Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
ЮРИДИЧЕСКИЙ ИНСТИТУТ
Кафедра «Уголовный процесс, криминалистика и судебная экспертиза»

ОСОБЕННОСТИ ПРОВЕДЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ФГАОУ ВО «ЮУрГУ» (НИУ) – 40.03.01. 2017. 470. ВКР

Руководитель работы,
преподаватель кафедры
_____Дарья Сергеевна Ермолаева
_____2021 г.

Автор работы,
студент группы Ю-470
_____Никита Витальевич Тупиков
_____2021 г.

Нормоконтролер,
преподаватель кафедры
_____Виталина Викторовна Гончаренко
_____2021 г.

Челябинск
2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 3

1 КИБЕРПРЕСТУПЛЕНИЯ ПОНЯТИЕ, КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА И МЕХАНИЗМ ОБРАЗОВАНИЯ ВИРТУАЛЬНЫХ СЛЕДОВ 6

1.1 Понятие киберпреступления 6

1.2 Криминалистическая классификация киберпреступлений 16

1.3 Криминалистическая характеристика киберпреступлений 26

1.4 Следы в киберпреступлениях: понятие, классификация и механизм образования 35

2 ТАКТИКА ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ 47

2.1 Тактика проведения осмотра места происшествия 47

2.2 Тактика проведения обыска и выемки при расследовании киберпреступлений 59

2.3 Назначение и виды судебных экспертиз при расследовании киберпреступлений 70

ЗАКЛЮЧЕНИЕ 80

БИБЛИОГРАФИЧЕСКИЙ СПИСОК 84

ВВЕДЕНИЕ

Компьютеризация общества, в результате научно-технического прогресса, позволила человечеству перенести любую информацию с бумажного на электронный носитель, тем самым упростив процесс обмена и хранения информации. С каждым годом компьютерные инженеры, программисты развивают технологии делая ее все более социально значимой. И на сегодняшний день в медицинских учреждениях от высокотехнологичных приборов зависит человеческая жизнь.

Но, наряду с развитием научно-технического прогресса также развивается преступность. Любая информация, хранящаяся на любом устройстве, потенциальна связанна с риском ее утраты или изменением в результате противоправных действий злоумышленников. Автоматический процесс обработки информации, ненадлежащая или того хуже отсутствующая защита, и другие объективные факторы делают информацию уязвимой для преступных манипуляций.

Согласно статистике, размещенной на официальном сайте МВД, с января по ноябрь 2020 года, на фоне снижения количества преступлений, против собственности таких как грабежей и разбоев, выросла преступность с применением IT-технологий.

Сотрудникам органов предварительного расследования достаточно сложно расследовать данную категорию преступлений, в связи с:специфичностью преступлений, отсутствием методических рекомендаций по организации расследования, отсутствие методических рекомендаций по производству следственных действий; не умение органов предварительного расследования работать с специфичными источниками доказательственной информации.

В связи с быстроразвивающийся киберпреступностью и развитием способов ее осуществления, проблема разработки методических рекомендаций касающихся теоретических положений природы

киберпреступлений и тактики производства следственных действий, непосредственно связанных с технологиями, представляется как никогда актуальной темой.

Цель выпускной квалификационной работы состоит в исследовании теоретических положений и позиций ученых криминалистов данной категории преступлений, исследование проблем производства следственных действий при расследовании киберпреступлений, изучение существующих позиций решения проблем, и выработка рекомендаций по повышению эффективности производства следственных действий.

Задачами выпускной квалификационной работы является:

- дать определение термину «киберпеступления»;

- составить криминалистическую классификацию киберпреступлений;

- составить криминалистическую характеристику киберпреступлениям;

- дать определение понятию «электронно-цифровой след», составить классификацию, выявить особенности природы их возникновения;

- выявить особенности тактики производства осмотра места происшествия;

- выявить особенности тактики производства обыска и выемки;

- выявить особенности назначения компьютерно-технической экспертизы.

Объектом выпускной квалификационной работы являются, осуществляемые преступления в киберпространстве; производство следственных действий при расследовании киберпреступлений осуществляемые органами предварительного расследования.

Предметом выпускной квалификационной работы являются закономерности механизма совершения киберпреступлений; закономерности механизма образования «электронно-цифрового следа»;порядок производства следственных действий; в аспекте производства следственных действий, теоретические положения криминалистики, уголовного права, уголовного процесса, теории судебных экспертиз.

Теоретическая основа. Данная категория преступлений представляет для научного сообщества наибольший интерес, в связи с ее спецификой совершения, так над данной тематикой работали отечественные ученые в области криминалистики, уголовного права, криминологии, уголовного процесса, судебной экспертизы: В.Б. Вехов , Е.С. Шевченко, В.Ю. Агибалов, Е.А. Ищенко О.Я Баева, Р.С. Белкина, Т.С В.С. Волчецкая, Ю.В. Гаврилина, В И. Комиссарова, В.В. Крылова, А.И. Усова и других авторов.

Нормативную и эмпирическую основу выпускной квалификационной работы составляют: Конституция РФ, нормы международного права, Уголовный кодекс РФ, Уголовно-процессуальный кодекс РФ, иные федеральные законы и иные нормативно правовые акты, материалами судебной практики, статистические данные с сайта правовой статистики, результатами проведенных исследований.

Методологической основой выпускной квалификационной работы является диалектический метод, а также общенаучные методы познания: анализа, синтеза, индукции. Кроме того, использовался статистический метод.

Структура выпускной квалификационной работы определена характером исследуемых в ней вопросов. Работа состоит из: введения, двух глав, включающих 7 параграфов, заключения и библиографического списка.

1 КИБЕРПРЕСТУПЛЕНИЯ ПОНЯТИЕ, КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА И МЕХАНИЗМ ОБРАЗОВАНИЯ ВИРТУАЛЬНЫХ СЛЕДОВ

1.1 Понятие киберпреступления

Компьютеризация общества, в результате научно-технического прогресса, позволила человечеству перенести любую информацию с бумажного на электронный носитель, тем самым упростив процесс обмена и хранения информации. С каждым годом компьютерные инженеры, программисты развивают технологии делая ее все более социально значимой. И на сегодняшний день в медицинских учреждениях от высокотехнологичных приборов зависит человеческая жизнь.

Но, наряду с развитием научно-технического прогресса также развивается преступность. Любая информация, хранящаяся на любом устройстве, потенциальна связанна с риском ее утраты или изменением в результате противоправных действий злоумышленников. Автоматический процесс обработки информации, ненадлежащая или того хуже отсутствующая защита, и другие объективные факторы делают информацию уязвимой для преступных манипуляций.

Так в США 2008 году в процессе эксперимента, взломщикам удалось проникнуть в систему дефибриллятора/кардиостимулятора компании Metronic при помощи специального оборудования, тем самым получить доступ к данным, которые передавал прибор. Помимо этого, удалось внести изменения в систему аппарата нарушив его работу, тем самым в случае реальной кибератаки мог погибнуть человек подключенный к данному прибору. В результате эксперимента ученные пришли к выводу, что вопрос кибербезопасности в медицинской сфере выходит на первый план.[1]

[1]Гудин Д. Эксперимент Билли Риос и Джонатан Баттс по взлому кардиостимулятора CareLink 2090. URL: https://arstechnica.com/information-technology/2018/08/lack-of-

На данный момент не было зарегистрировано случаев смерти человека в результате кибератак аппаратов и устройств имплантированных в телах пациентов, но риск существует. За последние 3 года медицинские организации больше подвергаются хакерским атакам, связанные с хищением персональной медицинской информации. Так в Сингапуре злоумышленники похитили персональные данные 1,5 млн. человек, включая информацию о премьер министре страны. По мнению аналитиков, причиной тому служит незащищенный доступ к базам данных и уязвимость интернет сетей.

Согласно статистике,размещенной на официальном сайте МВД, с января по ноябрь 2020 года, на фоне снижения количества преступлений, против собственности таких как грабежей и разбоев, выросла преступность с применением IT-технологий. Кражи на 81,6%, а также противоправных деяний, предусмотренных статьями 159, 159.3, 159.6 УК РФ, на 76,1%.[1] По мнению генерального директора компании, специализирующейся в сфере кибербезопасностиGroup-IB Сачков И.К., утверждает, что причиной данного роста киберпреступности является режим дистанционной работы в связи с возникшей эпидимиологической ситуацией, так как выросла потребность в использовании онлайн услуг с применением электронных средств платежей через цифровые сервисы, что для злоумышленников представляет в корыстных целях наибольший интерес.[2]

Для пресечения дальнейшего развития данного вида преступлений необходима координация действий на международном уровне.Так Члены ООН в руководстве по предотвращению и контролю над преступлениями, связанными с использованием компьютерной сети Интернет, признали глобальной международной проблемой посягательства, возникающие в

---

encryption-makes-hacks-on-life-saving-pacemakers-shockingly-easy/ (дата обращения 05.01.2021).

[1] Краткая характеристика состояния преступности в Российской Федерации за январь ноябрь 2020. Официальный сайт МВД РФ. URL: https://xn--b1aew.xn--p1ai/reports/item/22501861/ (дата обращения: 05.01.2012).

[2] Интервью И.К. Сачкова РИА Новости. URL : https://ria.ru/20200707/1573997584.html (дата обращение 05.01.2012)

киберпространстве. Эквивалентная позиция содержится и в таких международных нормативно-правовых актах, как: Конвенция Совета Европы о киберпреступности, Бангконской декларации, Окинавской Хартии глобального информационного общества.[1]

Не обращая внимание на то, что киберпреступность превратилась в острейшую проблему и борьба с ней уже стала задачей всего мирового сообщества, до настоящего момента не решен вопрос общепризнанном наименовании и определении преступлений в информационно-технологическойсфере.

На международном уровне используется несколько подходов к термину и определению данного вида преступлений. Преимущественно в нормативных актах международного уровня используется термин киберпреступность.На десятом Конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями от 19 июля 2000 года, были выработаны два определения.Первое,киберпреступность в узком смысле (компьютерная преступность) под которым понималось возникшие в форме электронных операций, любое противозаконное поведение, направленное против безопасности компьютерных систем и обрабатываемых ими данных. Второе, киберпреступность в широком смысле (преступления, связанные с применением компьютерных технологий), понимается как противоправное поведение, осуществляемое с использованием компьютерной системой или сетью, включая такие преступления как незаконное владение, распространение или предложение компьютерных данных посредством компьютерных систем или сетей.[2] Другие же подходы отражаются в таких международных актах как Соглашении Содружества Независимых

---

[1]Окинавская хартия глобального информационного сообщества (принята на о. Окинава (Япония) 22.07.2000 на совещании руководителей Глав государств и правительств стран «Группы Восьми»). Дипломатический вестник. 2000. № 8. С. 51 – 56.

[2] Лунев, В. В. Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями, его место в истории конгрессов. Государство и право. 2000. № 9. С. 95 – 100.

Государств от 1 октября 2018 года и Будапештской Конвенции Совета Европы ETS 185 23 ноября 2001 года.

В Соглашении СНГ за место термина «киберпреступность» используется определение «преступления в сфере компьютерной информации» под которым понимается уголовно наказуемое деяние, предметом которого является компьютерная информация. Так же аналогично в Соглашении между правительствами государств членов Шанхайской организации сотрудничества используется понятие «информационная преступность» под которым понимается использование в противоправных целях информационных ресурсов, а также воздействие на них в информационном пространстве.Стоит отметить, что данные подходы отражают лишь часть совершаемых преступлений, предметом которого является компьютерные данные (информация).

В Будапештской Конвенции Совета Европы ETS 185 от 23 ноября 2001 года используется понятия «cybercrime - киберпреступление» и «computer-relatedcrime – компьютерные преступления» в качестве аналогичных по смыслу, при этом не дается определение данным дефинициям в ст. 1 гл. 1.

А.Г. Волевоз[1] и И.А. Попов[2] считают, что основной идеей данного международного договора является введение норм об уголовной ответственности за «киберпреступления» в национальное законодательство участников Совета Европы, перечень которых включает уголовную ответственность за: 1) противоправные действия, направленные против компьютерной информации (предмета посягательства), а также ее использование в роли уникального орудия совершения преступления; 2) противоправные действия, направленные на какие-либо охраняемые законом права, свободы и интересы, где информация, компьютер и иное выступает в качестве одним из признаков объективной стороны состава преступления.

[1]Волеводз А. Г. Конвенция о киберпреступности: новации правового регулирования. Правовые вопросы связи. 2007. № 2. С. 17 – 25.

[2] Попов И. А. Правовое и организационное обеспечение раскрытия и расследования преступлений в сфере компьютерной информации: состояние и пути совершенствования. Библиотека криминалиста. 2013. № 5 (10). С. 325.

Управление ООН по борьбе с наркопреступностью, в 2013 году опубликовал отчет «Всестороннее исследование проблемы киберпреступностии ответных мер со стороны государств – членов, международного сообщества и частного сектора», в нем термин «киберпреступность» отражен в зависимости от контекста и цели его употребления.Помимо этого, в отчете указывается, что в перечень компьютерных преступлений включаются не только преступления против конфиденциальности, целости или доступности данных, или систем, но и любые другие деяния, предполагающие использование компьютера в целях причинение личного или финансового вреда, (и) или с целью получения прибыли, включая преступления предметом которого являются персональные данные. Авторы отчета также указывают что нет необходимости в создании универсального определения киберпреступности, так как в целях расследования киберпреступности на международном уровне важнее согласовать нормы, относящиеся к сбору и предоставлению электронных доказательств, а не искать широкое, искусственное определение концепции «киберперсутпления».[1]

В Российском законодательстве также нет определения киберпреступности, однако в Уголовном Кодексе РФ имеется ряд статей предусматривающие уголовную ответственность за общественно-опасные деяния в данной категории преступлений:[2]

- ст.159.6 Мошенничество в сфере компьютерной информации;

- ст. 272. Неправомерный доступ к компьютерной информации;

- ст. 273. Создание, использование и распространение вредоносных компьютерных программ;

---

[1] Доклад ООН Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств – членов, международного сообщества и частного сектора. Документ ООН. UNODC/ CCPCJ/EG.4/2013/2: UNODC.Comprehensive Study on Cybercrime,
February 2013, P. XVII. URL: https://www.unodc.org/documents/organized crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (дата обращения 10.01.2021).

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. СЗ РФ.1996. № 25. Ст. 2954.

- ст. 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

При анализе статей следует вывод, что законодатель выделил важный элемент компьютерную информацию в качестве предмета или средства преступления. Так как именно компьютерная информация объединяет различные виды преступлений.

В примечании 1 ст. 272 УК РФ,«под компьютерной информацией понимается сведения, сообщения или данные имеющие форму электрических сигналов, независимо от средств хранения, обработки или передачи». А примирительно к процессу доказывания компьютерной информацией являются, фактические данные, обработанные средствами системы и (или)передающиеся по телекоммуникационным каналам, которые доступны для восприятия человеком, на основе которых устанавливаются обстоятельства имеющие значения по уголовному делу. А.А. Васильев[1] и К.Е. Демин[2] отмечают в качестве источников данной информации могут выступать: файл, данные на различных электронных устройствах, листинг, машинная распечатка.

В отечественных научных кругах также существует разброс мнений о подходе к понятию и теоретическим аспектам данной категории преступлений. Большинство научных работ в сфере криминалистикинаправленны на исследование проблемы расследования преступлений, связанных с электронно-вычислительными машинами, их системами и сетями. В них же отражается проблема не изученности понятийного аппарата данной категории преступлений и отсутствие единого подхода к термину «киберпреступение» в криминалистическом аспекте.

---

[1] Васильев А. А.; Дёмин, К. Е. Электронные носители данных как источники получения криминалистически значимой информации: учеб. пособие. М., 2009. С. 47

[2] Дёмин К. Е. К вопросу о выделении криминалистического исследования электронных носителей информации как новой отрасли криминалистической техники. Библиотека криминалиста. 2013. № 5 (10). С. 174 – 189.

В.А. Дуленко, В.А. Пестриков и Р.Р. Мамлеев, в широком смысле выделяют понятие киберпреступление как «любое противоправное деяние, совершаемое с использование или связи с компьютерными устройствами, выключая незаконное хранение, предложение или распространение информации посредством компьютерных технологий»[1]. Указанные авторы в целом связывают киберпреступления с правонарушениями, совершаемые в различных информационных сетях.

Другие же учебные определяют киберпреступения к противоправным деяниям совершаемые с использованием компьютерных и мобильных связей в сетях.

Так, И.Г. Чекунова считает «киберпреступления - это общественно опасные деяния, совершаемые посредством использования компьютерной и мобильной техники, их программ в отношении информации, размещённой, обрабатываемой и используемой в виртуальном пространстве сети Интернет».[2]

В.Д Курушина и В.А. Минаев в свою очередь определяют киберпреступление как действие в Интернет сети, при которых компьютер используется в качестве орудия либо является предметом преступных посягательств в киберпространстве. А по мнению И.М. Россоловой«киберпрестулпения являются общественно опасные деяния, совершаемые с использованием средств компьютерной техники, с целью посягательства на информацию, обрабатываемую и используемую в сети Интернет».[3]

Справедливо отмечает Е.С. Шевченко, что данные определения имеют узкую направленность и не полностью отражают специфику и природу

---

[1]Дуленко В. А. Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации: учебное пособие. УЮИ МВД России. Уфа. 2007. С. 15.

[2]Чекунов И. Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений. Право и кибербезопасность. М., Юрист. 2012. С. 9 – 22.

[3] Рассолов И. М. Право и Интернет. Теоретические проблемы. Изд. 2-е. Норма. М., 2009. С. 135.

данной категории преступлений. Она же определяет «кибепреступления», как «общественно опасное деяние, совершаемое в киберпространстве, посягающее на охраняемые законом отношения, необходимым элементом механизма подготовки, совершения, сокрытия и отражения которого является компьютерная информация, выступающая в роли предмета или средства преступления».[1] Под киберпространством она определяет «область взаимодействия информационных многоуровневых систем, включая элементы: системы, сети, программы,а также иные данные циркулирующие в них». Так же она выделяет общие и частные признаки данной категории преступлений «под общими признаками выступают деяния в киберпространстве с использованием предмета посягательства либо предоставление дистанционного доступа к нему посредством виртуальных сетей и иных средств, а к частным признакам относит: специфичность способов совершения деяний, международный характер, особые качества преступника».

