Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 10, Is. 4, pp. 145-151, 2016

DOI: 10.13187/vesp.2016.10.145
www.ejournal21.com

Technical Means

UDC 004.056.53

Criminalistic Identification and the Identification Feature in Cybercrimes

Xenia N. Zolotareva [a, *], Ekaterina N. Zolotareva [a]

[a] ITMO University, Russian Federation

Abstract

This article discusses the concept of forensics in computer crime, presented actual problems of computer crimes in terms of the improvement of information and telecommunication technologies and proposed solutions to them. Provides basic identification characteristics of computer crimes in forensic science. The author analyzed the trends, which are based on the primary sign of the perp in the information sphere.

Keywords: computer crimes, forensics, forensic identification, the identification tag.

1. Введение

В настоящее время все более актуальным становится исследование проблем, возникающих в сфере использования, распространения, переработки информации, случаев и ситуаций, в которых информация является элементом криминальной деятельности.

С точки зрения уголовно-правовой охраны, под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства (Об информации...).

В целом преступления в сфере компьютерной информации являются очень сложным уголовно-правовым институтом. При их квалификации необходимо исходить из того, что данные преступления, посягая на основной объект, всегда посягают и на дополнительный объект, поскольку затрагивают блага более конкретного свойства: личные права и неприкосновенность частной сферы, имущественные права и интересы, общественную и государственную безопасность и конституционный строй.

При расследовании преступлений часто возникает необходимость по следам и иным отображениям определить связь человека, предмета или иного объекта с расследуемым событием. Например, по следам рук установить лицо, оставившее эти следы; по следам транспортного средства разыскать автомобиль.

Эти предположения находят подтверждение в практике и показывают, что отдельные положения методики расследования преступлений в сфере компьютерной информации могут быть использованы тогда, когда в ходе расследования устанавливаются

* Corresponding author
E-mail addresses: ksenya2894@rambler.ru (X.N. Zolotareva), katerina2794@rambler.ru (E.N. Zolotareva)

обстоятельства, связанные с исследованием машинных носителей и компьютерной информации.

Поэтому особое внимание в данной статье уделено вопросу криминалистической идентификации и идентификационным признакам в компьютерных преступлениях.

Криминалистическая идентификация один из основных методов установления истины в уголовном судопроизводстве, когда возникает необходимость выявить связь подозреваемого, принадлежащих ему предметов и других объектов с расследуемым событием по оставленным следам и иным материальным отображениям. Суть идентификации заключается в том, чтобы по отображениям установить конкретный объект, который их оставил. Поэтому с криминалистической точки зрения характеристику компьютерного преступника целесообразнеесчитать понятием собирательным в широком смысле этого слова, хотя и с некоторым делением на самостоятельные обособленные группы по ряду оснований.

2. Материалы и методы

Основным источником для написания данной статьи стали официальные документы в сфере информационной безопасности, УК РФ 1996 г. указывающий несколько видов преступного в компьютерных преступлениях, а также документы, регламентирующие действия правоохранительных органов в криминалистической деятельности.

Методологическую основу данного исследования составили логические приемы, определения, описания, анализа и синтеза. Также использован общенаучный метод анализа.

3. Обсуждение

В криминалистической идентификации сравнение является одним из методов познания, предполагающее изучение двух или нескольких объектов с целью выявления как общего, объединяющего их, так и различного. Выявление и оценку различий между объектами, принадлежащими к одной или разным группам, в криминалистике и судебной экспертизе принято называть различением, или дифференциацией**.** Положительный результат идентификации означает установление тождества, а дифференциации — его отсутствие. Дифференциация может выступать и как самостоятельная задача.

На угрозу кибербезопасности до недавнего времени слабо реагировали не только правоохранительные органы. Зачастую IT-сфера не располагает соответствующим техническим оснащением для своевременного выявления кибер-шпионажа. Ресурсы так называемых хакеров все еще остаются на порядок выше техники правоохранительных органов. Необходимо грамотно подойти к организации методов, противодействующих киберпреступности и обеспечивающих безопасность в виртуальном пространстве.

