему мнению, застал врасплох правоохранительные органы, оказавшиеся неподготовленными к полноценному противодействию и активной борьбе с этим новым противоправным явлением как "киберпреступность". Так по оценкам Российских и иностранных ученых, проблема расследования и раскрытия подобных преступлений представляет собой проблему на много труднее, чем, к примеру, задачи по их предупреждению. Именно поэтому уровень латентности кибер преступлений в большей степени, зависящий и от указанных обстоятельств, определяется таким высоким процентом, а из остальных 10% выявленных киберпреступлений, раскрывается около 1%.

Для многих следователей раскрытие киберпреступлений является весьма сложной задачей, что обусловлено особенностью этого вида преступлений. Ведь по статистике только 5% сотрудников следственных органов помимо юридического образования имеют подготовку по специальности, связанной с компьютерной техники. 64% владеют компьютером на уровне "рядового пользователя", 36% на уровне "продвинутого пользователя". Большинство сотрудников осваивают компьютерные системы самостоятельно, в результате информационная подготовленность сотрудников следственных подразделений оставляет желать лучшего.[2]

Часто, сотрудники следственных отделов в ходе расследования компьютерных преступлений связываются с рядом проблем, среди которых:

- несовершенство существующего уголовного законодательства.

- ошибки, возникающие при производстве следственных действий

-низкий уровень подготовленности следователей для работы со специфическими источниками доказательств, оцифрованной в виде электронных страниц, сообщений, сайтов; Все это, несомненно, только благоприятствует деятельности киберпреступников, открывая перед ними большие возможности. Примером тому, может послужить случай, произошедший в одном из городов России, когда при раскрытии очередного киберпреступления, а именно при попытке изъятия следователями орудия преступления (компьютерного оборудования) оно, будучи в выключенном состоянии, загорелось без всякой причины. Оказалось, что задолго до приезда сотрудников правоохранительных органов, злоумышленник установил в дверном проеме датчик, создающий сильное магнитное поле, уничтожающий

компьютерную систему при любой попытке выноса оборудования за пределы комнаты. В результате изощренности киберпреступника, следственные органы остались без доказательств. К сожалению, это не первый случай, когда талант и сноровка киберпреступников берет вверх над всей следственной системой.

Немало известными также являются случаи, когда сложно установить факт совершенного преступления. Это связано в первую очередь с тем, что внешние проявления компьютерного преступления обычно менее явное, чем при ограблении продуктового магазина. Действительно, при совершении компьютерных преступлениях мало когда наносится какой-либо визуально видимый материальный ущерб. К примеру, незаконное копирование сведений с компьютера чаще всего остается не раскрытым, внедрение в компьютер вируса чаще всего похоже на ошибку системного администратора, который не смог его "отловить" при обращении с компьютерным миром.[3]

На практике большинство проблем появляются при проведении ОМП и выемке 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 глобальной системой киберсети. Что же касается экспертизы, то из-за высокой перезагруженности государственных судебно-экспертных учреждений, несвоевременность производства экспертиз возросло вдвое. Согласно официальным данным СК РФ, В 58% случаев проведение экспертизы возлагается на государственно-экспертные учреждения и лишь в 5% - не государственные.

Безусловно, профессиональный следователь, ведущий дела по преступлениям в компьютерной сфере, должен быть и прекрасным программистом или, по крайней мере, разбираться в тонкостях использования и возможностях вычислительной техники. Поэтому, проанализировав нормативно-правовую базу, научно-практическую литературу, и статистику МВД, мы считаем целесообразным предложить следующие пути решения выше указанных проблем:

Во-первых. Разработать комплексную, криминалистическую методику расследования данного вида преступных посягательств.

Во-вторых. Разработать программы по повышению квалификации следователей по расследованию данной категории преступлений.

В-третьих, ввести в учебные заведения, готовящие следователей России специальные дисциплины по "выявлению, расследованию и предупреждению правонарушений совершаемых с помощью ПК"

В - четвёртых. Рассмотреть вопрос о создании базового координационного экспертно-криминалистического центра по выше названному кругу проблем.

Источники и литература

1) Голубев В. Некоторые вопросы расследования компьютерных преступлений. – Выступление 26 февраля 2003 года. Атланта США.

2) Голубев В.А. Информационная безопасность: Проблемы борьбы с киберпреступлениями. – ГУ «ЗИГМУ» 2003.

3) Козлов В. «ComputerCrime» Что стоит за названием? (Криминалистический аспект). – http://www.crime-research.org