Все же ранееуказанные подходы объединила Т.Л. Тропина определив киберпреступления как «виновно совершенное, общественно опасное, уголовно наказуемое деяния, по вмешательству в работу компьютерных технологий, программ, сетей и несанкционированная модификация данных, а также иные противоправные , общественно опасные действия совершаемые с помощью или посредством компьютеров, их сетей и программ , включая с помощью или посредством каких-либо устройств доступа к моделируемому информационному пространству».[2]

Также существуют и другие подходы к наименованию данной категории преступлений, так А.В. Суслопаров выделяет понятие информационные преступления, определяя их как «общественно опасные противоправные деяния, причиняющие вред общественным отношениям по

---

[1] Шевченко Е. С. О криминалистической трактовке понятия «киберпреступность». Информационное право. 2014. № 3 (39). С. 29 – 32.

[2] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. … канд. юрид. наук. Владивосток. 2005. С. 9.

обеспечению информационной безопасности личности, общества и государства, имеющие своим предметом информацию как особый нематериальный объект»[1]. Он так же рассматривал компьютерные преступления как разновидность информационных преступлений, в силу наличия дополнительного объекта в виде общественных отношений по информационной безопасности, а также специфического признака выступающим в качестве предмета преступления особый вид информации (компьютерные данные).[2]

В свою очередь В.А. Номоконов относит киберпреступностьк преступлениям, совершаемым с использованием компьютерной техники против охраняемых законом прав и интересов. Он определяет «киберпреступность» в качестве родового понятия, которое охватывает компьютерную преступность в узком смысле, где предметом преступления является компьютер, а информационная объектом преступления выступает безопасность, так и иные посягательства, направленные против собственности, авторских прав, общественной безопасности и др, где компьютер используется как орудие или средство преступления.[3]

Также в литературе выделяется термин «компьютерная преступность» и используется для идентификации преступной деятельности с применением компьютерных технологий, однако данное понятие не способно в полной мере отразить природу данного явления. Так как термин «киберпреступление» имеет более широкий смысл и охватывает целый спектр противоправных деяний.

---

[1] Суслопаров, А. В. Информационные преступления: авт. дис … канд. юрид. наук. Суслопаров А. В. Красноярск, 2008. С. 23 .

[2]Суслопаров А. В. Компьютерные преступления как разновидность преступлений информационного характера: Дис. … канд. юрид. наук. Красноярск, 2010. С. 25

[3]Номоконов В.А. Актуальные проблемы борьбы с киберпреступностью. Компьютерная преступность и кибертерроризм. Запорожье. 2004. № 1. С. 77.

Так В.В. Воробьев компьютерные преступления определяет, как «противоправное посягательство объектом или орудием которого выступает электронно-вычислительная машина».[1]

Н.А. Селиванов и В.Б. Вехов, считают, что объектом посягательства являются компьютерные данные, а компьютер выступает в качестве орудия совершения деяния.Исходя из этого они определяют компьютерные преступления как противоправные, общественно опасные, виновные посягательства, с использованием информационно-вычислительных систем либо с воздействием на них.[2]

При анализе данных позиций следует вывод о том, что в определении «компьютерные преступления» главным критерием в качестве предмета выступают «компьютерные технологии», что не в полной мере отвечает действительности, так как в современное время преступления совершают с использованием мобильных гаджетов, приставок и другого оборудования. Так же не следует забывать о научно-технологическом процессе входе которого создаются новые технологии, которые могут стать как объектом, так и предметом преступного посягательства.

Следует согласиться с точкой зрения В.В. Крылова, который считает, что использование термина «компьютерные преступления» не полно отражает сущность данной категории преступлений, так как конкретизируется лишь одно используемое техническое средство компьютер. В качестве альтернативы предлагает более широкое понятие «информационные преступления», которое дает абстрагироваться от определенный технических средств. Однако стоит отметить, что данный термин носит оценочный характер, так как информация может выступать не только в качестве средства преступления, а также может быть предметом

---

[1] Воробьев В.В. Преступления в сфере компьютерной информации, юридическая характеристика составов и квалификация: дис. … канд. юрид. наук. Н. Новгород, 2006. С. 12.

[2] См., например, Селиванов Н. А. Проблемы борьбы с компьютерной преступностью. Законность. 1993. № 8. С. 37; Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия. Право и Закон. М., 1996. С. 24-25.

преступления, вынуждая тем самым проводить анализ связи информации с преступлением.

Таким образом, в результате вышеизложенных позиций следует вывод, что понятие «киберпреступление» несет в себе более широкое смысловое значение и точно отражает сущность преступлений в киберпространстве чем указанные выше понятия.

Определение «киберпреступление» можно понимать, как термин более широкий, нежели те, что были указаны ранее. Он в своей сути охватывает множество терминологий противоправных деяний. Все эти факты дают право определять киберпрестулпение с точки зрения криминалистики, а также понимать его как общественно опасное деяние, которое совершается в данном киберпространстве. Киберпреступлениепосягает на собственность и права человека, а также общественную безопасность с одной стороны, и, является необходимым элементом процесса как совершения преступления, так и его подготовки, и сокрытия. Отражением данных преступлений является компьютерная информация, которая выступает как предмет или средства совершённого преступления.

Следовательно, под «кибербреступлением» следует понимать, совершаемое в кибернетическом пространстве виновное, общественно-опасное деяние, посягающее на охраняемые уголовным законом права, свободы и интересы, в котором необходимым элементом механизма преступления является компьютерная информация, выступающая в качестве предмета или средства преступления.

1.2 Криминалистическая классификация киберпреступлений

В ходе следственных действий криминалистическая классификация преступлений получает самое непосредственное и активное практическое применение. С ее помощью у следователя формируется понимание сути расследуемых событий, что и позволяет ему в дальнейшем грамотно

выстраивать, выбирать и применять предлагаемые практиками криминалистических методик расследования определенных видов киберпреступлений.

Отсутствие единой выработанной криминалистической классификациикиберспреступленийпорождает проблемы в разработке рекомендаций и методик расследования преступлений, что и безусловно в полной мере скажется на ход расследования.

На международно-правовомуровнев рамках Конвенции Совета Европы построена классификация с выделением пяти групп киберпреступлений.[1]Данная классификация является наиболее востребованной в международном сообществе включая Российскую Федерацию, что и подтверждается судебной практикой.

К первой группе преступлений относится противоправные действия, направленные на конфиденциальность, целостной и недоступность компьютерных данных и систем, таких как несанкционированный доступ, незаконный перехват, вмешательство в базы данных и систему (272 УК РФ).

Так согласно мотивировочной части приговора центрального районного суда, г. Челябинска от 17 июня 2019 года. Федоренко С.С. в период с 23.11.2017 по 30.10.2017 г.г., используя вредоносную компьютерную программу, предназначенную для несанкционированного копирования информации, работающую на устройствах под управлением операционной системы «Windows» и предназначенную для обнаружения установленных на компьютерной технике пользователей сети Интернет разных браузеров, осуществляя поиск информации, хранящийся в служебной директории логино-парольных комбинаций и url-адресов веб-сайтов, с последующим копированием данной информации на Интернет-ресурс, неправомерно получил доступ к охраняемой законом компьютерной информации, повлекший копирование указанной информации.Своими

[1]Волеводз А. Г. Конвенция о киберпреступности: новации правового регулирования. С. 22.

действиями Федоренко С.С. совершил преступление, предусмотренное ч.1 ст. 272 УК РФ.[1]

К второй группе относятся преступления, связанные с использованием компьютера в качестве средства совершения противоправных действий (компьютерное мошенничество или подлог), т.е. средства манипуляции с информацией (159.6УК РФ).

Так согласно мотивировочной части приговора от 29.07.2020 г. Октябрьского городского суда Республики Башкортостан, осуждена Данилова Е.С. по ст.159.6, исходя из обстоятельств дела 2.02.2020 г. в офисе обслуживания продаж ПАО «Вымпелком», Данилова Е.С. являясь специалистом офиса обслуживания и продаж в указанной организации, имея навыки работы в компьютерной программе «1С», умышленно из корыстных побуждений, использовав свое служебное положение и данные ей учетные данные от программы, с целью неправомерного доступа к охраняемой законом информации и дальнейшей ее модификацией, неправомерно внесла сведения в товарный чек о внесении суммы клиентом в кассу предприятия определенной суммы денежных средств, для совершения платежа в биллинг, без фактического внесения денег в кассу, тем самым модифицировала компьютерную информацию, что повлекло за собой материальный ущерб в размере 516 050 рублей.[2]

К третьей группе относится, киберпреступления, связанные с размещением в информационно-коммуникационной сети Интернет запрещенного законом материала. К примеру, порнографические материалы с лицами не достигшие четырнадцати летнего или несовершеннолетнего возраста (ст. 242.1 УК РФ).

---

[1] Приговор Центрального районного суда г. Челябинска Челябинской области от 17 июня 2019 по делу № 1-297/2019. URL: //sudact.ru/regular/doc/nEzPAOLxrPlT/ (дата обращения: 17.01.2021).

[2] Приговор Октябрьского городского суда республики Башкортостан от 29 июля 2020 по делу 1-243/2020. URL: //sudact.ru/regular/doc/eLKpELsMEF5w/ (дата обращения: 17.01.2021).

Так Калужским районным судом Калужской области, было рассмотрено уголовное дело данной группы киберпреступлений. Согласно приговору от 25.11.2019 г. под №1-1084/2019 обвиняемый, находясь дома, обнаружил в социально сети «Вконтакте» видеозапись порнографического характера, в которой содержались изображения половых гениталий и сцен сексуальных действий с лицом не достигшего четырнадцатилетнего возраста.[1]

К четвертой группе относятся киберпреступления посягающие на авторские и смежные права, при этом установление данных правонарушений отнесено Конвенцией к компетенции национальных государств.

Комсомольским районным судом г. Тольятти было рассмотрено уголовно дело данной группы преступлений. Так согласно приговору от 21.07.2020 года под № 1-278/2020 было установлено, что

19.02.2020 в установленный следствием период времени обвиняемый, не имеющий авторского права, находясь в жилом помещении, с целью обогащения посредством персонального компьютера с (не указанного) сайта в сети «Интернет» осуществил копирование приложения «Компас 3D» на внешний жесткий диск модулей, для дальнейшего хранения, сбыта и незаконного сбыта путем предоставления внешнего жесткого диска с указанным программным продуктом и последующей установки на ПК. В результате незаконного использования программного продукта, обвиняемый нарушил авторские права ООО «Аскон» причинив вред в размере 1 230 600.[2]

К пятой группе преступлений относятся противоправные деяния, совершаемые посредством компьютерных сетей, представляющие из себя акты экстремизма, расизма (ч. 2 ст.280 УК РФ).

---

[1] Приговор Калужского районного суда Калужской области от 25 ноября 2019 по делу № 1-1084/2019. URL: //sudact.ru/regular/doc/sOj2ljzYGvr5/ (дата обращения: 17.01.2021)

[2] Приговор Комсомольского районного суда г. Тольятти Самарской области от 21 июля 2020 по делу №1-278/2020. URL: //sudact.ru/regular/doc/zn9pbUgYsooY/ (дата обращения: 17.01.2021)

Киселевским городским судом Кемеровской области был вынесен приговор от 27.07.2020 г. под №1-310/2020где было установлено, что обвиняемый в июне 2017 г. зарегистрировался на сайте в сети «Интернет» где и получил возможность размещать любые сведения. Имея личную неприязнь к представителям Федеральной службы исполнения наказания РФ, находясь у себя дома, у обвиняемого возник преступный умысел, направленный на совершение публичных призывов неограниченного круга лиц к экстремисткой деятельности, путем размещения текстовых сообщений на указанном сайте при помощи смартфона.

Представленная Конвенцией классификация является далеко не единственной, помимо нее в рамках отечественной криминалистической доктрины существуют иные подходы. Исследование вопросов криминалистической классификации проводили В.А. Голубев, В.В. Крылов, В.А. Мещеряков, В.Н. Черкасов, В.Б. Вехов, А.Л. Осипенко, Д.А. Илюшин, и другие ученные.

А.Н. Яковлев и Н.В. Олиндер приводят свою криминалистическую классификацию преступлений,которые совершаются с использованием электронных средств и платежей. Вышеуказанные ученые подразделяют криминалистическую классификацию по следующим элементам: по объекту, предмету преступного посягательства, количеству субъектов, по признаку территориальности и способу совершения.

По объекту преступного посягательства преступления, совершённые с использованием электронных платёжных средств и систем, они подразделяют на преступления:

1. против собственности совершенные с использованием электронных платежных средств и систем: а) мошенничество; б) кража;

2. в сфере экономической деятельности, где используются преимущественно электронные платёжные средства и системы: а) легализация доходов, которые были получены в результате совершения

преступных действий; б) незаконная деятельность в предпринимательской сфере.

3. в сфере компьютерной информации: а) неправомерный доступ к компьютерной информации, являющейся информационным объектом электронных платёжных систем: б) создание, использование и распространение вредоносных программ, предназначенных для осуществления неправомерных действий в электронных платёжных системах или с электронными платёжными средствами;

4. с использованием электронных платёжных средств и систем против государственной власти, интересов государственной службы и службы в органах местного самоуправления.

По предмету преступного посягательства подразделяются: а) имеющие материальный предмет посягательства; б) не имеющие материального предмета посягательства.

По количеству субъектов, преступления, совершенные одним лицом или группой лиц.

По способу совершения: а) злоупотребление уязвимостью электронной платёжной системы без неправомерного применения реквизитов доступа легального пользователя; б) неправомерное использование реквизитов доступа легального пользователя электронной платёжной системы.[1]

Д.А. Ильюшин разработал криминалистическую классификацию интернет преступлений по способам совершения и криминальным целям, которые включают в себя:[2]

1) Неправомерное подключение к информационно-телекоммуникационной сети Интернет: а) неправомерное получение и использование чужих учётных данных (логинов и паролей) с целью получения доступа в сеть Интернет; б) частичная подмена учётных данных

---

[1] Яковлев А. Н. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем: научно-методическое пособие. М., 2012. С 80-81.

[2] Илюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: Дис. … канд. юрид. наук: Волгоград, 2008. С. 87 – 88.

(МАСиIРадреса) с целью неправомерного доступа в сеть Интернет; неправомерное подключение к сети оператора электросвязи с целью уклонения от оплаты полученных услуг Интернет.

2) Создание, использование и распространение для ЭВМ сетевых вредоносных программ.

3) Незаконные изготовление, хранение, распространение, рекламирование и (или) публичная демонстрация информации, запрещённой к свободному обороту, совершённые с использованием сети Интернет: а) незаконное изготовление, хранение, распространение, рекламирование и (или) публичная демонстрация порнографических материалов, совершённые с использованием сети Интернет; б) незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, совершённое с использованием сети Интернет; в) нарушение тайны переписки, телефонных переговоров, почтовых или иных сообщений, передаваемых по сети Интернет; г) незаконное собирание или распространение информации о частной жизни лица, составляющей его личную или семейную тайну, в том числе персональных данных, совершённые с использованием сети Интернет; д) оскорбление, нанесённое путём распространения порочащих сведений в информационных ресурсах сети Интернет; е) возбуждение ненависти либо вражды, а равно унижение человеческого достоинства, совершённые с использованием сети Интернет.

4) Нарушение авторских и смежных прав, а также незаконное использование чужого товарного знака, совершённые с использованием сети Интернет.

5) Мошенничество, совершаемое в сфере предоставления услуг Интернет: а) продажа фиктивных услуг, несуществующих товаров и предложение фиктивной надомной работы, совершённые с использованием Интернет-магазинов или рекламных электронных сообщений; б) привлечение средств на ложную благотворительность; в) мошенничество в электронных платёжно-расчётных системах сети Интернет; г)

мошенничество в интернет-казино, букмекерских конторах (на тотализаторах), в розыгрышах лотереи и на аукционах; д)мошенничество, совершённое с использованием фиктивных брачных Интернет-агентств; е) создание финансовых «Интернет-пирамид».

6) Хищение электронных реквизитов и сбыт поддельных кредитных либо расчётных карт.

7) Незаконное предпринимательство в сфере предоставления услуг Интернет.

8) Вымогательство, совершённое с использованием сети Интернет.

9) Кибертерроризм.

Используя методологический подход Ю.М. Батурина В.Б. Вехов выделяет 5 основных групп компьютерных преступлений:1) Изъятие средств компьютерной техники; 2) перехват информации; 3) несанкционированный доступ средствам компьютерной техники; 4) манипуляция данными и управляющими командами; 5) комплексные методы. Под комплексным методом понимаются использование преступником двух и более способов указанных ранее групп.[1]

Д.В. Пашнев предлагает следующую криминалистическую классификацию по критерию средств совершения преступлений и преследуемой криминальной цели.

1) Преступления где компьютерные технологии (по критерию цели) выступают в качестве: а) основной цели преступления (уничтожение, искажение, искажение, блокирование, нарушение установленного порядка маршрутизации компьютерной информации, существенное нарушение порядка ЭВМ, их системы и сети); б) промежуточной цели (по средством ране указанных действий на компьютерные технологии достигает иная цель):

[1]Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия. Право и Закон. М.,1996. С. 34.

2) Преступления где компьютерные технологии (по критерию средства) выступают в качестве: а) автоматизированного средства противоправного деяния (фальшивомонетничество, подделка документов, печатей, штампов, бланков, ценных бумаг, знаков почтовой оплаты и проездных билетов, марок акцизного сбора или контрольных марок, распространение незаконной информации, заведомо ложное сообщение об угрозе безопасности граждан, уничтожения или повреждения объектов собственности, сводничество); б) средства информационного обеспечения совершения преступления (незаконный сбор и систематизация информации, ведение «чёрной» бухгалтерии, ведение баз данных по распространению предметов, находящихся в ограниченном обороте, – наркотиков, оружия и СКТ для занятия сутенёрством, переписка по электронной почте).[1]

В.А. Мещеряков предлагает свою классификацию преступлений в сфере компьютерных технологий по видам.[2]

1. Уничтожение компьютерной информации.