Криминалистическая идентификация — одно из средств, способствующих установлению истины в судопроизводстве.

Из приведенных определений следует, что у каждого способа совершения преступления существует свой механизм. Именно обобщенные данные о механизме совершения преступления содержат сведения о наиболее характерных следах преступления и позволяют найти виновного. Ниже рассмотрим основные направления, по которым можно составить механизм совершения преступления. Этот механизм в некоторой степени схож моделью нарушителя в информационной безопасности.

В первую очередь – это определение преступного поведения. Можно выделить для преступлений в сфере компьютерной информации несколько видов данного поведения (Яблоков, 1994):

1) получение возможности знакомиться и осуществлять операции с чужой компьютерной информацией, находящейся на машинных носителях, т.е. направленные прежде всего на нарушение конфиденциальности информации;

2) изготовление и распространение вредоносных программ («вредных и опасных инфекций»), которые приводят к нарушению целостности информации;

3) изготовление и использование вредоносных программ (инфекций проникновения»), которые направлены на нарушение целостности и конфиденциальности информации;

4) действия, связанные с нарушением порядка использования технических средств, повлекшие нарушение целостности и конфиденциальности информации.

Можно отметить, что виды преступного поведения 1 и 2 всегда связаны с нарушением порядка использования информационной системы (в том числе и составляющих ее технических средств, например, ЭВМ), установленного ее собственником (владельцем).

Следующим направлением является изучение способа преступных действий в сфере компьютерной информации, которые могут быть разделены на две группы (Каторин и др., 2000).

Первая группа преступных действий осуществляется безиспользования компьютерных устройств в качестве инструмента для проникновения извне в информационные системы или воздействия на них. Это могут быть, например, хищение машинных носителей информации в виде блоков и элементов ЭВМ (например, флоппи-дисков); использование визуальных, оптических и акустических средств наблюдения за ЭВМ; считывание и расшифровка различных электромагнитных излучений и «паразитных наводок» в ЭВМ и в обеспечивающих системах; фотографирование, в том числе издалека, информации в процессе ее обработки;

- изготовление бумажных дубликатов входных и выходных документов, копирование распечаток; использование визуальных, оптических и акустических средств наблюдения за лицами, имеющими отношение к необходимой злоумышленнику информации и подслушивание их разговоров;

- осмотр и изучение не полностью утилизированных отходов деятельности вычислительных центров; вступление в прямой контакт с лицами, имеющими отношение к необходимой злоумышленнику информации и получение от них под выдуманными предлогами необходимых сведений и др. Для таких действий, как правило, характерны локальная следовая картина, определяющаяся стандартным пониманием места происшествия (место совершения преступных действий и местонахождение объекта преступного посягательства находятся вблизи друг от друга или совпадают), и традиционные приемы по их исследованию.

Вторая группа преступных действий осуществляется с использованием компьютерных и коммуникационных устройств в качестве инструмента для проникновения в информационные системы или воздействия на них. Характерной особенностью данного вида преступной деятельности является то обстоятельство, что место совершения непосредственно преступных действий и место, где наблюдаются и материализуются их результаты, могут находиться на значительном удалении друг от друга (например, в разных точках земного шара). В этих случаях при неправомерном доступе и распространении вредоносных программ, а также при нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети, картина преступления включает в себя (Герасименко, 1994):

-следы на машинных носителях, посредством которых действовал преступник на своем рабочем месте и возле машинных носителей, принадлежащих преступнику;

- следы на «транзитных» (коммуникационных) машинных носителях, посредством которых преступник осуществлял связь с информационными ресурсами, подвергавшимися нападению;

- следы на машинных носителях информационной системы, в которую осуществлен неправомерный доступ.

