Смысл принятых поправок заключается в том, что контент интернет-сайтов должен непременно маркироваться возрастным цензом для защиты детей от вредной для них информации – то есть, 6+, 12+, 16+, 18+, что соответственно старше шести лет, двенадцати и т.д. Также законом вносится положение, что доступ к сети Интернет в «местах доступных для детей» должен быть ограничен [7].

Как мы видим, нормативная база регулирования Интернет-СМИ внушительна. Ранее, до формирования данных законов, в системе регулирования Интернет-СМИ присутствовали серьезные пробелы, к примеру – трудности с блокировкой запрещенных материалов. Однако, как мы видим, законодатели собрали воедино масштабные проблемы в сфере регулирования сетевых СМИ и проложили пути разрешения данных пробелов в нормативно-регулятивную законодательную базу в форме вышеуказанных универсальных законов.

1. Конституция РФ. Принята на всенародном референдуме 12 декабря 1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30 декабря 2008 № 6-ФКЗ, от 30 декабря 2008 № 7-ФКЗ, от 05 февраля 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 7-ФКЗ) // Российская газета. 1993. 25 декабря.
2. Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с посл. изм. и доп. от 03.04.2020 № 105-ФЗ) // Собрании законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448.
3. Федеральный закон от 29 декабря 2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с посл. изм. и доп. от 01.05.2019 № 93-ФЗ).
4. Закон Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» (с посл. изм. и доп. от 01.05.2019 № 93-ФЗ) // Собрании законодательства Российской Федерации от 3 января 2011 г. № 1 ст. 48.
5. Колобаева Н.Е. Особенности реализации права на распространение информации при использовании сети Интернет // Российское право: образование, практика, наука. № 4. 2019. С.4.
6. Колобаева Н.Е. Особенности реализации права на распространение информации при использовании сети Интернет // Российское право: образование, практика, наука. № 4. 2019. С.4.
7. Потгорельская Т.А. Правовое регулирование деятельности Интернет-СМИ // Научно-практический электронный журнал Аллея Науки. №2(29). 2019.

Селезнев А.В.

Киберпреступления – как объект криминалистического исследования

*Тамбовский государственный технический университет
(Россия, Тамбов)*

doi: 10.18411/lj-11-2020-241

idsp: ljjournal-11-2020-241

Аннотация

В статье рассмотрены теоретические подходы к расследованию киберпреступлений в современных условиях развития общества. Выявлены особенности способов совершения такого рода преступлений. Проанализированы основные типы киберпреступников. Рассмотрены особенности следовой картины киберпреступлений.

Ключевые слова: информационные технологии, компьютерная информация, киберпреступления, криминалистическая характеристика преступления.

Abstract

The article discusses theoretical approaches to the investigation of cyber crimes in the modern conditions of the development of society. The features of the ways of committing this kind of crimes are revealed. The main types of cybercriminals are analyzed. The features of the trace pattern of cybercrimes are considered.

Keywords: information technology, computer information, cybercrime, forensic characteristics of a crime.

Современное существование человечества неразрывно связано с повсеместным использованием различных информационных технологий. Практически любой вид жизнедеятельности человека в настоящее время в той или иной мере компьютеризирован. Тенденция к все большей информатизации и автоматизации имеет как положительную, так и отрицательную стороны. К положительной стороне информатизации можно отнести, например, повышение производительности труда работников любого уровня, которые отказываются от рутинных и малоэффективных операций и которые на себя берет компьютер. К отрицательной стороне можно отнести достаточно высокую уязвимость современных рабочих мест, имеющих доступ к локальной или глобальной компьютерной сети, через которые совершается большинство, так называемых компьютерных преступлений или киберпреступлений, порождающих один из важнейших негативных факторов современного общества как киберпреступность.

Киберпреступления представляют собой широкий класс преступлений, который давно уже вышел за рамки действующего российского уголовного законодательства.

Стоит отметить, что наряду с проблемами правового характера, возникающими в процессе квалификации такого рода преступлений существует еще ряд проблем, непосредственно связанных с определением системы типичных признаков, имеющих наибольшее криминалистическое значение для раскрытия и расследования киберпреступлений, и обуславливающих применение соответствующих криминалистических методов, приемов и средств.

К числу таких типичных признаков (элементов криминалистической характеристики любого преступления) можно отнести:

- типичную исходную информацию;
- общие признаки предмета преступного посягательства;
- способ совершения преступления;
- характеристику личности преступника;
- особенности следовой картины на месте преступления;
- обстоятельства совершенного преступления (место, время и др.).

Рассмотрим основные элементы криминалистической характеристики киберпреступлений.

Типичная исходная информация поступает, как правило, от жертвы преступления. Таковыми могут быть обычные граждане, учреждения и организации, различные предприятия и т.д. Эта информация должна содержать общую характеристику совершенного противоправного деяния, связанного с незаконным использованием информационного пространства, что поможет следственным органам наиболее точно сориентироваться в расследуемом преступлении. Успех работы следователя в расследовании киберпреступлений во многом зависит от оперативности реагирования на заявления и сообщения об их совершении, своевременного и обоснованного принятия решения о возбуждении уголовного дела. Для того, чтобы следователю получить максимальное количество исходной информации ему необходимо истребовать соответствующие документы, свидетельствующие о противоправности проведения операций в сфере обработки компьютерной информации, а также возможные средства преступления (машинные носители информации, программы для компьютеров и других компьютерных устройств, базы данных, отдельные файлы и др.), проверить подлинность документов, имеющихся в распоряжении дознавателя, получить объяснения от заявителя и т.д.