2. Неправомерное завладение компьютерной информацией или нарушение исключительного права на её использование: а) неправомерное завладение компьютерной информацией как совокупностью сведений, документов – нарушение исключительного права владения; б) неправомерное завладение компьютерной информацией как алгоритмом (методом) её преобразования; в) неправомерное завладение компьютерной информацией как товаром.

3. Действия или бездействие по созданию (генерации) компьютерной информации с заданными свойствами: а) распространение по телекоммуникационным каналам информационно-вычислительных сетей компьютерной информации, наносящей ущерб абонентам; б) разработка и

---

[1] Пашнев Д. В. Криминалистическая классификация преступлений, совершаемых с использованием компьютерной техники. Доля. Симферополь, 2004. С. 164 – 166.

[2] Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: Дис. … д-ра юрид. наук. Воронеж, 2001. С. 70-77.

распространение компьютерных вирусов и прочих вредоносных программ для ЭВМ.

4. Неправомерная модификация компьютерной информации: а) неправомерная модификация компьютерной информации как совокупности фактов, сведений; б) неправомерная модификация компьютерной информации как алгоритма; в) неправомерная модификация компьютерной информации как товара с целью воспользоваться её полезными свойствам.

Классификация, указанная выше, а также другие, которые относятся к такой же категории – некая предпосылка, помогающая в разработке средств, задач и методов преступлений (например, таких, как методы исследования и обнаружения материальных объектов, а также различные специально разработанные технические средства). Чтобы облегчить процесс воспроизведения и реализации методик расследования преступлений, следует учитывать тот факт, что криминалистическая классификация киберпреступлений должна служить основой единой криминалистической характеристики киберпреступлений.

Важность данной классификации объясняется ее логическим содержанием, который помогает выдвигать и практически применять различные комплексы типичных следственных действий по уголовному делу. Данный факт гарантирует всесторонность и полноценный объем информации при расследовании преступлений, которые относятся к определенной категории. Таким образом, из вышеперечисленного следует вывод о том, что актуальной научной задачей представляется дальнейшая разработка теоретических основ криминалистической классификации. Актуальность данной задачи объясняется тем, что возрастает потребность в криминалистической практике, совмещенной с теорией выявления преступлений данной категории.

1.3 Криминалистическая характеристика киберпреступлений

Криминалистическая характеристика киберпреступлений это система взаимосвязанных обобщенных данных о наиболее типичных признаках, проявляющихся в способе и механизме киберпреступлений, обстановке его совершения, личности убийцы и др., сведения о которых важны для практического решения задач расследования.

В основе криминалистической характеристики киберпреступлений лежат объективные процессы совершения и сокрытия данной категории преступлений, определяющие закономерности отражения признаков содеянного в реальности.

В криминалистической характеристике выделяют различные элементы, такие как способ совершения преступления, особенности обстановки совершения преступления, личностная характеристика преступника, особенности непосредственного предмета преступного посягательства. особенности следовой информации,

По вопросу о способах совершения киберпреступлений встречается много различных мнений, но несмотря на это можно выделить две главные группы, где в первую группу входят способы с непосредственным воздействием (проникновение в систему ПК и введение команд), а ко второй группе относятся способы удаленного воздействия (использование вредоносных программ для удаленного доступа к информации).

И.О. Морар приводит свою классификацию компьютерных преступлений, которая основывается на своеобразии способ совершения: 1) способы для получения доступа к информации, находящейся на машинных носителях (телефоны, пейджеры, аппаратные устройства компьютерного типа); 2) способы с использованием компьютерных техник и средств коммуникации в качестве орудий и средств совершения (сокрытия) преступлений; 3) способы с применением высокотехнологичных устройств с

целью незаконного доступа к компьютерной информации, ее модификации и блокирования.[1]

В общем понимании киберпреступления охватывают наибольший спектр устройств используемых в совершении преступлений. Было бы целесообразней разделять устройства на малогабаритные (телефон, ноутбук) и крупногабаритные (ПК, суперкомпьютер, сервер), которые могут разделять на стационарные и нестационарные.

Следует согласиться с распределением , предложеннымВехов В.Б. и Зуев В.Б., которые группируют следующим образом: 1) непосредственный доступ к электронным носителям и средствам компьютерной техники, содержащей в своей памяти компьютерную информацию; 2) дистанционный доступ к электронным носителям и охраняемой законом компьютерной информации; 3) фальсификация входных и выходных данных и управляющих команд; 4) внесение изменений в существующие программы для ЭВМ и иную компьютерную информацию, которая в результате становится вредоносной; 5) создание, использование и распространение вредоносных программ, в том числе с использованием вредоносных компьютерных сетей; 6) комплексные способы.[2]

Данные позиции полно отражают способы совершения киберпренступлений.

Как отмечает Поляков В.В.: «в обстановку совершения преступления включается объекты, процессы и явления, характеризующие время, место, вещественные и иные условия окружающей среды, поведения участников, косвенно связанных с преступлением, а также иные факторы, которые определяют возможность, условия и обстоятельства совершения преступления. Общие знания об обстановке совершения преступления,

---

[1]Морар И.О. Могут ли в рамках науки криминологии рассматриваться способы совершения компьютерных преступлений и их последствия. Российский следователь. 2012. № 12. С. 37 – 41.

[2]Вехов В.Б., Зуев С.В. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов. Изд-во Юрайт. М., 2021. С. 40-41

которые взаимосвязаны с другими элементами криминалистической характеристики, позволяют обратить внимание следствия на поиск и установления обстоятельств, входящих в предмет доказывания».[1]

Д.А. Ильюшин к элементам обстановки совершения преступления относятся: вещественные, пространственные, временные, производственно-бытовые, программно-технические, поведенческо-технические, психологические меры защиты. Помимо этого, зачастую общественно-опасные последствия наступают не вместе совершения преступления.

Также В.Е. Козлов к элементам обстановки совершения киберпреступлений относит: 1) место и время действия преступника; 2) особенности компьютеризации субъекта хозяйствования; 3) особенности организации информационной безопасности; 4) возможности нарушения компьютерной информации и безопасности компьютерной системы без непосредственного участия человека; 5) уровень классификации специалистов, обеспечивающих защиту информации, а также администрирование компьютеров и их сетей.

По мнению ряда, ученых специфичной особенностью обстановки совершения киберпреступлений, является то, что они совершаются в киберпространстве, где злоумышленники имеют возможность задействовать несколько технологических средств для достижения одной цели, причем данные средства могут находится в разных местах.

Так Е.С. Шевченко провела анкетирование среди следователей, результаты которого свидетельствуют об испытываемых трудностях не только с использованием терминологии, но и при применении норм, обеспечивающих практическое определение места совершения преступления и места производства его расследования. Злоумышленник может совершить преступление за тысячи километров от места наступления последствий. Местом совершения может считаться как любое здание, место на улице,

[1] Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики. Известия АГУ. 2013. № 2-1 (78). С. 115.

транспортное средство в том числе находящиеся в иностранном государстве, что делает невозможным произвести определенный спектр следственных действия для фиксации следов преступления.

Стоит согласится с точкой зрения Е.С. Шевченко о том, что обстановкой совершения преступления является киберпространство, под которым онаопределяет, «область взаимодействия информационных систем различного уровня, включающий следующие элементы: компьютерные системы, сети (как глобальные, так и локальные), компьютерные программы пользователей, а также данные, циркулирующие в перечисленных элементах».

А.Л. Осипенко выделяет следующие характеризующие особенности преступлений, совершаемые в киберпространстве: 1) высокая степень скрытности совершения преступления; 2) трансграничный характер; 3) интеллектуальный характер преступной деятельности; 4) нестандартность, сложность, многообразие и динамичное обновления способов совершения преступления и специальных средств; 5) автоматизированный режим совершения преступления и многоэпизодичный характер противоправных действий; 6) неосведомленность потерпевших о том, что подверглись преступному посягательству; 7) дистанционный характер.[1]

На киберпреступников сильно влияет обстановка, поэтому в большинстве случаев злоумышленники основательно подготавливаются к совершению преступления. Задачей киберпреступника является адаптация и внедрение в коммуникационные сети, поэтому он собирает и изучает необходимую информацию о технологиях, средствах защиты и их характеристиках.

В результате совершения преступления в киберпрестранстве могут оставаться характерные изменения в виде электронно-цифровых следов. Но

[1] Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы: Монография. Омск. акад. МВД России. Омск, 2009. С. 109 – 110.

следует отметить, что любые изменения могут остаться практически незаметными.

Низкая информационная безопасность как частная, так и корпоративная во многом способствует киберпреступлениям. В.В. Поляков отмечает такой фактор «косвенным образом способствует противоправной деятельности преступников недостаточный уровень квалификации правоохранительных органов в области расследования киберпреступлений».[1]

Что касается непосредственно личности преступника, являющегося элементом криминалистической характеристики киберпреступлений, то здесь следует говорить о сведениях, которые характеризуют его социально-демографические, социальные, психические и психологические стороны. Подобные данные свидетельствуют о поле, возрасте, образовании, социальном положении и гражданстве, а также профессиональной деятельности определенного лица. К этим же категориям следует относить информацию о прошлых судимостях, его типе темперамента и характера. Следовательно, это будет способствовать определению мотивов и целей совершения преступлений данным лицом.

Существует множество классификаций лиц, совершающих киберпреступления.

А.В. Кузнецов разделяет преступников на три группы: 1) лица с устойчивым сочетанием профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма, и изобретательности, они воспринимают технические средства как вызов их творческим и профессиональным знаниям, умениям и навыкам; 2) лица страдающие новыми видами психических заболеваний – информационными или компьютерными фобиями; 3) лица являющиеся профессиональными

[1] Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики. С. 116.

преступниками в данной сфере, имеют ярко выраженные корыстные мотивы.[1]

Автор подразумевает, что субъектом преступления может быть абсолютно любой человек обладающий базовыми знаниями в технологической сфере, не являясь при этом высококвалифицированным специалистом.

В данной категории преступлений больше всего преобладает корыстная цель совершения преступлений, выражающиеся в кражах, реализации похищенного программного обеспечения и др. Однако также возможны преступлений из хулиганских побуждений, когда лицо имеет цель лишь нанесения вреда.[2]

А.Н. Косенков и Г.А. Чернов в зависимости от мотивации выделяют следующие типы киберпреступников: 1) корыстный тип, характерен для обыкновенного преступник, который имеет целью надивиться за счет чужого имущества; 2) насильственный тип, не смотря на отсутствие физического контакта лицо способно воздействовать психологически на живую цель посредством электронных устройств; 3) сексуальный тип, характерен для лиц которые распространяют порнографические материалы или предметы, понуждают к действиям сексуального характера, осуществляют развратные действия; 4) социально-дезорганизующий тип, основной целью является нарушение законодательно закрепленных социальных норм, негативно влияют на общественные отношения; 5) статусный тип, стремятся получить высокий неформальный социальный статус за счет совершенного преступления, в киберпространстве статусность может иметь важное значение в качестве мотива; 6) исследовательский тип, характерно изучение программных и аппаратных составляющих электронных устройств и их

---

[1] Кузнецов А. В. Некоторые вопросы расследования преступлений в сфере компьютерной информации. Информационный бюллетень следственного комитета МВД РФ. М., 1998. № 2. С. 42-48.

[2] Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. Горячая линия-Телеком М., 2002. С. 161.

сетей, пытаются найти уязвимости с целью дальнейшего использования или устранения.[1]

Интересное мнение высказал ОрлиТургеман-Голдшмита «Свою деятельность и цели киберпреступники истолковывают по- разному. Все они характеризую себя как положительные и экстраординарные личности, которые являются носителями социальных изменений и демонстрируют лучшее поведение, а вину за свои преступные действия не ощущают».[2]

Н.Н. Федотов также описал образы киберпреступников: 1) хакер, основной мотив данного преступника является исследовательский интерес, честолюбие, желание показать свои возможности. Сложные компьютерные системы воспринимаются как вызов. Могут иметь как высокие так и средние знания в сфере ИТ; 2) инсайдер, самый распространенный тип киберпреступника, с невысоким знанием уровнем знаний в сфере ИТ. В силу служебного положения (сотрудник компании) имеет доступ в информационную систему; 3) белый воротничок, «заядлый казнокрад» компьютерные системы выступают в качестве нового инструмента преступной деятельности, для данного типа характерны следующие виды преступлений хищение средств, взяточничество, коммерческий подкуп, продажа информации; 4) «Е-бизнесмены», как правило лица не являются квалифицированными специалистами в ИТ сфере и не имеют служебного положения, совершают правонарушения ради выгоды, которая связана со сложной организацией или техническим обеспечением, данный тип отличается хорошими способностями в предпринимательской сфере, для них характерны «кардинг» и «фишинг»; 5) антисоциальный тип, социопаты, т.е.

---

[1] Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника. Криминологический журнал БГУЭП. 2012. № 3 (21). С.87 - 94

[2]OrlyTurgeman–Goldschmidt. Meanings that Hackers Assign to their Being a Hacker. Copyright. Israel, 2008. Vol. 2 (2) С. 382-
396 URL: http://www.cybercrimejournal.com/Orlyijccdec2008.pdf (дата обращения 02.02.2021).

патологически тянет к данному роду деятельности, не способны к планированию поэтому действуют импульсивно.[1]

Е.С. Шевченко в зависимости от локализации преступной деятельности определяет три группы киберпреступников: 1) ведущие основную преступную деятельность только в киберпространстве; 2) ведущие преступную деятельность в равной степени как в реальной действительности, так и в киберпространстве; 3) лица ранее совершившие преступления не относящемуся к киберпреступленям, и совершающие киберпреступления в настоящее время.

Стоит отметить, что в ходе расследования киберпреступления отсутствие достаточного количества материальных следов преступника, разнообразия возможных мотивов и невозможность установления определенного круга лиц, которые могли совершить, обусловливает необходимость применения юридической психологии. Данные выработанные классификации могут быть положены в основу концепции предупреждения и профилактики кибепреступлений, использована в разработке методик и расследования преступлений.

Следующим элементом криминалистической характеристики является предмет преступного посягательства. Под предметом преступного посягательства понимается стоимостная оценка определенной вещи материального мира, воздействуя на которую причиняется вред объекту преступного посягательства.

В большинстве научныхработ в качестве предмета преступного посягательства выделяется «компьютерная информация» или «информация» в целом, которая имеет определенную материальную ценность.

Применительно к процессу доказывания под компьютерной информацией понимаются фактические данные, обработанные средствами системы и (или) передающиеся по телекоммуникационным каналам,

---

[1] Федотов Н. Н. Форензика – компьютерная криминалистика. Юридический мир. М., 2007. С. 254 – 255.

доступные для восприятия человеком, на основе которых устанавливаются имеющие значение для уголовного дела обстоятельства. Источниками информации могут быть различные файлы, листинги или машинные распеб́чатки, данные на электронных носителях, пластиковых банковских картах, флэш-картах и др. [1]

Согласно соглашению «О сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации компьютерная информация на машинном носителе в электронно-вычислительной машине, их системе или сети. Исходя из данного определения следует вывод, что компьютерной является любая информация, содержащаяся на электронном материальном носителе.[2]

Также выделяются следующие признаки информации: объёмная, быстро обрабатывается, легко уничтожается, не материальна и может находится только на электронном (машинном) носителе, различные операции совершаются посредством высокотехнологичных средств, легко передается по телекоммуникационным каналам.

Исходя из смысла понятия имеется необходимость совершенствовании понятийного аппарата так, как термин «электронно-вычислительная машина» утратило свою актуальность в силу научно технического прогресса и имеет мало чего общего с современной реальностью борьбы с киберпреступлениями и мобильными коммуникациями.

Немаловажным и специфичным элементом криминалистической характеристики выступает следовая информация о совершенном преступлении. Данный элемент будет подробно рассмотрен в следующем параграфе.

---

[1] Васильев А. А.; Дёмин К. Е. Электронные носители данных как источники получения криминалистически значимой информации. С. 47.

[2] О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: федеральный закон от 01.10.2008 № 164-ФЗ. Собрание законодательства РФ. – 06.10.2008. № 40. Ст. 4499.

1.4 Следы в киберпреступлениях: понятие, классификация и механизм образования

В настоящий момент ученые-криминалисты не выделили единое понятие и определение следов, возникающих в результате киберпреступлений. Так, например, ряд авторов В.А. Мещеряков, А.Ю. Головин, А.Б. Смушкин, В.Ю. Агибалов склоняются к термину виртуальный след, В.В. Борисов, Г.М. Шаповалова предлагают название «информационный след, В.Б. Вехов, А.В. Шебалин, В.В. Поляков оперируют понятием «электронно-цифровой след».

В.А. Мещеряков предлагает понятие «виртуальные следы» под которыми понимает, «связанное с событием преступления, любое изменение в состоянии автоматизированной информационной системы, представленной в виде информации и зафиксированное на материальном носителе».[1]

А.Ю. Головин придерживается схожего подхода к понятию следов, так он под «виртуальными следами понимает, «зафиксированное в виде цифрового образа формальной модели изменение состояния информации в памяти абонентных устройств, вызванное алгоритмом установленного программного обеспечения и связанное с событием преступления».[2]

В.Б. Вехов критикуя использование понятия «виртуальный след», указывает на этимологию слова «виртуальный». По его мнению, «оно происходит от латинского слова «virtualis», что подразумевает отсутствие физического воплощения или воспринимаемый иначе, чем реализован в действительности». Таким образом, вопрос об использовании данного термина является дискуссионным.

Так же В.В. Борисов выдвигает неоднозначную трактовку «информационный след», по его мнению, информационный след имеется на

---

[1] Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Издательство Воронежского государственного университета. Воронеж, 2002. С.94 – 119.

[2] Давыдов В. О., Головин А. Ю. Значение виртуальных следов в расследовании преступлений экстремистского характера. Известия Тульского государственного университета. Экономические и юридические науки. Тула, 2016. № 3. С. 254-259.

компьютерном оборудовании подозреваемых в совершении преступления.[1] Стоит отметить, что данная позиция является узконаправленной поэтому является не совсем правильной. Так как, хоть и компьютерное оборудование является комплексным, но все же не включает в себя перечень всех объектов, где способен образоваться след, а также информационный след может отразиться у потерпевшего, свидетеля, иных лиц и на просторах сети «Интернет», а не только на компьютерном оборудовании преступника.