Для действий с «безвредными» и «опасными инфекциями» характерно изучение устройств ЭВМ и программного обеспечения с целью поиска и дальнейшего использования их недостатков; разработка задачи на изготовление вредоносной программы (далее ВП), определение будущих среды существования и цели ВП; выбор средств и языков реализации ВП;

- написание непосредственно текста ВП; отладка программы (проверка соответствия содержания информации поставленной задаче); запуск и непосредственное действие ВП, наблюдение за результатами действия ВП. Для действий с «инфекциями проникновения» характерны, кроме указанных дополнительно, активное использование преступником возможностей, возникших в результате действия данной ВП, т.е. копирование, модифицирование и иные действия с информацией в системе, подвергнувшейся нападению.

Таким образом можно выделить следующие идентификационные признаки:

- следы на машинных носителях, посредством которых действовал преступник на своем рабочем месте и возле машинных носителей, принадлежащих преступнику;

- следы на «транзитных» (коммуникационных) машинных носителях, посредством которых преступник осуществлял связь с информационными ресурсами, подвергавшимися нападению;

- следы на машинных носителях информационной системы, в которую осуществлен неправомерный доступ.

Третье направление изучения механизма совершения компьютерного преступления и идентификации преступника – это определение обстановки совершения преступления. Под обстановкой совершения преступления понимается система различного рода взаимодействующих между собой до и в момент преступления объектов, явлений и процессов, характеризующих место, время, вещественные, природно-климатические, производственные бытовые и иные условия окружающей среды, особенности поведения непрямых участников противоправного события, психологические связи между ними и другие факторы объективной реальности, определяющие возможность, условия и обстоятельства совершения преступления (Вихров и др., 2014).

Обстановка преступлений в сфере компьютерной информации характеризуется существенными факторами.

Прежде всего следует указать, что эти преступления совершаются в области профессиональной деятельности по обработке компьютерной информации. Преступники, как правило, владеют специальными навыками не только в области управления ЭВМ и ее устройствами, но и специальными знаниями в области обработки информации в информационных системах в целом. При этом для корыстных преступлений, связанных с использованием информационных систем, характерны и специальные познания в соответствующих финансовых, банковских и подобных информационных технологиях. Для преступлений, касающихся нарушений правил эксплуатации ЭВМ и манипуляций с вредоносными программами, характерны специальные познания в узкой предметной профессиональной области устройств ЭВМ и программного обеспечения.

Четвертое – это предположение о том, кто мог совершить компьютерное преступление. УК РФ разделил «компьютерных преступников» на следующие категории (Уголовный кодекс...): лица, осуществляющие неправомерный доступ к компьютерной информации; лица. осуществляющие неправомерный доступ к компьютерной информации в группе по предварительному сговору или организованной группой; лица, осуществляющие неправомерный доступ к компьютерной информации с использованием своего служебного положения; лица, имеющие доступ к ЭВМ, но осуществляющие неправомерный доступ к компьютерной информации или нарушающие правила эксплуатации ЭВМ; лица, создающие, использующие и распространяющие вредоносные программы.

Далее предполагая, что в стандартную криминалистическую характеристику данного вида преступной деятельности необходимо включить следующую классификацию преступников, обеспечивающую выдвижение версий о лице в зависимости от способа и мотивации действий, выражающихся в следовой картине:

-«хакеры» — лица, рассматривающие защиту компьютерных систем как личный вызов и взламывающие их для получения полного доступа к системе и удовлетворения собственных амбиций;

-«шпионы» — лица, взламывающие компьютеры для получения информации, которую можно использовать в политических, военных и экономических целях;

- «террористы» — лица, взламывающие информационные системы для создания эффекта опасности, который можно использовать в целях политического воздействия

- «корыстные преступники» — лица, вторгающиеся в информационные системы для получения личных имущественных или неимущественных выгод;

- «вандалы» — лица, взламывающие информационные системы для их разрушения;

- психически больные лица, страдающие новым видом психических заболеваний — информационными болезнями или компьютерными фобиями.