Под предметом преступного посягательства обычно понимают стоимостную оценку определенной вещи материального мира, воздействие на которую влечет причинение вреда объекту преступного посягательства.

При совершении киберпреступления предметом преступного посягательства непосредственно является какая-либо компьютерная информация, которая имеет чаще всего определенную материальную ценность для ее владельца.

Под компьютерной информацией применительно к процессу доказывания понимаются фактические данные, обработанные средствами системы и (или) передающиеся по телекоммуникационным каналам, доступные для восприятия человеком, на основе которых, в регламентированном законом порядке устанавливаются обстоятельства, имеющие значение по делу. Источниками такой информации могут быть данные на различных электронных носителях (винчестерах, картах систем мобильной идентификации – sim-картах), пластиковых банковских картах, флеш-картах и др.

Способ совершения преступления представляет собой обусловленный (детерминированный) целым рядом субъективных и объективных факторов комплекс действий субъекта (субъектов) по подготовке, совершению и сокрытию преступного деяния.

К основным способам совершения киберпреступлений можно отнести следующие:

- несанкционированный (незаконный) доступ и копирование компьютерной информации;
- незаконный перехват информации;
- воздействие на компьютерные данные, в том числе с помощью программ-вирусов (противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных);
- противоправное использование специальных компьютерных программ, разработанных или адаптированных для совершения преступлений, в частности для получения паролей, кодов доступа к компьютерной системе и др.

Среди широкого спектра различного рода «компьютерных» преступников можно выделить следующие наиболее встречаемые типы:

- «хакер» - «компьютерный взломщик», программист, намеренно обходящий системы компьютерной безопасности. Основной мотивацией этого типа правонарушителей являются: исследовательский интерес, любопытство, стремление доказать свои возможности, честолюбие. Средства защиты компьютерной информации, ее недоступность они воспринимают как вызов своим способностям;
- «инсайдер» («внутренний взломщик») – злоумышленник, не слишком хорошо владеющий знаниями в области информационных технологий, но владеющий доступом в какую-либо информационную систему в силу служебного положения. Основной своей задачей он считает нанесение материальных убытков собственной компании, иногда даже во вред себе.
- «белый воротничок» - по сути тот же инсайдер, но имеющий более чистосердечные планы и обремененный только чувством собственной нужды.

Что касается следовой картины киберпреступлений, то она представляет собой своеобразное сочетание так называемых традиционных (материальных) и виртуальных следов, которые остаются в основном в памяти компьютера. Виртуальные следы обычно состоят из большого количества отдельных информационных элементов, которые могут быть записаны как на одном, так и на нескольких физических носителях цифровой информации, подключенных как к одному, так и нескольким компьютерам, объединенным в вычислительную сеть. Примером таких следов могут служить записи об установке, удалении и изменении различных программ в реестре компьютера, отдельных операциях, связанных с работой компьютера, в журналах администрирования, безопасности, сведения из log-файлов о работе в сети Интернет, локальных сетях и др. Виртуальные следы могут послужить доказательствами незаконного проникновения в память компьютера или другого электронного устройства, а также создания, использования и распространения вредоносных компьютерных программ, совершения или подготовки к совершению преступления отдельным лицом или группой лиц.

Одним из важнейших вопросов, связанных с изучением криминалистической характеристики киберпреступлений, является определение понятия места происшествия, при совершении такого рода правонарушений.

Обычно под местом совершения киберпреступления понимают место физического нахождения злоумышленника в момент совершения им преступных действий, а также место расположения аппаратных и программных средств, используемых им. В тоже время местом происшествия можно также считать персональный компьютер (рабочую станцию) или сервер, являющиеся местом хранения и обработки информации и ставшие предметом преступного посягательства.

Необходимо отметить, что в отличие от таких «классических» видов преступлений, как убийство, изнасилование, грабеж, где преступник и жертва находятся в непосредственной близости и контакте между собой, при совершении киберпреступления они могут находиться на любом расстоянии друг от друга, а во многих случаях в разных странах и на разных концах земного шара.

В заключении хотелось бы сделать вывод о том, что рассмотренные выше элементы криминалистической характеристики киберпреступлений требуют тщательного и комплексного рассмотрения и изучения, как в теоретическом, так в практическом аспектах, что позволит поднять на более высокий уровень качество расследования и раскрытия рассмотренных в данной статье правонарушений.

1. Васильев, А.А. Электронные носители данных как источники получения криминалистически значимой информации: учебное пособие / А. А. Васильев, К. Е. Демин. – М.: МГОУ, 2009. – 200 с.
2. Зверьянская Л.П. Современные проблемы исследования криминалистических особенностей киберпреступлений [электронный ресурс] / Зверьянская Л.П. // Приоритетные научные направления: от теории к практике. - 2015. - Выпуск № 15. – Режим доступа: <http://cyberleninka.ru/article/n/sovremennye-problemy-issledovaniya-kriminalisticheskikh-osobennostey-kiberprestupleniy>.
3. Криминалистика XXI-века. Стратегия и тактика / Отв. ред. Е.П. Ищенко. - М.: Проспект, 2016. – 269 с.
4. Мещеряков В.А. Следы преступлений в сфере высоких технологий / В.А. Мещеряков // Библиотека криминалиста: научный журнал. – 2013. - № 5 (10). – С. 265 - 269.
5. Федотов Н.Н. Форензика - компьютерная криминалистика [электронный ресурс] / Н.Н. Федотов. – Режим доступа: <http://www.bnti.ru/showart.asp?aid=998&lvl=01.02.01>.
6. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... канд. юрид. наук / Е.С. Шевченко. – М., 2016. – 249 с.