Поэтому с точки зрения теории криминалистики и практики сформулированная позиция В.В. Борисовым и Г.М. Шаповаловой не отражает необходимое ценностное содержание и не характеризует в полной мере данный вид следов.

В.Б. Вехов предлагает понятие «электронно-цифровой след» определяя его как «любая криминалистическая значимая компьютерная информация т.е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных воздействий либо передающиеся по каналам связи посредством электромагнитных сигналов».[2]Данное определение дает наиболее общее представление о следе, но следует отметить, что использование термина компьютерная информация придает узкое значения смыслу данного определения, так как информация (данные и сведения) замыкаются в рамках компьютера. На наш взгляд, чтобы отразить полное смысловое значение, следует использовать термин «информация» в широком смысле.

Так же справедливо отметила А.Н. Колычева, которая согласилась с подходом к определению данным В.Б. Веховым, но внесла свои корректировки по причине «синонимического дублирования». Так под «электронно-цифровым следом» она подразумевает «криминалистически значимая информация, выраженная посредством электромагнитного

[1] Борисов В.В. Об особенностях фиксации информационных следов в практике защиты информации. Известия Южного федерального университета. Технические науки. М., 2009. №5. С. 164 - 168.

[2]Вехов В. Б. Электронные следы в системе криминалистики. Судебная экспертиза. Волгоград. 2016. Вып. 2. С. 100-101

взаимодействия или сигналов в форме, пригодной для обработки с использованием компьютерной техники, в результате создания определенного набора двоичного кода на материальном носителе, либо его преобразование, выразившееся в модификации, копировании, удалении, блокировании»[1].

Исходя из вышеизложенных позиций авторов, необходимо систематизировать весь объем признаков присущие следам возникших в результате киберпреступлений, и дать определение в узком и широком смысле.

Под электронно-цифровым следом в узком смысле следует понимать криминаличтиески значимую информацию, выражаемуючерез электромагнитныевзаимодействия или сигналы в форме, которая будет пригодна для обработки посредством использования любого вида технологии, в результате создания двоичного кода на материальном носителе, либо его преобразование, выразившееся в модификации, копировании, удалении, блокировании и др. процессах.

В широком смысле под электронно-цифровом следе понимается, криминалистически значимая информация, образованная в киберпространстве в результате человеческой деятельности.

Так же в настоящее время вопрос о классификации следов, возникающих в киберпространстве, является не менее спорным и значимым, чем вопрос о сущности самого понятия и определения. Значимость классификации проявляется в том, что она позволяет систематизировать накопленные знания и тем самым определить особенности отдельных видов следов, сформировать методические рекомендации по работе с ними, а также выявить типичные проблемы, которые могут выявиться в работе со следами при расследовании уголовных дел.

---

[1]Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: автореф. канд. юрид. наук. М., 2019. С. 10.

К классификации данной категории следов существует множество подходов, предложенные учеными криминалистами такими как: В.А. Мещеряковым, А.Г. Волеволдз, В.Е. Козловым, А.Ю, Семеновым, Л.Б. Красновой, В.П. Леонтьевым, А.Б. Смушкиным, В.Б. Веховым.

В трасологии традиционно сложилась общая классификация всех следов на материальные и идеальные. С появлением электронно-цифровых следов в научных кругах появились споры к какому же виду относить данный след.

Так В.А. Мещеряков полагает, что данная категория следов относится к материальным, аргументируя их существованием на определённом материальном носителе при их обнаружении, а после и изъятии при помощи программно-технических средств. Из этого следует вывод, что непосредственно восприниматься данные объекты не могут. [1]

Данное мнение является не совсем правильным так как данная категория следов зависит от способа считывания и не воспринимается человеком с помощью органов чувств.

Необходимо отметить, что было бы ошибочным относить электронно-цифровые следы к идеальным следам, так как они существую не в памяти человека, а в памяти устройства.

Интересную позицию выделяют В.Б. Вехов, В.В. Крылов, А.Н. Колычева, А.Б. Нехорошев[2], которые считают, что электронно-цифровые следы следует относить к невидимым материальным следам, аргументируя тем, что данную информация можно преобразовать с помощью технических средств для восприятия человеком с помощью органов чувств. В сравнении с типичными параметрами присущие идеальным следам, электронно-

---

[1] Мещеряков В. А. Следы преступлений в сфере высоких технологий. Библиотека криминалиста. 2013. № 5 (10). С. 265 – 269

[2] См., например, Нехорошев А.Б. Компьютерные преступления: квалификация, расследование, экспертиза. Саратов, 2004. Ч. 2. С. 61-65; Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет С. 10; Вехов В.Б. Электронные следы в системе криминалистики №2. С. 17.

цифровые следы обладают определенные характеристики (объем, формат, и т.д.).

Также Р.А. Дерюгина, А.А. Жижелева считает, что данная категория следов не может относится ни к материальным, ни к идеальным, так как не обладают определенными признаками следов присущие каждой из этих видов. Поэтому, они выделяют «промежуточную».[1]

Данная позиция является наиболее подходящей к электронно-цифровым следам, так как данную категорию нельзя отнести к материальным и идеальным следам, в силу специфичности следовой картины.

Также существуют мнения разделении следов данной категории преступлений по различным основаниям.

С.Ю. Скобелин и Ю.Л Соловьева разделяет классификацию цифровых следов по следующим основаниям: 1) по видам преступной деятельности: а) следы преступлений, предусмотренных главой 28 УК РФ, б) следы преступления совершенные с использованием сети Интернет (сбыт наркотиков, развратные действия, доведение до самоубийства, мошенничество, азартные игры, и т. д.), б) следы любых преступных деяний (в т. ч. неосторожных); 2) в зависимости от места их обнаружения: а) обнаруженные в мобильных цифровых устройствах (подразумевая малогабаритные устройствах подлежащих постоянному перемещению, например смартфон), б) стационарных устройствах (понимая под ними устройства предназначенные для статического использования в силу их предназначения или крупного размера предмета, например персональный компьютер), в) в устройствах смешанного типа (устройства которые совмещают в себе признаки первого и второго типа, например ноутбук); 3) по значимости для раскрытия преступления: а) непосредственно уличающие лицо, б) ориентирующие и направляющие ход расследования; 4) в

[1]Дерюгин Р. А. Перспективы развития цифровой криминалистики в условиях информационного общества. Технологии XXI века в юриспруденции : Материалы Всероссийской научно-практической конференции. Екатеринбург, 2019. С. 40-46.

зависимости от решаемых следствием целей: а) позволяющие проверить местонахождение принадлежавшее лицу устройства, б) позволяющие получить информацию о готовящемся, совершаемом или скрываемом преступлений, а также иных сведений о преступлений.[1]

Недостаток данной классификации заключается в том, что авторами не учитывался научно-технический прогресс из-за которого могут появляется новые виды преступных посягательств, а также технические устройства в которых может отразиться след преступления. Поэтому считаем, что следы стоит разделять в зависимости от цели преступного посягательства: а) уничтожения, б) изменения, в) незаконного вторжения в систему, г) хищения, д) посредственное воздействие и т.д. (открытый перечень), что касаемо места обнаружения следов предлагаем разделить их на две большие группы: а) следы, обнаруженные на стационарных предметах и объектах, б) следы, обнаруженные на не стационарных предметах и объектах, а каждую из данных подкатегорий разделить на малогабаритные и крупного габаритные предметы и объекты. Данные изменения имеют широкое смысловое значение и тем самым позволяют в дальнейшем дополнять данную классификацию.

В результате анализа научных работа В.Б. Вехова и В.В. Крылова, А.О. Сукманов подразделяет электронно-цифровые следы на следующие виды: 1) «следы-предметы» машинные носители информации, различные технические устройства, микросхемы, микроконтроллеры, компьютерные системы; 2) «следы-отображения»: электромагнитные сигналы, компьютерные программы, базы данных, электронные сообщения, электронные страницы на устройствах и их сетей и т.д.[2]

А.Г. Волеводз различает локальные (под которыми понимаются следы, возникающие на устройствах преступника и жертвы) и сетевые следы (под которыми понимались следы, возникающие в серверах и коммуникационных

---

[1] Соловьева Ю.Л. Скобелин С.Ю. Классификация цифровых следов преступлений. БЮИ МВД России. Барнаул, 2021. №2. С. 417 – 418.

[2]Льянов М. М. Современный подход к классификации виртуальных следов. Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 4(30). С. 47-55.

оборудованиях). На его основании выделяются: 1) следы на жестком диске, магнитной ленте, оптическом диске и т.д.; 2) следы, сохраняющиеся в ОЗУ компьютерных технологий; 3) следы в ОЗУ периферийных устройствах (принтер, факс); 4) следы в ОЗУ связи и сетевых компьютерных устройствах; 5) следы в электромагнитных, радиооптических системах и сетях связи.[1]

В.Ю. Агибалов комментируя данную классификацию, отмечает что ее существенным недостатком является то, что она основывается на размещении криминалистически значимой информации и совершенно не учитывала особенности сложность и многоэтапность следообразования.

Дополнил данную классификацию А. Ю. Семенов по их расположению на две группы:[2] 1) следы на компьютере преступника; 2) следы на компьютере жертвы: таблица расширения файлов, системный реестр, отдельные кластеры магнитного носителя информации (жесткий диск, дискета, в которых записываются фрагменты программ и файлов конфигурации), папки и каталоги хранения электронной почты и так далее.

В.Е. Козлов предложил свою классификацию следов в преступлениях в сфере информационных технологиях. Он отметил, что в процессе образования, словообразующим объектом выступает специфический «виртуальный объект» - система команд ЭВМ, тем самым предлагает классифицировать по следующим основаниям: 1) по характеру изменений (структурные файловые следы и внешние файловые следы); 2) по степени завершенности обработки процесса команд (стабильные и временные файловые следы); 3) по размещению (локальные и сетевые).[3]

В.Ю. Агибалов не соглашается с утверждением, что система команд ЭВМ является виртуальным объектом, так как считает систему команд

---

[1]Волеводз, А.Г. Противодействие компьютерным преступлениям.Юрлитинформ. М., 2002. С. 159 - 160.

[2] Семенов А.Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации. Сибирский юридический вестник. 2004. № 1. С. 53 – 55.

[3] Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. С. 156

«выступает в роли формализованной математической модели обработки информации».[1]

В.В. Казанцев обратил внимание на особенности «следообразующего воздействия» и выделил характерные для преступлений в сфере компьютерной информации следующие группы следов:[2]1) не входящие в стандартный состав системы, программы и текстовые файлы включая их части, которые функционировали на устройстве до совершения преступления: 2) содержащие в программах системы, документах иных файлах команды, знаки, символы и др., которые были внесены в систему преступником для изменения работы системы; 3) записи в учетных файлах системы (log-файлы), в которых содержится информация о пользователях, которые когда-либо использовали данное устройство.

В.Ю. Агибалов считает, что данная классификация имеет ряд недостатков. Во-первых, она не имеет четкого основания для классификации. Во-вторых, она является не полной, и существуют множество материальных реальных цифровых следов, которые не попадают в данную классификацию.[3]

Перечислять различные мнения о классификации следов данной категории преступлений можно бесконечно, но следует отметить что вышеперечисленные позиции и их комментариями могут иметь немалое значения для выработки методических рекомендации по расследованию киберперступлений.

В.Б. Веховсчитая, что «научные знания об механизме образования данной группы следов являются размытыми. фрагментарными и системными». Предложил обобщить и систематизировать эти знания в рамках криминалистического исследования компьютерной информации.[4]

---

[1]Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе. Юрлитинформ. М., 2012. С. 42.

[2] Казанцев В.В. Криминалистическое исследование средств компьютерных технологий и программных продуктов: учебно-практическое пособие. Терра линк. Алматы, 2003. С. 50.

[3]Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе. С. 43.

[4]Вехов В. Б. Электронные следы в системе криминалистики. С.60

Полагая, что «основу механизма следообразования при совершении компьютерных преступлений, всегда составляет электромагнитные взаимодействия». При этом между следообразующим и следовоспринимающим объектом отсутствует механический контакт, поскольку внутренние свойства изменяются с помощью электромагнитных сигналов и полей, имеющие свою признаки (частота, напряженность, направленность, и т.д.). Данные сигналы распространяются в пространстве и передаются по каналам электросвязи, фиксируются на различных носителях по определенным правилам, обусловленным системой кодирования данных.

Механизм воздействия одного объекта на другой может быть обнаружен по наблюдаемому различию между тремя состояниями:

1) изменение содержания, формата и иных характеристик;

2) изменение алгоритма работы;

3) по автоматически создаваемым программой файлов, которые используются программами и операционными системами для фиксации обработки информации, восстановления или программного обеспечения.

Данные изменения и будут являться следами отображения.

Также В.Б. Вехов выделяет «следообразующие и следовоспринимающие объекты, которыми являются: электромагнитный сигнал, файл, программа для ЭВМ, база данных, электронное сообщение, документ, страница, сайт и т. д.А под следами предметами понимается: машинные носители информации, интегральные микросхемы, микроконтроллеры, системы и сети ЭВМ».[1]

Следует согласиться с данной позицией, так как указывает основной элемент механизма образования электронно-цифрового следа, который является отличительной особенностью образования от других видов следов.

В.Ю. Агибалов считал «для того чтобы устранить недостатки классификаций следов, нужно верно определить критерий, который может

[1]Вехов, В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. ВА МВД России.Волгоград, 2008. С.105.

быть положен в основу конструкции разбиения всех следов на группы и подгруппы», и на его взгляд «результирующим свойством в решающей степени будет зависеть от того, каким образом будет реализована та или иная стадия формирования следовой информации».[1]

Он выделяет 4 стадии (этапы) механизма образования виртуального следа:

1) Физическая реализация свойств следообразующего объекта в окружающей среде, путем проявления звука, изображения, цифрового набора данных, температуры, давления, и др.

Данные физические проявления могут фиксироваться различными техническими средствами, к примеру внешность человека-цифровой фото-видео камерой, звуки – цифровыми звукозаписывающими устройствами и т.д.

2) Преобразование в цифровую форму физических свойств следообразующего объекта (к примеру тепловые датчики, преобразующие температуру в цифровой образ, для дальнейшей передачи информации на экран устройства или компьютер).

3) Предварительная обработка и (или) передача полученной на втором этапе цифровой информации (программа WinRAR, 7-Zip могут служить примерами подобных преобразований информации).

Так же следует указать что последние два этапа могут применяться программы, которые способы сжимать файл с дальнейшей потерей криминалистически значимой информации. К примеру программы для кодирования информации, на CD диск.

4) Стадия записи и хранения полученной на третьем этапе информация. Целью преобразования является приведение ее к виду, обеспечивающему ее надежное и эффективное хранение.

Данный подход к формированию следа позволит привлечь достаточно мощеный формализованный аппарат, используемый при индексировании

[1]Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе. С. 44

полей и записей баз данных. Однако следует сказать, что не каждый электронной-цифровой след формируется через физическое проявление объекта, но и способен формироваться в результате электронных процессов.

С учетом вышеизложенного в данной главе приходим следующим выводам:

1) Целесообразно использовать термин киберпреступление, так как смысловое значение данного понятия позволяет включать найбольший спектр видов преступлений, совершаемый в киберпространстве.

Под «кибербреступлением» следует понимать совершаемое в кибернетическом пространстве виновное, общественно-опасное деяние, посягающее на охраняемые уголовным законом права, свободы и интересы, в котором необходимым элементом механизма преступления является компьютерная информация, выступающая в качестве предмета или средства преступления

2) Постоянно набирающий обороты научно-технический прогресс не позволяет выделить единую классификацию. Но указанные классификации могут использоваться для разработки криминалистической характеристики киберпреступлений.

3) Криминалистическая характеристика киберпреступлений состоит из 4 важных элементов: способы совершения, обстановка совершения, личность киберпреступника, предмет преступного посягательства и следовая информация.

4) Под электронно-цифровым следом в узком смысле следует понимать криминаличтиески значимую информацию, которая выражается посредством электромагнитных взаимодействий или сигналов в форме, пригодной для обработки с использованием любого вида технологии, в результате создания двоичного кода на материальном носителе, либо его преобразование, выразившееся в модификации, копировании, удалении, блокировании и др. процессах.

В широком смысле под электронно-цифровом следе понимается, криминалистически значимая информация, образованная в киберпространстве в результате человеческой деятельности.

5) Основу механизма следообразования при совершении компьютерных преступлений, всегда составляет электромагнитные взаимодействия. Механизм воздействия одного объекта на другой может быть обнаружен по наблюдаемому различию между тремя состояниями:

1. изменение содержания, формата и иных характеристик;

2. изменение алгоритма работы;

3. по автоматически создаваемым программой файлов, которые используются программами и операционными системами для фиксации обработки информации, восстановления или программного обеспечения.

Также можно использовать подход В.Ю. Агибалова в понимании стадийности процесса образования следа.

2 ТАКТИКА ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

2.1 Тактика проведения осмотра места происшествия

На первоначальном этапе расследования киберпреступления основным источником объективной информации является такое следственное действие как смотр места происшествия.

При проведении данного следственного действия у следователя появляется возможность сбора информации о наличии признаков преступления, механизме и обстоятельствах его совершения, с дальнейшей фиксацией обнаруженного.

Осмотр места происшествия при расследовании киберпреступления, производится в целях: 1) обнаружение признаков преступления, фиксация, изъятие и их дальнейшая оценка; 2) путем исследования обнаруженных признаков преступления устанавливаются обстоятельства его совершения (способ, место, время совершения, личность преступника и т. д.); 3) получение информации, которая будет использоваться для построения следственных версий и осуществления оперативно-розыскных мероприятий.[1]

Также Вехов В.Б. к целям осмотра места происшествия при расследовании преступления в сфере компьютерной информации относит: 1) установление места нахождения устройства с помощью которого осуществлялось противоправное деяние, 2) установление лица совершившего преступление, 3) обнаружение, осмотр, изъятие предметов, документов и иной информации, подтверждающей факт осуществления преступных действий, 4) поиск, обнаружение, осмотр и изъятие литературы, методический рекомендаций раскрываемых способ совершения преступления, электронных записей и документов, находящиеся в памяти

[1]Пропастин С. В. Расследование неправомерного доступа к электронной почте. Уголовный процесс. 2017. № 2(146). С. 60-64.