4. Результаты

Безусловно, специфика совершения компьютерных преступлений связана с фактическим отсутствием межгосударственных границ. Но УК РФ предусмотрен ряд наказаний за киберпреступления, так как правовой защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее владельцу, пользователю и иному лицу (Бондарь, 2013). Именно поэтому подчеркивается общественная опасность каких-либо действий с вредоносными программами и не только.

Таким образом, мы рассмотрели 4 направления, по которым можно идентифицировать преступника с точки зрения криминалистики. К ним относятся:

- Определение преступного поведения: подразумевает собой мотивацию преступника, что побудило его к действиям, здесь можно выделить три основных направления нарушения – это личный интерес, корыстные побуждения, конкуренция, в любом случае все направлено на нарушение целостности, конфиденциальности и доступности таким образом, чтобы нанести наибольший ущерб;

- Техническая оснащенность преступника (с использованием или без использования компьютерных средств): в данном случае конечно сложнее искать преступника, если он использует специальные средства, так при их использовании сложнее определить местоположение подозреваемого, так как в информационном пространстве возможна подмена ip-адресов;

- Определение обстановки совершения преступления: здесь особое внимание необходимо уделить профессиональной сфере, так как чаще всего преступления подобного характера встречаются в работе с финансовыми, банковскими информационными технологиями;

- Квалификация преступника: область данного направления достаточно обширна, так как уровень квалификации, может быть какой угодно, начиная от новичка-хакера и заканчивая опытным шпионом.

Помимо направлений, рассмотренных выше, важно учитывать социально-психологические условия, как идентификационный признак киберпреступлений, в которых ведется расследование. Настрой общества по отношению к информационным преступлениям под воздействием средств массовой информации периодически меняется. Это обстоятельство влияет на поведение участников расследования. Полярными значениями этих отношений является неприятие действий преступников, совершивших действия, влияющие на интересы некоторых слоев общества в отдельной стране до возвеличивания отдельных преступников.

Однако все эти преступления связаны с нарушением установленного порядка профессиональной деятельности и личных интересов. Становится понятно, что для правонарушителей в данной области обычно ясен механизм нарушения правил пользования информационными ресурсами и его связь с событиями, повлекшими наступление криминального результата.

5. Заключение

Таким образом, можно сказать, что проблемы в данной области обусловлены отчасти 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. Кроме того, с появлением нового средства обработки информации компьютер и программное обеспечение могут быть предметом законных и незаконных сделок, а также предметом хищения как ценных объектов или противоправного использования. Они могут быть также инструментом преступной деятельности, например, средствами незаконного доступа к удаленным информационным ресурсам, инструментами разработки и запуска «компьютерных вирусов», причиняющих существенный материальный ущерб, хранилищем и инструментом обработки информации о преступной деятельности, например, данных о действительном состоянии учета и движения материальных ценностей, о партнерах по

противоправным сделкам и их содержании, использованы как средство подготовки управленческих решений, которые повлекли негативные результаты.

Для решения данных проблем уже существует решение: необходимо повысить уровень мониторинга данного вида преступлений; разработать программы повышения квалификации сотрудников полиции по расследованию данной категории дел; повысить технические возможности экспертов, специализирующихся в области исследования компьютерных технологий; увеличить объем научно-методической литературы, посвященной прикладным аспектам расследования компьютерных преступлений и кроме того в высших учебных заведениях появилось специальное направление – 10.03.01 «Информационная безопасность».

Иными словами, для расследования преступлений, совершенных в киберпространстве, требуются как технические, так и теоретические знания, реализация определенной схемы сбора криминалистических данных и идентификационных признаков. Соответственно, возникает необходимость выработки единого понятия киберпространства с точки зрения криминалистики.

Примечания

Бондарь, 2013 – *Бондарь В.В.* (2013). Киберпреступность – современное состояние и пути борьбы. Юридические записки №2. [Электронный ресурс]. URL: http://cyberleninka.ru/article/n/kiberprestupnost-sovremennoe-sostoyanie-i-puti-borby

Вихров и др., 2014 – *Вихров Н.М., Каторин Ю.Ф., Нырков А.П., Соколов С.С.* (2014). О безопасности инфраструктуры водного транспорта. СПб.: Ж. «Морской вестник» №4 (58), с. 99–102.

