Колина Юлия Валерьевна
Магистрант НАЧОУ ВПО СГА

Направление: Юриспруденция
Магистерская программа: Уголовный процесс, криминалистика и судебная экспертиза, теория оперативно-розыскной деятельности

© Бюллетень магистранта 2014 год № 1

Актуальные проблемы расследования компьютерных преступлений

Аннотация: В статье рассматриваются основные проблемы, возникающие при расследовании компьютерных преступлений, а также вопросы повышения эффективности их расследования, на основе проведенного автором анализа теоретических и практических материалов, выводов, полученных в результате изучения судебной практики данного вида преступления за последние годы в России.

Ключевые слова: компьютерные преступления, расследование, эффективность, следственное действие, оперативно-техническое мероприятие, следователь.

В современном мире противодействие компьютерным преступлениям является одной из главных задач правоохранительных органов. Изучение материалов по данной теме позволяет нам говорить о том, что в этой сфере перед мировым сообществом возникли серьезные проблемы. Так в развитых странах совершаются сотни тысяч компьютерных правонарушений, приносящих миллиардные ущербы.

Компьютерные преступления являются достаточно сложным и проблемным видом преступлений. Одной из первых проблем, с которой можно столкнуться при расследовании таких преступлений, – это установление самого факта совершения преступления. Данная проблема может возникнуть в связи с

тем, что зачастую ущерб не виден, например, незаконное копирование информации с использованием вируса.

Другой серьезной проблемой, затрудняющей расследование, является то, что социум зачастую не рассматривает компьютерные преступления по сравнению с традиционными, как серьезную угрозу. «Обыватель обычно воспринимает компьютерного пирата как умную и интересную личность, а жертву как жадную и глупую. Поэтому общественность редко льет слезы по поводу ущерба организаций, пострадавших от компьютерных преступлений, а сами они не спешат выставлять себя на посмешище» [3].

Недостаток в квалификации кадров, расследующих преступление, также является проблемой при расследовании такого вида преступлений. Для раскрытия киберпреступлений следователь должен быть хорошим программистом или разбираться в тонкостях вычислительной техники, отмечает А. Белоусов. Однако в правоохранительных органах таких сотрудников очень мало [1].

Часто возникает проблема в проведении некоторых следственных действий, так как не достаточно компетентный следователь в данном вопросе может сам и уничтожить улики преступления при сборе доказательств с компьютера.

По мнению А. Белоусова, раскрытие компьютерных преступлений затрудняется и тем, «что безошибочных программ не бывает и на ошибки компьютера очень удобно списать попытки преступления» [1].

Также следственные действия затрудняет и то, что зачастую при эксплуатации вычислительной техники происходит совмещение профессий. Часто встречается, что сам бухгалтер является и программистом, и оператором, в результате чего взаимные проверки исключаются, возможность злоупотреблений возрастает, а следственные действия затрудняются.

Отметим еще и то, что компьютерные преступления, это преступления, требующие больших финансовых вложений и аппаратного обеспечения,

© Бюллетень магистранта 2014 год № 1

поэтому иногда бывает, что «организации не желают увеличивать свои потери добавлением к ущербу расходов на расследование. Зная свои ограниченные материальные ресурсы, жертвы отказываются от идеи раскрыть преступление» [1].

Все вышеперечисленные проблемы усложняются несовершенством законодательства и государственной системы борьбы с компьютерными преступлениями.

Рассматриваемая тема актуальна тем, что в современных условиях социально-экономического развития Российской Федерации и с появлением нового вида общественных отношений и общественных ресурсов (информационного), стало совершаться большое количество компьютерных преступлений, представляющих реальную угрозу процессу становления российской государственности и успешному проведению социально-экономических реформ.

Немаловажным является и тот факт, что сегодня весь мир с развитием технологических, экономических и политических процессов ведет борьбу за информацию (информационные войны). Таким образом, возникает угроза национальной безопасности страны, ее информационно-вычислительных систем. Похитителем информации здесь могут быть как другие государства, отстаивающие свои геополитические интересы, так и преступные организации, преследующие экономические и политические цели, обычно связанные с борьбой за сферы влияния.