устройств, и содержащих криминалистически значимые сведения, 6) выявление, фиксация, предварительное исследование и изъятие следов по которым можно идентифицировать лиц, прикасавшихся к предметам, 7) обнаружение, осмотр и изъятие документов из автоматизированного системы видеонаблюдения, контроля доступа на место происшествия.[1]

Следует согласиться с позицией Шевченко Е.С. которая отметила, что общей задачей осмотра в первую очередь является установление механизма совершения преступления. Однако тактика осмотра места происшествия по каждому виду киберпреступления будет иметь сою специфику. Так, например, в случае расследования киберпреступлений связанных с порнографическими материалами, общая задача подразделяется на несколько последовательных частей: 1) изучение и фиксация обстановки совершения преступления, 2) установление характера преступного воздействия на общественные отношения и интересы пострадавших лиц; 3) обнаружение, фиксация и изъятие следов, 4) выявление злоумышленника и его мотивов, 5) установление причин и условий, способствующих совершению преступления, 6) получение необходимой информации для осуществления последующих следственных действий.[2]

Главной особенностью киберпреступлений выступает элемент киберпространство, через которое злоумышленник посягает на охраняемые законом права, свободы и интересы. При расследовании следователь сталкивается с проблемой определения места, которое и выступает в качестве отправной точки совершения, так как в киберпространстве не существует географических границ. Так, например, злоумышленник, который намерен похитить денежные средства с чужого лицевого банковского счета, может осуществлять основные действия для достижения данной цели разместившись на любом месте (помещении, улице, парке, транспорте,

[1]Вехов В.Б., Зуев С.В. Расследование преступлений в сфере компьютерной информации и электронных средств платежа. С. 36 – 38.

[2] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений: дис. … кан. юрид. наук. М., 2016 С. 101

другом городе, стране и т.д.). Следователю, в свою очередь, для того, чтобы установить личность злоумышленника следует выполнить ряд следственных действий, отправной точкой является место происшествия. Следует отметить, что в киберпреступлениях не всегда может быть место происшествия, в случае если преступные посягательства был осуществлены без физической реализации злоумышленника. Примером может быть случай возникший в 2015 г., когда осуществлялась крупная атака на мобильные устройства клиентов «Сбербанка». Злоумышленники создали троянский вирус под названием «Android.BankBot.358.origin» и рассылали SMS которые отправлялись от имени пользователей «Avito.ru». Жертве предлагалось перейти по ссылке, чтобы ознакомиться с информацией, при клике по которой адресат попадает на сайт автоматически скачиваемым «apk-файлом», который устанавливается на смартфон. При нажатии на значок приложения показывалась ошибка и значок пропадал. После чего вирус считывал данные мобильного банка \, «мониторил» пользование, и незаметно отправляла информацию злоумышленникам SMS командами.[1]

В приведенном примере, в традиционном криминалистическом понимании, места происшествия нету, так как все основные действия осуществлялись в киберпространстве. Электронно-цифровые следы можно установить посредством осмотра мобильного телефона, объектом которого будет являться данные хранящиеся в системе мобильного устройства.

Существует позиция современных ученных криминалистов, которые считают, что местом происшествия следует считать «киберпространство». [2] Данное суждение является противоречивым, так как киберпространство хоть и является местом где находятся следы преступления, но в традиционном смысле место происшествия, это физически реализованное

---

[1]Вирусные аналитики компании «Доктор Веб» зафиксировали распространение троянца Android.BankBot.358.origin, который нацелен на клиентов Сбербанка. URL: https://news.drweb.ru/show/?lng=ru&i=11802&c=9

[2]Протасевич, А. А. Особенности осмотра места происшествия по делам о киберпреступлениях. Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). 2013. № 2. С. 23.

место, содержащее признаки преступления, которые возможно обнаружить с помощью органов чувств. Как нам известно киберпространство невозможно изучить при помощи технических устройств, а не органов чувств.

Помимо вышесказанного, в киберпреступлениях местом происшествия могут быть различные участки местности где возможно установить или переносить техническое устройство начиная лесной местностью, транспортным средством. парком заканчивая помещением или рядом помещений.

С целью проведения качественного следственного действия следователю следует провести ряд подготовительных мер.

Е.П. Ищенко определила общий перечень подготовительных мероприятий, которые положительно скажутся на результат проведения осмотра места происшествия.[1]

1) Следователь, приняв сообщение, должен уточнить, что и где произошло, при это позаботиться об охране обстановки места происшествия. Для охраны привлекаются работники структуры правоохранительных органов, а также возможно привлечение военных;

2) Дать указание по установлению очевидцев лицам привлеченных к охране места происшествия. Данные сведения могут оказаться полезными в начале осмотра;

3) Если же есть пострадавшие лица (к примеру, в результате кибертерроризма) отдать распоряжение об оказании им помощи;

4) Следует выяснить, были ли приняты меры задержанию подозрительных лиц работниками полиции, а также предотвращены ли последствия произошедшего, если нет, то привлечь вызвать на место происшествия спецслужбы к устранению последствий;

5) Уточнить оперативную обстановку на месте происшествия и готовиться к выезду;

---

[1] Ищенко, Е.П. Егоров, Н.Н. Руководство по производству следственных действий. Проспект. М., 2021. С. 20.

6) Проверить укомплектованность следственного чемодана, на наличие понадобившихся средств;

7) Пригласить специалистов и понятых.

При подготовке к осмотру места происшествия по киберпреступлениям, следователь должен решить вопрос о лицах, участвующих в следственном действии. Данный вопрос стал дискуссионным в научных кругах.

Так Д.А. Илюшин отмечает, что «для осмотра места происшествия целесообразно проводить следственно оперативной группой, состоящей в зависимости от определенной следственной ситуации», в которую включаются: следователь (желательно) специализирующий по данной категории уголовных дел; сотрудник отдела «К» УСТМ УВД (ГУВД, МВД) субъекта РФ; либо оперативно-технического подразделения; оперативный уполномоченный уголовного розыска (территориально закрепленный); специалист-криминалист, который обладает знаниями об особенностях обнаружения, изучения, фиксации и изъятии следов в зависимости от категории преступлений; специалист обладающий знаниями в сфере средств вычислительной техники; специалист, обладающий знаниями о технологических процессах; оператор проводящий видео фиксацию следственного действия; сотрудники полиции, привлекаемы в целях охраны места происшествия, задержания, конвоирования задержанного, или оказания иной помощи; представитель администрации предприятия, учреждения или организации, на территории (в помещении) которых производится осмотр (ч. 6 ст. 177 УПК РФ);[1] представитель службы безопасности или вневедомственной охраны организации, на территории (в помещении) которой производится осмотр; лицо, несущее материальную ответственность за компьютерную информацию, которая подверглась преступному воздействию, машинный носитель информации (МНИ) или

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 08 декабря 2020 г. № 419-ФЗ). Российская газета. 2001. 22 декабря.

средство обработки (ЭВМ); ответственный квартиросъёмщик, если осмотр выполняется в жилом помещении по правилам, регламентированным ч. 5 ст. 177 УПК РФ; инспектор-кинолог с собакой для розыска и задержания преступника по горячим следам; инспектор или ревизор, проводивший инвентаризацию, ревизию, аудиторскую или иную документальную проверку, вскрывшую признаки правонарушения.[1]

Предложенный Д.А. Илюшиным подход о привлечении к участию лиц в осмотре места происшествия является верным, и позволит следователю качественно провести следственное действие за счет распределения объема нагрузки на каждого участника. Однако следует учитывать, что в рамках осмотра, следственные ситуации могут сложиться по-разному, и нет смысла следователю привлекать абсолютно всех указанных им лиц, если нет необходимости их участия.

В судебной практике существуют примеры, когда указывается возможность изъятия электронных носителей информации без участия специалиста, в случае если с электронного носителя информации не осуществляется копирование информации, либо его изъятие не представляет какой-либо сложности и не требует специальных навыков и знаний.

Так к примеру, в Судебную коллегию оренбургского областного суда поступила жалоба осужденного, в которой он просил отменить приговор, ссылаясь на то что изъятие мобильного телефона производилось сотрудниками Линейного отдела МВД России на транспорте без участия специалиста. Суд признал довод осужденного необоснованным, указав, что участие специалиста при производстве следственного действия в ходе изъятия электронных носителей информации требуется при наличии нуждаемости в данном специалист, когда есть необходимость применения специальных познаний и навыков. К примеру, при копировании информации

[1] Илюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг интернет. С. 118 – 119.

участие специалиста обязательно, так как это тесно связано с риском утраты или изменения информации. [1]

Так же немаловажным вопросом является применение технических средств. Помимо основных технических средств, которые входят в чемодан следователя (осветитель ультрафиолетовый портативный; фонарь с питанием от аккумуляторов, тип ААА; линейка масштабная пластиковая матовая; рулетка карманная 5м металлическая, с фиксатором; штангенциркуль, диапазон измерения от 1 до 125 мм, цена деления 0,1; линейка офицерская; компас; указка лазерная; конверт почтовый; специальный пакет для вещественных доказательств и т.д.), могут использоваться технические устройства для обнаружения, исследования и изъятия электронно-цифровых устройств.

Примером устройства, посредством которого можно обнаружить и исследовать след является «UFED TK аппаратно-программный комплекс для съема, исследования и анализа данных из мобильных устройств». Аппаратно-программный комплекс позволяет проводить криминалистические исследования в неблагоприятных условиях, посредством подключения мобильных устройств для работы на разных этапах процесса – извлечения, декодирования, анализа и подготовки отчетов.[2]

Исходя из анализа сведений из сайта «Единой информационной системы в сфере закупок» ФКУ «Центральное окружное управление материально-технического снабжения МВД РФ» в 2021 году заказали данные устройства на сумму 41 129 370 рублей, из этого следует вывод, в

---

[1]Апелляционное определение Судебной коллегии по уголовным делам Оренбургского областного суда от 03.11.2016 по делу № 22-4229/2016 URL: https://oblsud--orb.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=1369693&delo_id=4&new=4&text_number=1

[2] Программный комплекс для криминалистических исследований UFED. URL: https://bakotech.ua/uploads/product/280/files/556/file.pdf

дальнейшей практике МВД планирует применять данные устройства при расследовании преступлений.[1]

Также в целях криминалистических исследований может применяться любое техническое устройство от компании «Cellebrite».

Изъятие и фиксация электронно-цифровых следов производиться посредством различных программ и устройств для хранения информации.

Следует согласиться с Александровым И.В. который отмечает, что невозможно привести исчерпывающий перечень используемых технических средств так как, арсенал постоянно изменяется вслед за увеличением разнообразия технического и программного обеспечения современных технологий. Поэтому он разделяет технические средства на два класса общеупотребительные (заимствованные из общей информатики), и специализированные (созданные для решения задач по исследованию данных находящихся в устройстве). К общеупотребительным относятся такие программы как Systeminformation, NortonUtilites, Symantec. К специализированным профессиональные программы IRC, DataExtractor, UDMA. Подобного рода программы позволяют изучить данные содержащиеся на технических устройствах, с дальнейшей возможностью изъятия посредством копирования.[2]

Следует заметить, что программы используемые программы должны соответствовать следующим требованиям, программа должна:

1) обеспечить доступ и работу с информацией на указанном устройстве без изменения ее содержания;

2) иметь возможность блокирования информации;

---

[1] Закупка в рамках ГОЗ. Аппаратно-программный комплекс для съема, исследования и анализа данных из мобильных устройств тип 1,2,3,4. Официальный сайт Единой информационной системы в сфере закупок. URL: https://zakupki.gov.ru/epz/order/notice/ea44/view/common-info.html?regNumber=0373100056021000093

[2] Александров И.В. Криминалистика Том 3. Криминалистическая техника : учебник для бакалавриата, специалитета и магистратуры.Юрайт. М., 2019. С.100 URL: https://urait.ru/bcode/426600 (дата обращения: 15.04.2021).

3) иметь возможность копирования информации с одного устройства на другое;

4) обеспечить доступ к файловой системе исследуемой информации;

5) иметь возможность вычисления хеш функций файлов, каталогов, разделов, диапазона секторов;

6) иметь возможность просмотра и интерпретации информации;

7) иметь возможность восстановления удаленной информации, а также обеспечить доступ к заблокированный информации;

8) иметь возможность просмотра и интерпретации служебной и системной информации;

9) иметь возможность поиска и манипуляции с информацией по различным критериям (контексту, свойствам, хеш-функциям);

10) обеспечить оформление результатов исследования и сохранения их в неизменном виде.

Изъятие же электронно-цифровых следов должны осуществляться на различные электронные носители с большим объемом памяти, такие как переносные жесткие диски, CD диски и т.д. Электронный носитель при копировании информации должен также обеспечивать неизменность перенесенных на него данных.

По прибытию на место происшествия следователю рекомендуется:

1) Зафиксировать время своего прибытия на место происшествия и в случае если есть необходимость, убедиться в том, что потерпевшему была оказана необходимая помощь, приняты меры по ликвидации последствий происшествия. Также провести ориентирующую и обзорную фотосъёмку для фиксации сложившейся обстановки на момент осмотра места происшествия;

2) Принять меры по сохранности возможных отображенных следов находящихся на поверхности или внутри устройств, для чего необходимо: а) никому из лиц находящихся на месте происшествия не разрешать прикасаться к компьютерному оборудованию; б) не разрешать лицам

находящихся на месте происшествия выключать электроснабжение; в) не производить никаких манипуляций с техникой без участия специалиста, в случае если в результате самостоятельных действий есть вероятность повредить криминалистически значимую информацию; г) обнаруженные устройства оставить в том состоянии в котором они находились на момент прибытия на место происшествие (включенное или выключенное состояние);

3) В случае если объектом осмотра будут являться стационарные устройства, которые соединены локальной сетью, установить есть ли централизованный сервер организующий работу всех устройств, а также установить иные соединения с оборудование вне осматриваемого помещения посредством локального подключения;

4) Выяснить имеются ли подключения осматриваемого оборудования с телефонной линией. В случае если есть подключение необходимо прекратить ее использование до момента выяснение наличия факта использования злоумышленником телефонной линии;

5) Определить какие программы запущенны на устройстве и помощью специалиста и описать детально их в протоколе, при этом если специалистом будет обнаружена вредоносная программа, способная уничтожить информацию, то следует уточнить у специалиста время работы данной программы, какие последствия наступят в случае ее отключения.

При наступлении рабочей стадии следователю следует использовать тактический прием «от центра – к периферии». Данной позиции придерживаются Д.А. Илюшин и Е.С. Шевченко.

При этом отправная точка определяется в зависимости от обстоятельств, так, например, «центром» может быть любое устройство с помощью которого осуществлялись противоправные действия или были объектом посягательства, либо место, на котором злоумышленником изготавливалось средство совершения преступления.

Шевченко Е.С. указывает, что «начальная стадия осмотра места происшествия состоит из проведения обзорного осмотра, а затем детального».[1]

В ходе обзорного определяется место осмотра и ее границы, так осмотру подлежат место использования компьютерного оборудования, место хранения обработки информации, место наступление вредных последствий.

В случае если осмотр производится в помещении, следователю необходимо установить границы осмотра, выяснить расположение локальных сетей, оборудование с помощью которого совершались преступления либо на которое осуществлялось посягательство.

При этом следует учитывать где находится осматриваемое помещение (административное здание, жилом доме, и т. д.), имеется ли система видеонаблюдения, сигнализации, охраны, а также состояние окон, дверей и их внутренних механизмов.[2]

После чего следует начертить схему с указанием границ осмотра, мест расположение технического оборудования и прилагающийся к ним устройств. В дальнейшем проводится по правилам обзорной фотосъемки фиксация общего вида помещения (включая общий коридор комнат в помещении), затем по правилам узловой съемки фиксирует техническое оборудование и подключенные к ним (или отдельно расположенные) устройства. Затем осуществляется детальный осмотр всего оборудования.

При проведении детального осмотра следователь поручает специалисту криминалисту осмотреть исследуемое оборудование на наличие материальных следов.

Следует уточнить, что как внешний, так и внутренний детальный осмотр технического оборудования и подключенный к нему устройств, производится при помощи специалиста в ИТ сфере, в целях избежание

---

[1] Шевченко, Е. С. Тактика производства следственных действий при расследовании киберпреступлений. С. 105.

[2] Беляев М.В. Актуальные вопросы раскрытия и расследования преступлений. Мастер Лайн. Следственный бюллетень. Казань 2001. Вып. 3. Ч. 2. С. 110

повреждения системных данных и технических элементах отвечающий за стабильную работу оборудования.

Вехов В.Б. и Зуев С.В. определили перечень фактических данных, которые должны быть установлены и отражены в протоколе: наименование объекта осмотра и его назначение; конструктивные и технические особенности местности или помещения с установкой и эксплуатацией технического оборудования и подключённых к нему устройств; расположение оборудования относительно вентиляционных и иных отверстий в строительных конструкциях, дверных и оконных проемов, рабочих мест и средств видеонаблюдения или охранной системы; нахождение иного технического оборудования; наличие линий, пунктов, разъемов систем инженерно-технических коммуникаций; следы преступника на оборудовании, подходах или отходах к нему; наличие или отсутствие учетно-справочной документации к осматриваемому оборудованию; актов на уничтожение конфиденциальной информации и их выдачи, заказов на обработку информации; следы применения иных технических средств связи; наличие, виды, особенности применения и показания систем защиты информации.[1]

Как верно указывает Шевченко Е.С. возможны случаи оставление преступником на компьютере следы кабельных соединениях, жестких дисков, флэш-носителей модемах и т. п. В этом случае все электронные носители могут осматривать с помощью специальных средств для доступа к информации с помощью специалиста, который устанавливает их возможную относимость к расследуемому преступлению, после чего если возникает необходимость изымаются следователем при помощи специалиста и упаковываются в соответствии ст. 177 УПК РФ.