Герасименко, 1994 – *Герасименко В.А.* (1994). Защита информации в автоматизированных системах обработки данных: В 2 т. М. Т. 1. С. 170-174.

Каторин и др., 2000 – *Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н.* (2000). Большая энциклопедия промышленного шпионажа. Спб.: ООО «Издательство Полигон», 856 с.

Об информации… – Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ (в ред. от 28.07.2012 г.). ГАРАНТ: информационно-правовой портал. URL: http://base.garant.ru/ 12148555/ (Дата обращения: 25.08.2016)

Уголовный кодекс… – Уголовный кодекс Российской Федерации. Глава 28. Преступления в сфере компьютерной информации.13.06.1996 N 63-ФЗ (ред. от 29.06.2015). Собрание законодательства РФ, 1996.

Яблоков, 1994 – *Яблоков Н.П.* (1994). Компьютерные технологии в юридической деятельности. М.: Криминалистика.

References

Bondar', 2013 – *Bondar' V.V.* (2013). Kiberprestupnost' – sovremennoe sostoyanie i puti bor'by. Yuridicheskie zapiski №2. [Elektronnyi resurs]. URL: http://cyberleninka.ru/article/n/kiberprestupnost-sovremennoe-sostoyanie-i-puti-borby

Vikhrov i dr., 2014 – *Vikhrov N.M., Katorin Yu.F., Nyrkov A.P., Sokolov S.S. (2014).* O bezopasnosti infrastruktury vodnogo transporta. SPb.: Zh. «Morskoi vestnik» №4 (58), s. 99–102.

Gerasimenko, 1994 – *Gerasimenko V.A.* (1994). Zashchita informatsii v avtomatizirovannykh sistemakh obrabotki dannykh: V 2 t. M. T. 1. S. 170-174.

Katorin i dr., 2000 – *Katorin Yu.F., Kurenkov E.V., Lysov A.V., Ostapenko A.N.* (2000). Bol'shaya entsiklopediya promyshlennogo shpionazha. Spb.: OOO «Izdatel'stvo Poligon», 856 s.

Ob informatsii… – Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii [Elektronnyi resurs]: federal'nyi zakon RF ot 27 iyulya 2006 g. № 149-FZ (v red. ot 28.07.2012 g.). GARANT: informatsionno-pravovoi portal. URL: http://base.garant.ru/ 12148555/ (Data obrashcheniya: 25.08.2016)

Ugolovnyi kodeks… – Ugolovnyi kodeks Rossiiskoi Federatsii. Glava 28. Prestupleniya v sfere komp'yuternoi informatsii.13.06.1996 N 63-FZ (red. ot 29.06.2015). Sobranie zakonodatel'stva RF, 1996.

Yablokov, 1994 – *Yablokov N.P.* (1994). Komp'yuternye tekhnologii v yuridicheskoi deyatel'nosti. M.: Kriminalistika.

УДК 004.056.53

Криминалистичекая идентификация и идентификационный признак в киберпреступлениях

Ксения Николаевна Золотарева [a, *], Екатерина Николаевна Золотарева [a]

[a] Университет ИТМО, Российская Федерация

Аннотация. В данной статье рассматривается понятие криминалистики в компьютерных преступлениях, изложены актуальные проблемы компьютерных преступлений в условиях совершенствования информационно-телекоммуникационных технологий и предложены пути их решения. Также приведены основные идентификационные признаки компьютерных преступлений в криминалистике. Проанализированы направления, на которых основан первичный признак поиска преступника в информационной сфере.

Ключевые слова: компьютерные преступления, криминалистика, криминалистическая идентификация, идентификационный признак.

[*] Корреспондирующий автор
Адреса электронной почты: ksenya2894@rambler.ru (К.Н. Золотарева), katerina2794@rambler.ru (Е.Н. Золотарева)