Также на современном этапе развития общества происходит процесс слияния организованной преступности и лиц, совершающих компьютерные и экономические преступления, что угрожает безопасности крупнейших корпораций.

Противодействие таким видам преступления требует более совершенных научных методов и технических средств раскрытия и расследования, проведения специальных оперативных мероприятий. Поэтому для эффективной

© Бюллетень магистранта 2014 год № 1

борьбы с преступлениями, совершенными в условиях научно-технического прогресса, и их расследования правоохранительные органы должны применять средства и методы, обладающие не меньшей эффективностью, чем у преступных лиц.

В этих целях также предлагается усовершенствовать механизмы взаимодействия правоохранительных органов с органами государственной и исполнительной власти. Создать единую базу данных с полной и достоверной информацией, избегая дублирования уже имеющейся информации. Развить единый документооборот между ведомствами и органами в отношении данного вида преступлений.

Необходимо также развивать знания и повышать квалификацию специалистов в области информационного права, подготовке грамотных специалистов-программистов. Поэтому следует организовать постоянное обучение специалистов связанных с расследованием преступлений, совершаемых с использованием высоких информационных технологий. Специалисту могут потребоваться знания в таких областях как: операционные системы, их функциональные возможности и области применения в юриспруденции; роль математических методов и вычислительной техники в различных видах юридической деятельности и в функционировании правовых систем различных регионов; современные информационные технологии; аппаратные и программные средства ПК; локальные и глобальные вычислительные сети и др.

Следует к тому же регулярно производить оснащение подразделений правоохранительных органов новой техникой, используемой в работе специалистов, немаловажно разработать методики по проведению компьютерных экспертиз.

Рекомендуется тщательное изучение документации по топологии (территориальному устройству) компьютерной сети с привлечением широкого

© Бюллетень магистранта 2014 год № 1

круга специалистов и проведение опроса администраторов сети для выяснения всей схемы устройства сети и особенностей коммуникаций.

Вслед за А.Ж. Кабановой, мы предлагаем добавить в УК РФ новую статью, предусматривающую ответственность в ч. 1 за изготовление или сбыт технических устройств, предназначенных для несанкционированного доступа к охраняемой законом компьютерной информации. В ч. 2 – за то же деяние, совершенное группой лиц по предварительному сговору или неоднократно. Ответственность за деяние, предусмотренное частями первой или второй, совершенное организованной группой внести в ч. 3 предлагаемой статьи УК РФ [4, с. 19].

Рассматривая практику применения норм об уголовной ответственности за совершение компьютерных преступлений можно сделать вывод о ее неоднородности и несформированности. Нет единства во мнениях относительно квалификации действий преступников и назначении сроков наказания. Однако на сегодняшний день увеличение раскрываемости компьютерных преступлений способствует развитию и формированию единого мнения в использовании норм законодательства относительного данного вида преступлений.

© Бюллетень магистранта 2014 год № 1

Литература

1. Белоусов А. Некоторые аспекты расследования компьютерных преступлений [Электронный ресурс] // Режим доступа: http://pycode.ru/2011/07/rassledovanie-kompyuternyh-prestuplenii/

2. Голубев В.А. Информационная безопасность: проблемы борьбы с киберпреступлениями. Запорожье: ГУ «ЗИГМУ», 2013.

3. Голубев В. Криминалистическая характеристика субъектов преступной деятельности в сфере использования компьютерных технологий [Электронный ресурс] // Режим доступа: http://www.crime-research.org/library/Golubev0104.html

4. Кабанова А.Ж. Преступления в сфере компьютерной информации (уголовно-правовые и криминологические аспекты): Автореф. дис. … канд. юрид. наук. Ростов-н/Д., 2004.

5. Козлов В. «Computer Crime» Что стоит за названием? (криминалистический аспект) [Электронный ресурс] // Режим доступа: http://www.crime-research.org/library/Ccrime.html.

6. Нечаев А.В. Некоторые аспекты защиты информации // Персональный компьютер на службе криминальной милиции и следствия. Возможности и перспективы. М., 2012.

© Бюллетень магистранта 2014 год № 1