В случае раскрытия и расследования преступлений по горячим следам целесообразно привлекать эксперта в силу его функций (как

[1]Вехов В.Б., Зуев С.В. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов С. 41

профессиональные, так и процессуальные), которые намного шире чем у специалиста. Эксперт при исследовании обстановки места происшествия как объекта экспертизы способен выявить не только свойства и признаки какого-либо объекта, но и познать механизм следообразования, что в дальнейшем поспособствует более успешному расследованию киберпреступления. Также он может провести ситуационную экспертизу, тем самым восстановить динамику деятельностного события и установить последовательность действий.

Изъятие технического оборудования и подключенных к нему устройств производится только в выключенным состоянии. При этом в протоколе отражаются следующие действия: установлено включенное состояние оборудования и зафиксирован порядок его отключения; описано местонахождение изымаемых предметов и их расположение относительно друг друга; описан порядок соединения всех устройств с указанием особенностей соединения; определено наличие или отсутствие компьютерной сети, канал связи и иные средства телекоммуникации; произведено разъединение аппаратных частей с одновременным опломбированием их технических входов и выходов; определен вид упаковки и транспортировки изъятых предметов.

В заключении следует указать, что вышеуказанные положения и позиции позволят следователю допустить меньше ошибок при проведении данного следственного действия, и тем самым успешно расследовать преступление.

2.2 Тактика проведения обыска и выемки при расследовании киберпреступлений

Производство обыска и выемки осуществляется на основании ст. ст. 182, 183 УПК РФ. Данные следственные действия

Следователь вправе провести обыск или выемку на основании вынесенного постановления (или судебного решения), в случае если он имеет

достаточные данные полагать, что у определенного лица или в определенном месте могут находится предметы, имеющие значение для уголовного дела.

Е.С. Шевченко провела опрос следователей и дознавателей по расследованию киберпреступлений, в общем количестве 78 человек. В 30% случаев при расследовании проводился обыск, а в 58,3% случаев выемка. При этом трудности проявлялись у 27,3% человек при проведении обыска, а у 37,2% при проведении выемки.[1]

Так можно привести пример, в г. Магнитогорске Челябинской области Мокроусов А.С. был признан виновным в «создании и распространении компьютерной программы, предназначенной для несанкционированного блокирования компьютерной информации и нейтрализации средств защиты компьютерной информации, совершенный в период, в период с 01.05.2015 по 11.05.2015 года». Вина подсудимого была доказана в том числе и результатами проведенного обыска в его квартире. Так 16.12.2016 а ходе обыска в квартире подсудимого был обнаружен и изъят системный блок от персонального компьютера, а так иные электронные носители информации и средства связи. Системный блок персонального компьютера был отправлен на компьютерно-техническую экспертизу, согласно заключению эксперта, на жестком диске персонального компьютера были обнаружены файлы, содержащие вредоносную компьютерную программу, созданную для несанкционированного подключения к информационному ресурсу, тем самым нарушить стабильность работы сетевого ресурса или ее блокирования.[2]

Обыск и выемка при расследовании киберпреступлений производится в целях получения доказательств в виде данных о способе совершения преступления, сопряженный с использованием компьютерной техники и телекоммуникационных сетей. Следовательно, перед следователем при

---

[1] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений: дис. … кан. юрид. наук. С. 228.

[2] Апелляционное постановление Челябинского областного суда от 23 апреля 2018 г. № 10 – 1934/2018. URL: //sudact.ru/regular/doc/7sZpql1IrkZd/

производстве обыска (выемки) при производстве обыска стоит цель обнаружить и изъять техническое устройство, на котором имеются следы совершенного преступления, в виде информации о совершенных действиях или о лице его совершавших, предметы и документы, которые могут иметь в своем содержании важную информацию для расследования преступления.

Так же было указанно, что у органа, проводившего предварительное расследование возникали трудности в проведении обыска. Полагаем, что данные трудности возникают из-за особенностей тактики проведения данных следственных действий.

На подготовительном этапе к проведению обыска (выемки) следователю выполнить ряд мероприятий организационного характера с целью реализации принятого решения: [1]

1) С момента принятия решения, следователю необходимо собрать ориентирующую информацию об объектах, подлежащих обнаружению и изъятию, об лицах, занимающих помещение. Имея исходную информацию следует ее проанализировать, и после определить вид, содержания компьютерной информации, выяснить на каких материальных носителях предположительно может хранится данная информация, на каком(их) технических устройствах имеется данная информация и предположительное ее количество. Данная информация позволит представить следователю о перечне участников, привлекаемых к следственному действию, и дальнейшем применении технических средств.

2) С целью установления обстановки и условий предстоящего обыска, следователю, необходимо будет установить точный адрес места проведения обыска, характеристика строения (к примеру является ли помещение отдельным зданием или помещением внутри организации, отдельной квартирой, комнатой в коммунальной квартире, строением на правах личной собственности), планировка помещения, пути подхода и проникновения в

[1]Гонтарь С.Н. Практикум по проведению следственных действий: тактика обыска выемки. Краснодарский университет МВД России. Ставрополь, 2014. С. 16.

обыскиваемое помещение, имеется ли на месте телефонная связь, работающий модем, имеются ли какие подключения сети как проводным, так и беспроводным способом, имеется ли между оборудованием локальное подключение, нахождение системы электропитания, место прокладки телекоммуникационных кабелей. Данная информация может находится как в материалах уголовного дела, так и из иных источников, к примеру, про сетевые подключения можно получить информацию оператора, который обслуживает данный адрес.

3) Следователю необходимо собрать исчерпывающую информацию об искомом объекте: характеристика, внешний вид, форма, размеры и другие индивидуальные признаки. Эта информация позволит следователю представить общий вид объекта, и в случае попытки сокрытия в ходе производства обыска определить вероятные места сокрытия объекта.

4) Изучить данные о лицах, проживающих или работающих в обыскиваемом объекте, профессии и характер занятий, возможные взаимоотношения между ними и окружающими; кто может оказаться в обыскиваемом помещении во время производства следственного действия, помимо проживающих и работающих лиц; могут ли у них находится огнестрельное оружие. Особую важность имеет информация о навыках лица в работе с информационными технологиями и телекоммуникационными сетями, о наличии профессиональных знаний, о месте работы и занимаемом должности. Шевченко Е.С. отметила, что данные сведения могут стать «ключевым элементом, если интересующие лица являются, например, провайдером интернет услуг, оператором или сотрудником учреждений, предоставляющих телекоммуникационные услуги, системным администратором, специалистом по обслуживанию компьютерных сетей). При изучении данной информации следователь сможет заранее предугадать

возможное (в том числе и «интеллектуальное») противодействие со стороны лиц, находящихся в месте проведения обыска (выемки)».[1]

И уже на основе данной информации следователь может определить: время начала проведения следственного действия (рекомендуется выбирать период времени, когда наиболее вероятно наличие искомых объектов, наиболее благоприятные условия для поисков и т.д.)

5) Далее следователь должен определить круг участников обыска (выемки). количество участников определяется в зависимости от выясненных обстоятельствах из ранее указанных действий. Обязательно должны участвовать понятые, при этом он должны иметь средний (пользовательский) уровень знаний в сфере компьютерных технологий. Также обязательно участие специалиста в сфере информационных технологий, при этом он подбирается в зависимости от искомого объекта (так к примеру, если искомым объектом является электронный след, то следует привлекать лицо, которое имеет знания в сфере программирования).

В качестве специалиста также могут привлекаться лица из организаций специализирующиеся в расследовании киберпреступлений. В качестве такой организации можно назвать уже ранее указанную организацию именуемой «GroupIB». Так к примеру, в 2020 г. сотрудники МВД при содействии специалистов «GroupIB» задержали организаторов преступной группы, которая перевыпускалаSIM-карты и похищала денежные средства у клиентов российских банков, ущерб преступной деятельности, которых оценивается в размере нескольких десятках миллионах рублей. В ходе обыска оперативника МВД и специалисты «GroupIB» обнаружили много численные сим-карты, различные технические устройства (ноутбуки, смартфоны, кнопочные телефоны, банковские карты и привязанные к ним сим-карты, на

[1] Гонтарь С.Н. Практикум по проведению следственных действий: тактика обыска выемки. С. 17.

них и приходили денежные средства). Всю конфиденциальную информацию мошенники хранили в «флешках-криптоконейнерах».[1]

Из данного инцидента также был обнаружен интересный факт, дело в том, что у данных мошенников были свои инсайдеры, в организациях, которые и способствовали совершению преступления, таковыми являлись: девушка которая перевыпускала сим-карты в салонах сотовой связи, и сотрудники российских банках с высоким уровнем доступа.

Из чего следует вывод, что не следует привлекать специалиста из организации «жертвы», так как привлеченное лицо может воспользоваться возникшим положением и попытаться противодействовать (к примеру, путем дезинформации, сокрытии следов преступления и т.д.) органу проводившего следственное действие.

6) Подготовить материально-технические средства. Любые технические устройства, которые планируется взять на следственное действие следует согласовать с специалистом. Следует согласиться с Шевченко Е.С. которая отметила, что «При обыске могут понадобиться следующее материально-техническое обеспечение: ноутбук, необходимые компьютерные программы (например, антивирусные программы; программы по созданию образа оперативной памяти); мобильный комплекс по сбору и анализу цифровых данных «UFED» (применяется для извлечения, декодирования и анализа данных с различных мобильных устройств: мобильных телефонов, смартфонов, планшетных компьютеров и телефонов с микросхемами китайского производства); мобильный подавитель работы сотовых телефонов «Мозаика+» (Россия), предназначенный для блокировки работы подслушивающих устройств и блокирования работы телефонов мобильной связи в пределах осматриваемой территории, а также для блокирования передачи данных с помощью устройств, работающих в

[1]МВД и Group-IB задержали мошенников, похищавших деньги у VIP-клиентов банков с помощью клонов SIM-карт. Официальная страница Group-IB. URL: https://www.group-ib.ru/media/sim-cards-clones/

стандартах Bluetoth и Wi-Fi».[1] Следует указать, что ранее указывались (в прошлом параграфе) специальные технические средства, которые также могут использоваться в ходе производства обыска (выемки).

После чего следователь проводит инструктаж лиц, участвующих в производстве обыска выемки. В ходе, которого следователь определяет в какое время производится следственное действие, каким способом будет осуществляться прибытие на место, далее разъясняет права и обязанности лиц, а также иные положения процессуального законодательства о порядке производства следственного действия, распределяет обязанности и определяет способы общения участников обыска.

Также следует уделить особое внимание к принятию мер к обеспечению внезапности обыска. Так как успешность проведения обыска в большем зависит от внезапности, следовательно, должны приниматься меры по неразглашению намерений следователя и в начальный момент обыска не возникли проблемы с попаданием в обыскиваемое помещение. Помимо этого, злоумышленник, узнав о проведении обыска в его отношении, попытается удалить всю значимую для уголовного дела информацию с компьютера. Поэтому подготовка к обыску должна осуществляться тайных условиях, и о проведении обыска и его плане должны знать только те лица, которые имеют прямое отношение к его проведению, при этом у данных лиц следует взять расписку неразглашении данных предварительного следствия.

Следует отметить что подготовительном этапе следователь должен вынести постановление о производстве обыска (выемки) или получить судебное решение позволяющее производство обыска (выемки).

По завершению подготовительного этапа следователь приступает к этапу производству обыска на месте.

Прибыв на обыскиваемое место, следователь предъявляет лицу, в отношении которого поводится следственное действия постановление о

---

[1] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений: дис. … кан. юрид. наук. С. 143

проведении обыска (выемки), либо судебное решение о разрешении проведения данного следственного действия. Затем следовать предлагает лицу выдать в добровольном порядке, искомые объекты. Если лицо отказывается от выдачи, то следователь должен уведомить всех лиц, находящихся в обыскиваемом помещении о запрете доступа к любому виду технического оборудования и телекоммуникационным сетям.

Далее следователь приступает к поисковым мероприятиям, которые делятся на две стадии называемые обзорная и детальная.

Шевченко Е.С. провела исследование уголовных дел по результатам которых выделила особенности производства обыска (выемки).[1] На наш взгляд выделенные особенности могут применяться в качестве рекомендаций по производству обыска (выемки) при расследовании киберпреступлений.

Так на обзорной стадии:

1. Следователю необходимо осмотреть все помещение. Первоначально следует обратить на компьютерное оборудование и телекоммуникационные сети, их расположение и состояние (включена или нет). Далее произвести поиск запоминающих устройств к примеру, как переносной жесткий диск, карты памяти, флэш-карты, а также потайные технические устройства маленького размера, которые могут иметь функцию хранения информации (кулон, часы и т.д.).

2. Установить имеет ли расположенная в обыскиваемом помещении компьютерная техника локальное подключение с другими электронными устройствами или к других телекоммуникационным сетям. В случае если такие подключения имеются, то определить с помощью специалиста какой из них является центральным звеном который регулирует работу всех остальных электронных техник.

---

[1] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений: дис. … кан. юрид. наук. С. 199 – 236.

Такое подключение чаще всего встречается в крупных организациях примеру в банках, где центральным звеном является сервер, в котором можно обнаружить электронные следы.

3. При осмотре компьютерной техники в случае если состояние включенное, следователю необходимо с помощь специалиста установить, есть ли на компьютере программы отвечающие за защиту системы и содержащихся в нем данных, а также иные вредоносные программы. При их наличии рекомендуется отключать подобные программы, так как их работа способна удалить данные содержащие электронный след. Также следует блокировать удаленный доступ на компьютере, так как ее работа позволяет злоумышленнику производить различные действия с содержащимися данными на данном устройстве, дистанционно.

Примером может служить программа LiteManagePro, которая позволяет пользователю, управлять питанием ПК, перезагружать и выключать ПК, производить различные действия с присоединенным оборудованием (монитор, клавиатура, мышь и т.д.), дистанционно просматривать рабочий стол ПК и запускать различные программы и так далее. [1]

4. Следователю также необходимо при осмотре электронного устройства: определить вид операционной системы, установленной на электронное устройство (это имеет значение для совместимости программ используемые при осмотре, которые могут позволить просмотреть определенный вид данных); просмотреть последние операции, выполненные на осматриваемом электронном устройстве; установить активность (историю активности) последних работающих программ с момента включения электронной техники. Данные обнаруженные сведения зафиксировать с помощью обычного фотоснимка, не рекомендуется делать скриншот с ПК так как существует возможность дистанционного выключение техники, и данный скриншот в последующем изъять не будет представляться

[1]Удаленный доступ, удаленное управление компьютером, удаленное администрирование. Сайт приложения LirleManager. URL: http://www.litemanager.ru/

возможным. Далее, в случае необходимости, работающие программы остановить.

После обзорной, следователь приступает к детальной стадии:

1. Производится детальный осмотр компьютера, на котором просматриваются различные данные в поисках информации, имеющей значение для расследования преступления. Данная информация может храниться как на жестких дисках (системном и дополнительном) так и на оперативной памяти. В случае если нужная информация была найдена, то следует записать в протокол сведения о ней: путь к ней (C:\Users\home\Documents\DAVAProject), наименование файла и его размер. В последующем, если представляется возможным изъять в реальном виде, электронное устройство выключается, упокоевается (специалистом) и изымается, если же устройство в силу своей громоздкости невозможно упаковать и изъять в таком случае либо изымается диск, отвечающий за хранение требуемых данных в порядке установленных законом, либо данные копируется на переносной носитель, с последующим описанием в протоколе действий копирования.

При производстве компьютерной техники в выключенном состоянии рекомендуется зафиксировать его местоположение и всех подключенных к нему устройств и телекоммуникационных сетей. Если есть иные подключения их следует разъединить эти устройства, после чего подготовить их к упаковке и изъятию. Следует уточнить что всю изымаемую технику и все последующие действия с ней следует отражать в протоколе, с точным указанием ее свойств, размеров и наличием портов для подключения.

6. В случае если при обыске обнаружен мобильный телефон, смартфон, или иная электронная техника, то осмотр содержащийся в нем данных можно осуществлять с помощью исследовательского комплекса по просмотру копированию информации «UFED», сущность которой описывалась в прошлом параграфе.

Стоит указать на то, что все вышеуказанные действия выполняются только с помощью специалиста, обладающего знаниями в требуемой сфере, так как высока вероятность, что следователь, выполняя данные действия самостоятельно, способен изменить созданную обстановку преступником в киберпространстве, где и хранится криминалистически значимая информация.

После детального осмотра информации наступает заключительный этап, на котором следователь выполняет комплекс действий, выполняемых для изъятия обнаруженных объектов и процессуального оформления хода и результатов обыска. Изымаемые предметы подлежат осмотру на месте производства следственного действия или в случае если не представляется возможным осмотреть предмет на месте, следователь упаковывает предмет, опечатывает и изымает, для дальнейшего осмотра на месте производства следствия.[1]

При этом электронная техника должна упаковываться правильно, исходя из особенностей устройства. К примеру, если устройство хрупкое, то оно помещается в коробку и свободное пространство (как по бокам, так и с верху, и с низу) забивается мягким материалом с целью исключения лишнего физического воздействия на внутренние технические компоненты устройства.

В заключении следует указать, что вышеуказанные положения и позиции позволят следователю допустить меньше ошибок при проведении данного следственного действия, и тем самым у эксперта при исследовании электронно-цифровых следов исключит возникновение перед экспертом препятствий ограничивающие возможность подготовить достоверное и допустимое заключение.

[1]Гонтарь С.Н. Практикум по проведению следственных действий: тактика обыска выемки. Краснодарский университет МВД России. Ставрополь, 2014. С. 20-25.

2.3 Назначение и виды судебных экспертиз при расследовании киберпреступлений

В соответствии с ст. 195 УПК РФ, следователь, признав необходимым назначение судебной экспертизы, выносит об этом постановление, в котором указываются: основания назначения судебной экспертизы; ФИО эксперта или наименование экспертного учреждения; вопросы, поставленные перед экспертом; предметы передаваемы эксперту для исследования.

Перечень экспертиз, которые возможно назначить при расследовании киберпреступлений очень обширен, и следователь может прибегнуть как к традиционным экспертизам, так и к не традиционным. Это связано с тем, что каждое уголовное дело имеет свои особенности и следователю приходится назначать экспертизы, исходя из вида киберпреступления и необходимости исследования конкретных следов преступления (объектов).

В.О. Давыдов проанализировал следственную практику, и выяснил перечень назначаемых экспертиз по данной категории преступлений.[1] Так из числа традиционных экспертиз назначаются: трасологические, дактилоскопические, технико-криминалистические экспертизы документов, почерковедческие, автороведческие экспертизы, а из числа нетрадиционных экспертиз: психофизиологические с использованием полиграфа, медико-психологические или психилого-психиатрические экспертизы в отношении лиц, страдающих интернет-зависимостью, комплексные психолого-искусствоведческие (по делам о незаконном изготовлении, распространении и обороте порнографических материалов или предметов), комплексная психолого-лингвистическая экспертиза и так далее.

Особым видом судебных экспертиз, назначаемых при расследовании киберпреступлений является компьютерно-техническая экспертиза, с помощью которой из специфичного объекта и предмета исследования

---

[1] Давыдов В. О. Методика расследования экстремистских преступлений, совершенных в компьютерных сетях: монография. Юрлитинформ. М., 2014. С. 98;

извлекается виртуальная информация, и фиксируется в заключении для придания ей доказательственного значения.

Исходя из проведенного исследования уголовных дел Шевченко Е.С. отмечает, «как показывает практика, назначение компьютерно-технической экспертизы вызывает у следователей наибольшие сложности, на что указали 39,5% опрошенных следователей и дознавателей».

В связи с чем возникает необходимость разобрать природу данного вида экспертизы, с целью установления порядка ее назначения и требованиям, предъявляемым к определению содержанию и формулировки вопросов для эксперта.

Компьютерно-техническая экспертиза, является самостоятельным родом судебных экспертиз, которая относится к инженерно-техническому классу и проводится в целях: определения статуса объекта, выявления и изучение роли в совершенном преступлении.[1]

Тушканова О.В. определяет следующие цели следователя при назначения данного вида экспертизы: 1) воспроизведение и распечатки компьютерной информации, которая может храниться на электронных носителях и в телекоммуникационных сетях; 2) восстановление утраченной информации, содержащейся на носителе; 3) установление даты и времени проведения различных операций с содержащейся на устройствах информацией; 4) расшифровка закодированной информации, подбор паролей и раскрытие системы защиты; 5) исследование на наличие вредоносных программ электронных носителей м содержащейся на нем информации; 6) установление источника происхождения и способы изготовления программ, файлов и т.д.; 7) установление источника утечки информации; 8) установление несанкционированных способов доступа к информации и ее носителям, охраняемых законом; 9) определение технического состояния электронных устройств, оценка износа, а также индивидуальные признаки

[1]Компьютерно-техническая экспертиза. Сайт Российский федеральный центр судебной экспертизы при Министерстве юстиций РФ. URL: http://www.sudexpert.ru/possib/comp.php

адаптации под определенного пользователя; 10) установление уровня профессионализма в области программирования лиц проходящих по уголовному делу; 11) установление лиц, нарушивших правила эксплуатации средств хранения, обработки или передачи охраняемой законом компьютерной информации, а также правил доступа к информационно-телекоммуникационным сетям; 12) установление даты и времени работы устройства в информационной системе, и получение сведений об использованных логинов и паролей для получения доступа к ней; 13) установление причин и условий способствующих совершению преступления.[1]

Компьютерно-техническая экспертиза подразделяется на следующие виды: аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную, компьютерно-сетевую экспертизу. Каждый из них имеет свои особенности.[2]

Так в рамках аппаратно-компьютерной экспертизы – проводится исследование технических средств компьютерной системы, к которым относятся: персональные компьютеры, периферийные устройства, сетевые аппаратные средства, схемы, блоки, приборы и устройства, составляющие материальную часть общей системы.

Программно-компьютерная экспертиза – исследует закономерности разработки и использования программного обеспечения. Задачей изучения является изучение характеристик, функций, особенностей структуры и состояние программного обеспечения компьютерной системы.

Так к примеру, Малов Е.А. реализовывая свой преступный умысел, использовав ранее изученные методы по обходу программно-аппаратной защиты игровых приставок MicrosoftXbox360, неправомерно получил доступ к охраняемой законом информации, что повлекло за собой модификацию

---

[1] Тушканова О.В Криминалистическое исследование компьютерной информации. Криминалистика: учебник для бакалавров. РГ-пресс. М., 2018. С. 365-375.

[2] Компьютерно-техническая экспертиза. Сайт Российский федеральный центр судебной экспертизы при Министерстве юстиций РФ. URL: http://www.sudexpert.ru/possib/comp.php

компьютерной информации, совершенный из-за корыстной заинтересованности. В ходе проведения оперативно-розыскных мероприятий актом осмотра и передачи предмета была передана игровая приставка, флэш-накопитель. Также в ходе обыска в жилище у Малова Е.А. были изъяты: 8 чипов, программатор, 6 адаптеров, системный блок.

Заключением эксперта программно-компьютерной экспертизы от 01.04.2018 г. установлено, что на игровой приставке MicrosoftXbox360 предусмотрена специальная программа и аппаратная защита, в которую были внесены изменения, тем самым нейтрализовало программно-техническое средство защиты от включения нелицензионных продуктов. Помимо того, на изъятых носителях информации были программы, которые предназначены для выполнение действии по внесению изменений.[1]

Компьютерно-сетевая экспертиза – исследует функциональное предназначение компьютерных средств, которые реализуют какую-либо сетевую технологию.

Так, например, Гражданин Г. незаконно распространял наркотики и психотропные вещества с использованием сети интернет. С целью реализации преступного умысла Г. установил на мобильный телефон программное обеспечение, которое предназначено для работы в интернет сети и получения доступа к информации предоставляющая возможность распространения некротических средств и психотропных веществ. Данный интернет-сайт был установлен и осмотрен, после чего была назначена компьютерно-сетевая экспертиза. Согласно заключению, интернет сайт, представляющий из себя главную страницу интернет-магазина, состоящий из разделов с ссылками на переход в вкладку по продаже наркотических средств и психотропных веществ на территории РФ, расположенный в сети (www)

[1] Приговор Дмитриевского городского суда Ульяновской области от 16 июля 2018 по делу №1-176/2018 URL: //sudact.ru/regular/doc/jiaWOZeD0exK/

форма общения с администратором сайта осуществляется через блокнот, в котором уничтожаются внесенные записи.[1]

Информационно-компьютерная экспертиза – осуществляется с целью поиска, обнаружения, анализа и оценки информации, оставленной после действия пользователя или работы программного обеспечения. является основным видом, в связи с тем, что путем разрешения большинства диагностических и идентификационных вопросов позволяет завершить построение доказательственной базы.

Подсудимый Котляров Я.А. совершил использование компьютерной программы, заведомо предназначенной для нейтрализации средств защиты компьютерной информации, при следующих обстоятельствах. протоколом обыска от 17.07.2019г. в ходе которого были изъяты: НЖМД «WD», НЖМД «Toshiba», НЖМД «Toshiba», НЖМД без указания фирмы производителя переносной НЖМД «Blueendless» в корпусе черного цвета, НЖМД «Seagate», и так далее. Согласно заключению эксперта № 5135 от 17.09.2019г., на жестком диске «WD» s/n имеется каталог, в котором имеется исполняемый файл, именующий себя «<данные изъяты>». Дата создания каталога 6.12.2017г., в 15 часов 21 минуту. На жестком диске «Toshib», имеются сведения об Интернет-ресурсах на которых производилась авторизация или попытка авторизации. Данная программа использовалась для поиска в сети интернет веб-интерфейсов сетевого оборудования, с целью дальнейшего получения несанкционированного доступа к нему. «Несанкционированный доступ достигается путем нейтрализации средств защиты веб-интерфейса сетевого оборудования с помощью подбора пары логин/пароль либо эксплуатации программных уязвимостей указанного оборудования. Программа «<данные изъяты>» предоставляет возможность пользователю нейтрализовать средства защиты компьютерной информации, то есть является вредоносной

[1] Приговор Краснодарского краевого суда от 23 июля 2019 по делу №2 8/2019 URL: //sudact.ru/regular/doc/PDXLfJbOWeLu/

компьютерной программой. Иного предназначения данное программное обеспечение не имеет».[1]

На первоначальном этапе расследования, когда следователь провел осмотр места происшествия, обыск, выемку, и понимает, что известной информации недостаточно для продолжения расследования, он принимает решение о назначении судебной компьютерно-технической экспертизы обнаруженных и изъятых объектов с ранее указанных следственных действий. После принятия решения следователь может столкнуться с перечнем проблем.

В научном сообществе, ученые криминалисты проводили исследование следственной практики и выделили следующие проблемы, с которыми может столкнуться следователь. Так Шевченко Е.С., Меженга М.М., Поляков В.В., Шебалин А.В., Сысенко А.Р., Смирнова И.С., Тимошенко С.Е., выделяют следующий перечень проблем.

Первой проблемой является, отсутствие единого подхода как к названию компьютерно-технической экспертизы, так и к пределам компетенции экспертов.

В приказе Министерства юстиций РФ от 27.12.2012 г. №237 «об утверждении перечня родов (видов) перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в ФБСЭУ Минюста РФ».[2] В нем используется термин «компьютерно-техническая экспертиза», и в компетенцию эксперта входит разрешение вопросов в отношении аппаратной части технических устройств, так и в отношении программного обеспечения и данных, имеющихся на электронных носителях.

---

[1] Приговор Павловского районного суда Воронежской области от 25 ноября 2020 г. № 1 – 40/2020. URL: //sudact.ru/regular/doc/KL22CmxCcxU/

[2]Приказ Минюста России "Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России" от 27.12.2012 N 237. Российская газета. 2013. № 26742.

В приказе МВД России от 29.06.2005 г. №511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях ОВД РФ».[1] Данный род экспертиз имеет наименование «компьютерная экспертиза», предметом которой является только компьютерная информация.

На наш взгляд предлагаемое название «компьютерно-техническая экспертиза», является оптимальным вариантом так как семантически объединяется основной цифровой объект (ПК, сервера, принтеры, мобильные устройства и т.д.), а также его составляющие системные элементы (системное программное обеспечение, информационные данные), а также составные элементы сети (проводные, беспроводные сети, компоненты их взаимодействия).

Второй проблемой является выбор подвида экспертизы. Следователь после принятия решения о назначении компьютерно-технической экспертизы, сталкивается с проблемой указания ее разновидности. Как указывает Менжега М.М. что, если следователь укажет ту или иную разновидность компьютерно-технической экспертизы, это может привести к излишнему усложнению назначения экспертизы, а также к привести к сложностям ее производства и в дальнейшем дачи ответа экспертом на поставленный вопрос.[2] Аналогичной позиции придерживаются В.В. Поляков и А.В. Шебалин. Следует согласиться с позицией М.М. Менжеги, «в случае если у следователя нет возможности взаимодействовать со специалистом (экспертом) и получить у него консультацию по определению вида СКТЭ, руководитель экспертного учреждения помогает решить ряд проблем,

---

[1]Приказ МВД России "Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации" (вместе с "Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации", "Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации") от 29.06.2005 N 511. Российская газета .2005. № 693.

[2]Менжега М. М. Методика расследования создания и использовании вредоносных программ для ЭВМ / М. М. Менжега.Юрлитинформ М., 2010. С. 122.

связанных как с разъяснением вопросов, которые могут быть решены экспертом в рамках назначаемой компьютерно-технической экспертизы, так и определением объема материалов, вещественных доказательств и объектов исследования, которые необходимы эксперту для полного всестороннего исследования с целью ответа не поставленные вопросы»[1], так как все материалы при назначении экспертизы направляются руководителю, и он в последующем отвечает за определение эксперта (из требуемой специальности), который будет проводить экспертизу. Тем самым советы и указания руководителя экспертного учреждения следователю по вопросу назначения конкретного подвида СКТЭ, способы исключить дальнейшие проблемы при производстве экспертизы и даче экспертом ответов на поставленные вопросы.

Третьей проблемой, стоящей перед следователем при назначении экспертизы, является выбор перечня составления вопросов и их корректность в формулировке. В проведенном опросе Шевченко Е.С., было установлено, что у 27% опрошенных органов предварительного расследования при назначении компьютерно-технической экспертизы, возникали проблемы в постановке грамотных вопросов эксперту. Федотов Н.Н. отметил, что причиной данной проблемы является низкий уровень знаний в области информационных технологий, а также с непонимание специальной терминологии.[2]

Шевченко Е.С., предлагает учитывать следующие особенности, которые помогут корректно составить вопросы к компьютерно-технической экспертизе:[3]

1) вопросы не должны нести в себе правовой характер (является ли объект контрафактным?);

---

[1] Менжега М. М. Методика расследования создания и использовании вредоносных программ для ЭВМ / М. М. Менжега.Юрлитинформ М., 2010. С 123.
[2] Федотов Н. Н. Форензика – компьютерная криминалистика. С. 254-255.
[3] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений: дис. …кан. юрид. наук. С. 160 – 161.

2) вопросы не должны затрагивать стоимость объекта, перевода текста, переписки и т.д.;

3) вопросы должны быть технического характера (какова общая характеристика объекта, из каких компонентов состоит?);

4) вопросы должны быть составлены исходя из задач исследования (идентификационные или диагностические);

5) согласовывать составленные вопросы со специалистом или составить вопросы с его помощью.

Вехов В.С. составил перечень требований к определению содержания и формулировке вопросов:[1]

1) при постановке вопроса использовать устоявшийся понятийный аппарат, избегая жаргонные и полупрофессиональные термины, к примеру: «СМС» - «SMS-сообщение», «винчестер» - накопитель на жестких магнитных дисках», и т.д. При это если нет терминов, установленных законодательство, следует применять ту терминологию, используемую в технической документации объекта (инструкции, техническом паспорте и т.д.);

2) формулировка вопроса не должна касаться этапов исследования информации (описание характеристик носителей информации и особенностей размещение информации на них, восстановление и исследование информации среди удаленных файлов, являются обязательным этапов исследования информации);

3) вопросы не должны: носить правовой характер, выходить за рамки компетенции эксперта, носить справочный характер (разъяснения о значении термина, интерпретации информации);

4) вопросы должны: соответствовать представленным объектам, соответствовать существующей методической и технической базе,

[1]Вехов. В.Б., Зуев С.В. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов. С. 48 – 50.

направляться на установление конкретных обстоятельств, отвечать уровню подготовки и инструментальному оснащению эксперта.

На наш взгляд, данные позиции способны облегчить следователю процесс составления перечня вопросов и формулировки вопроса.

Далее следователь подготавливает все сведения и материалы относящиеся к предмету экспертизы, оценивает и проверяет их достаточность после чего оформляет для дальнейшей передачи в экспертное учреждение.

В заключении данной главы можно сделать вывод, что следователю необходимо при проведении следственных действий привлекать соответствующих специалистов (экспертов), с целью исключения при дальнейшем расследовании преступлений ошибок, которые могут повлиять на дальнейшее использование полученных доказательств в суде.

ЗАКЛЮЧЕНИЕ

В заключении выпускной квалификационной работы были сформированы следующие выводы:

1. Понятие «киберпреступление» несет в себе более широкое смысловое значение и точно отражает сущность преступлений в киберпространстве чем указанные выше понятия.

Определение «киберпреступление» можно понимать, как термин более широкий, нежели те, что были указаны ранее. Он в своей сути охватывает множество терминологий противоправных деяний. Все эти факты дают право определять киберпрестулпение с точки зрения криминалистики, а также понимать его как общественно опасное деяние, которое совершается в данном киберпространстве. Киберпреступление посягает на собственность и права человека, а также общественную безопасность с одной стороны, и, является необходимым элементом процесса как совершения преступления, так и его подготовки, и сокрытия. Отражением данных преступлений является компьютерная информация, которая выступает как предмет или средства совершённого преступления.

Главной особенностью киберпреступлений выступает элемент киберпространство, через которое злоумышленник посягает на охраняемые законом права, свободы и интересы. При расследовании следователь сталкивается с проблемой определения места, которое и выступает в качестве отправной точки совершения, так как в киберпространстве не существует географических границ.

2. Успешность расследования преступления следователь во многом зависит от наличия исходной информации, одной из таких информационных без можно рассматривать криминалистическую классификацию. Криминалистическая классификация способствует правильному пониманию сути расследуемых событий, грамотному построению, выборы и применению предлагаемых практиками методик расследования отдельных видов киберпрступлений. Однакопостоянно набирающий обороты научно-

технический прогресс не позволяет выделить единую классификацию. Но указанные в выпускной квалификационной работе классификации могут использоваться для разработки криминалистических методик.

3. Криминалистическая характеристика киберпреступлений состоит из 4 важных элементов: способы совершения, обстановка совершения, личность киберпреступника, предмет преступного посягательства и следовая информация.

4. Под электронно-цифровым следом в узком смысле следует понимать криминаличтиески значимую информацию, которая выражается посредством электромагнитных взаимодействий или сигналов в форме, пригодной для обработки с использованием любого вида технологии, в результате создания двоичного кода на материальном носителе, либо его преобразование, выразившееся в модификации, копировании, удалении, блокировании и др. процессах.

В широком смысле под электронно-цифровом следе понимается, криминалистически значимая информация, образованная в киберпространстве в результате человеческой деятельности.

5. Основу механизма следообразования при совершении компьютерных преступлений, всегда составляет электромагнитные взаимодействия. Механизм воздействия одного объекта на другой может быть обнаружен по наблюдаемому различию между тремя состояниями:

а) изменение содержания, формата и иных характеристик;

б) изменение алгоритма работы;

в) по автоматически создаваемым программой файлов, которые используются программами и операционными системами для фиксации обработки информации, восстановления или программного обеспечения.

6. В киберпреступлениях местом происшествия могут быть различные участки местности где возможно установить или переносить техническое устройство начиная лесной местностью, транспортным средством. парком заканчивая помещением или рядом помещений.

Тактика осмотра места происшествия имеет свою специфику. Исходя из сложности производства данного следственного действия рекомендуется создавать следственно оперативные группы, состав которой определяется в зависимости сложности производства следственного действия.

Предложенный Д.А. Илюшиным подход о привлечении к участию лиц в осмотре места происшествия является верным, и позволит следователю качественно провести следственное действие за счет распределения объема нагрузки на каждого участника. Однако следует учитывать, что в рамках осмотра, следственные ситуации могут сложиться по-разному, и нет смысла следователю привлекать абсолютно всех указанных им лиц, если нет необходимости их участия.

Все действия с исследуемой техникой на место осмотра рекомендуется проводить с помощью специалистов.

7. Обыск и выемка при расследовании киберпреступлений производится в целях получения доказательств в виде данных о способе совершения преступления, сопряженный с использованием компьютерной техники и телекоммуникационных сетей. Следовательно, перед следователем при производстве обыска (выемки) при производстве обыска стоит цель обнаружить и изъять техническое устройство, на котором имеются следы совершенного преступления, в виде информации о совершенных действиях или о лице его совершавших, предметы и документы, которые могут иметь в своем содержании важную информацию для расследования преступления.

Результативность обыска, обусловленная тщательной ее подготовкой, порядок которой описан в параграфе.

8. Компьютерно-техническая экспертиза подразделяется на следующие виды: аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную, компьютерно-сетевую экспертизу. Каждый из них имеет свои особенности.

Термин «компьютерно-техническая экспертиза», является оптимальным вариантом так как семантически объединяется основной

цифровой объект (ПК, сервера, принтеры, мобильные устройства и т.д.), а также его составляющие системные элементы (системное программное обеспечение, информационные данные), а также составные элементы сети (проводные, беспроводные сети, компоненты их взаимодействия).

Необходимо выбирать вид СКТЭ с помощью специалиста, с целью исключения дальнейших сложностей при ее производстве, в случае если нет возможности прибегнуть к помощи специалиста, рекомендуется обратится к руководителю экспертного учреждения.

Следователю рекомендуется составлять перечень и формулировку вопросы с помощью специалиста. При этом при постановке вопроса учитывать перечень особенностей, выделенных ученными криминалистами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ I НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

1. Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. // Российская газета. 1993. № 237.
2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СЗ РФ.1996. № 25. Ст. 2954.
3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 08 декабря 2020 г. № 419-ФЗ) // Российская газета. 2001. 22 декабря.
4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. //СЗ РФ. 2006. N 27. ст. 2711
5. О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: федеральный закон от 01.10.2008 г. № 164-ФЗ // Собрание законодательства РФ. – 06.10.2008. – № 40. – Ст. 4499.
6. Окинавская хартия глобального информационного сообщества (принята на о. Окинава (Япония) 22.07.2000 на совещании руководителей Глав государств и правительств стран «Группы Восьми») // Дипломатический вестник. 2000. № 8.С. 51 – 56;
7. Приказ Минюста России "Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России" от 27.12.2012 N 237// Российская газета. 2013. № 26742.

8. Приказ МВД России "Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации" (вместе с "Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации", "Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации") от 29.06.2005 N 511//Российская газета .2005. № 693.

РАЗДЕЛ II ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. OrlyTurgeman–Goldschmidt. Meanings that Hackers Assign to their Being a Hacker / Copyright. Israel, 2008. Vol. 2 (2) C. 382-396 URL: http://www.cybercrimejournal.com/Orlyijccdec2008.pdf (дата обращения 02.02.2021).
2. Агибалов, В.Ю. Виртуальные следы в криминалистике и уголовном процессе: Монография / А.Ю. Агибалов // Юрлитинформ. М., 2012. 152 с.
3. Александров, И.В. Криминалистика Том 3. Криминалистическая техника : учебник для бакалавриата, специалитета и магистратуры / отв. редактор Н. Н. Егоров, И. В. Александров // Юрайт . М., 2019. 216 с. URL: https://urait.ru/bcode/426600 (дата обращения: 15.04.2021).
4. Беляев, М.В. Актуальные вопросы раскрытия и расследования преступлений / М.В. Беляев //Мастер Лайн. Следственный бюллетень. Казань 2001. .Вып. 3. Ч. 2. С. 110.
5. Борисов, В.В. Об особенностях фиксации информационных следов в практике защиты информации / В.В. Борисов // Известия Южного федерального университета. Технические науки. М., 2009. №5.-С. 164 - 168.

6. Васильев, А. А. Электронные носители данных как источники получения криминалистически значимой информации: учебное пособие / А. А. Васильев; К. Е. Демин. М., 2009. 200 с.
7. Вехов, В. Б. Компьютерные преступления: способы совершения и раскрытия / В. Б. Вехов; под ред. Б. П. Смагоринского. Право и Закон, М.,1996. – 182 с.;
8. Вехов, В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография / В. Б. Вехов. // ВА МВД России.Волгоград, 2008. 404 с.
9. Вехов, В. Б. Электронные следы в системе криминалистики / В. Б. Вехов, Б. П. Смагоринский, С. А. Ковалев // Судебная экспертиза. Волгоград. 2016. Вып. 2. 127 с.
10. Вехов, В.Б., Зуев, С.В. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / В.Б. Вехов, С.В. Зуев // Изд-во Юрайт. М., 2021. – 243 с.
11. Волеводз, А. Г. Конвенция о киберпреступности: новации правового регулирования / А.Г. Волеводз // Правовые вопросы связи. – 2007. – № 2. – С. 17 – 25.
12. Волеводз, А.Г. Противодействие компьютерным преступлениям. / А.Г. Волеводз // Юрлитинформ. М., 2002. С. 159 - 160.
13. Воробьев, В.В. Преступления в сфере компьютерной информации, юридическая характеристика составов и квалификация :дис. … канд. юрид. наук. / В.В. Воробьев. Н. Новгород, 2006. С. 12.
14. Гонтарь, С.Н. Практикум по проведению следственных действий: тактика обыска выемки / С.Н. Гонтарь // Краснодарский университет МВД России. Ставрополь, 2014. 30 с.
15. Давыдов, В. О. Методика расследования экстремистских преступлений, совершенных в компьютерных сетях: монография / В. О. Давыдов; под. ред. А. Ю. Головина. // Юрлитинформ. М., 2014. – 184 с.;

16. Давыдов, В. О., Головин, А. Ю. Значение виртуальных следов в расследовании преступлений экстремистского характера / В. О. Давыдов, А.Ю. Головин // Известия Тульского государственного университета. Экономические и юридические науки. Тула, 2016. № 3. С. 254 – 259.
17. Дёмин, К. Е. К вопросу о выделении криминалистического исследования электронных носителей информации как новой отрасли криминалистической техники / К. Е. Дёмин // Библиотека криминалиста. – 2013. – № 5 (10). – С. 174 – 189;
18. Дерюгин, Р. А. Перспективы развития цифровой криминалистики в условиях информационного общества / Р. А. Дерюгин, А. А. Жижилева // Технологии XXI века в юриспруденции : Материалы Всероссийской научно-практической конференции. Екатеринбург, 2019. – С. 40-46.
19. Дуленко, В. А. Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации: учебное пособие / В. А. Дуленко; Р. Р. Мамлеев; В. А. Пестриков. // УЮИ МВД России. Уфа. 2007. С. 15.
20. Илюшин, Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: Дис. … канд. юрид. наук: / Д.С. Илюшин. Волгоград, 2008. – 233 с.
21. Ищенко, Е.П. Егоров, Н.Н. Руководство по производству следственных действий / Е.П. Ищенко, Н.Н. Егоров // Проспект. М., 2021. 144 с.
22. Казанцев, В.В. Криминалистическое исследование средств компьютерных технологий и программных продуктов: учебно-практическое пособие / В.В. Казанцев // Терра линк. Алматы, 2003. 150 с.
23. Козлов, В. Е. Теория и практика борьбы с компьютерной преступностью. / В.Е. Козлов // Горячая линия-Телеком М., 2002. – 336 с.
24. Колычева, А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: автореф. канд. юрид. наук: / А.Н. Колычева.-М., 2019.-С. 10.

25. Косенков, А.Н., Черный, Г.А. Общая характеристика психологии киберпреступника / А.Н. Косенков, Г.А. Черный // Криминологический журнал БГУЭП. 2012. № 3 (21). С.87 – 94
26. Кузнецов, А. В. Некоторые вопросы расследования преступлений в сфере компьютерной информации / А.В. Кузнецов // Информационный бюллетень следственного комитета МВД РФ. М., 1998. № 2. С. 42-48.
27. Лунев, В. В. Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями, его место в истории конгрессов / В. В. Лунев // Государство и право. 2000. № 9. С. 95 – 100;
28. Льянов, М. М. Современный подход к классификации виртуальных следов / М. М. Льянов // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 4(30). С. 47-55.
29. Менжега, М. М. Методика расследования создания и использовании вредоносных программ для ЭВМ / М. М. Менжега. // Юрлитинформ М., 2010. 184 с.;
30. Мещеряков, В. А. Основы методики расследования преступлений в сфере компьютерной информации: Дис. … д-ра юрид. наук / В.А. Мещеряков. Воронеж, 2001. – 387 с.;
31. Мещеряков, В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В. А. Мещеряков. // Издательство Воронежского государственного университета. Воронеж, 2002. 408 с.
32. Мещеряков, В. А. Следы преступлений в сфере высоких технологий / В. А. Мещеряков // Библиотека криминалиста. 2013. № 5 (10). С. 265 – 269
33. Морар, И.О. Могут ли в рамках науки криминологии рассматриваться способы совершения компьютерных преступлений и их последствия. / И.О. Морар // Российский следователь. 2012. № 12. С. 37 – 41.
34. Нехорошев, А.Б. Компьютерные преступления: квалификация, расследование, экспертиза/под ред. В.Н. Черкасова. // СЮИ МВД России. Саратов, 2004. Ч. 2. С. 61-65.

35. Номоконов, В.А. Актуальные проблемы борьбы с киберпреступностью. Компьютерная преступность и кибертерроризм / В.А. Номоконов // Запорожье. 2004. № 1. С. 77.
36. Осипенко, А. Л. Сетевая компьютерная преступность: теория и практика борьбы: Монография. / А.Л. Осипенко // Омск. акад. МВД России. Омск, 2009. С. 109 – 110.
37. Пашнев, Д. В. Криминалистическая классификация преступлений, совершаемых с использованием компьютерной техники / Д. В. Пашнев. // Доля. Симферополь, 2004. С 164 – 166.
38. Поляков, В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики / В.В. Поляков // Известия АГУ. 2013. № 2-1 (78). С. 114 – 116.
39. Попов, И. А. Правовое и организационное обеспечение раскрытия и расследования преступлений в сфере компьютерной информации: состояние и пути совершенствования / И.А. Попов // Библиотека криминалиста. 2013. № 5 (10). С. 325.
40. Пропастин, С. В. Расследование неправомерного доступа к электронной почте / С. В. Пропастин // Уголовный процесс. 2017. № 2(146). С. 60-64.
41. Протасевич, А. А. Особенности осмотра места происшествия по делам о киберпреступлениях / А. А. Протасевич, Л. П. Зверянская // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). 2013. № 2. С. 23
42. Рассолов, И. М. Право и Интернет. Теоретические проблемы. Изд. 2-е / И.М. Рассолов. // Норма. М., 2009. С. 135.
43. Селиванов, Н. А. Проблемы борьбы с компьютерной преступностью / Н.А. Селиванов // Законность. 1993. № 8. С. 37
44. Семенов, А.Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере

компьютерной информации / А.Ю. Семенов // Сибирский юридический вестник. 2004. № 1. С. 53 – 55.

45. Соловьева, Ю.Л. Скобелин, С.Ю. Классификация цифровых следов преступлений. / Ю.Л. Соловьева, С.Ю. Скобелин // БЮИ МВД России. Барнаул, 2021. №2. С. 417 – 418.
46. Суслопаров, А. В. Информационные преступления. авт. дис … канд. юрид. наук / А. В. Суслопаров Красноярск, 2008. – 23 с.
47. Суслопаров, А. В. Компьютерные преступления как разновидность преступлений информационного характера: Дис. … канд. юрид. наук: 12.00.08 / А.В. Суслопаров. Красноярск, 2010. – 206 с.;
48. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовноправовые меры борьбы: Дис. … канд. юрид. наук / Т. Л. Тропина Владивосток, 2005. – 235 с.;
49. Тушканова, О.В Криминалистическое исследование компьютерной информации / Криминалистика : учебник для бакалавров / под ред. Л.В. Бертовского. // РГ-пресс. М., 2018. С. 365-375.
50. Федотов, Н. Н. Форензика – компьютерная криминалистика. / Н.Н. Федотов // Юридический мир. М., 2007. С. 254 – 255.
51. Чекунов, И. Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И.Г. Чекунов // Право и кибербезопасность. М., Юрист. 2012. С. 9 – 22.
52. Шевченко, Е. С. О криминалистической трактовке понятия «киберпреступность» / Е.С. Шевченко // Информационное право. 2014. № 3 (39). С. 29 – 32.
53. Шевченко, Е. С. Тактика производства следственных действий при расследовании киберпреступлений: дис. … кан. юрид. наук / Е.С. Шевченко. М., 2016 С. 101.
54. Яковлев, А. Н. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем: научно-методическое пособие / А. Н. Яковлев; Н. В. Олиндер. М., 2012. – 182 с.

РАЗДЕЛ IIIПОСТАНОВЛЕНИЯ ВЫСШИХ СУДЕБНЫХ ИНСТАНЦИЙ И МАТЕРИАЛЫ ЮРИДИЧЕСКОЙ ПРАКТИКИ

1. Апелляционное определение Судебной коллегии по уголовным делам Оренбургского областного суда от 03.11.2016 по делу № 22-4229/2016. URL: https://oblsud-orb.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=1369693&delo_id=4&new=4&text_number=1
2. Апелляционное постановление Челябинского областного суда от 23 апреля 2018 г. № 10 – 1934/2018. URL: //sudact.ru/regular/doc/7sZpql1IrkZd/
3. Приговор Центрального районного суда г. Челябинска Челябинской области от 17 июня 2019 г. по делу № 1 - 297/2019. URL: //sudact.ru/regular/doc/nEzPAOLxrPlT/ (дата обращения: 17.01.2021)
4. Приговор Октябрьского городского суда республики Башкортостан от 29 июля 2020 г. по делу 1 - 243/2020. URL: //sudact.ru/regular/doc/eLKpELsMEF5w/ (дата обращения: 17.01.2021)
5. Приговор Калужского районного суда Калужской области от 25 ноября 2019 г. по делу № 1-1084/2019. URL: //sudact.ru/regular/doc/sOj2ljzYGvr5/ (дата обращения: 17.01.2021)
6. Приговор Комсомольского районного суда г. Тольятти Самарской области от 21 июля 2020 г. по делу №1 - 278/2020. URL: //sudact.ru/regular/doc/zn9pbUgYsooY/ (дата обращения: 17.01.2021)
7. Приговор Дмитриевского городского суда Ульяновской области от 16 июля 2018 по делу №1-176/2018 URL: //sudact.ru/regular/doc/jiaWOZeD0exK/
8. Приговор Краснодарского краевого суда от 23 июля 2019 по делу №2 - 8/2019 URL: //sudact.ru/regular/doc/PDXLfJbOWeLu/

9. Приговор Павловского районного суда Воронежской области от 25 ноября 2020 г. № 1 – 40/2020. URL: //sudact.ru/regular/doc/KL22CmxCcxU/

РАЗДЕЛ IV ЭЛЕКТРОННЫЕ РЕСУРСЫ

1. Гудин Д. Эксперимент Билли Риос и Джонатан Баттс по взлому кардиостимулятора CareLink 2090. URL: https://arstechnica.com/information-technology/2018/08/lack-of-encryption-makes-hacks-on-life-saving-pacemakers-shockingly-easy/ (дата обращения 05.01.2021).
2. Краткая характеристика состояния преступности в Российской Федерации за январь ноябрь 2020 г. Официальный сайт МВД РФ. URL: https://xn--b1aew.xn--p1ai/reports/item/22501861/ (дата обращения: 05.01.2012).
3. Интервью И.К. Сачкова РИА Новости. URL: https://ria.ru/20200707/1573997584.html (дата обращение 05.01.2012)
4. Доклад ООН Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств – членов, международного сообщества и частного сектора // Документ ООН (UNODC/ CCPCJ/EG.4/2013/2: UNODC.ComprehensiveStudyonCybercrime, February 2013, P. XVII). URL: https://www.unodc.org/documents/organized crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (дата обращения 10.01.2021).
5. Компьютерно-техническая экспертиза. Сайт Российский федеральный центр судебной экспертизы при Министерстве юстиций РФ. URL: http://www.sudexpert.ru/possib/comp.php
6. МВД и Group-IB задержали мошенников, похищавших деньги у VIP-клиентов банков с помощью клонов SIM-карт. Официальная страница Group-IB. URL: https://www.group-ib.ru/media/sim-cards-clones/
7. Закупка в рамках ГОЗ. Аппаратно-программный комплекс для съема, исследования и анализа данных из мобильных устройств тип 1,2,3,4.

Официальный сайт Единой информационной системы в сфере закупок. URL: https://zakupki.gov.ru/epz/order/notice/ea44/view/common info.html?regNumber=0373100056021000093

8. Программный комплекс для криминалистических исследований UFED. URL: https://bakotech.ua/uploads/product/280/files/556/file.pdf
9. Вирусные аналитики компании «Доктор Веб» зафиксировали распространение троянца Android.BankBot.358.origin, который нацелен на клиентов Сбербанка. URL: https://news.drweb.ru/show/?lng=ru&i=11802&c=9

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

Отчет о проверке на заимствования №1

Автор: УНИВЕРИС univeris@susu.ru / ID: 640
Проверяющий: (univeris@susu.ru / ID: 640)
Организация: Южно-Уральский государственный университет

Отчет предоставлен сервисом «Антиплагиат» - http://susu.antiplagiat.ru

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 241890
Начало загрузки: 01.06.2021 21:15:51
Длительность загрузки: 00:00:32
Имя исходного файла: Основная часть.docx
Название документа: Основная часть.docx
Размер текста: 127 кБ
Символов в тексте: 130370
Слов в тексте: 15373
Число предложений: 865

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 01.06.2021 21:16:25
Длительность проверки: 00:07:11
Комментарии: не указано
Поиск перефразирований: да
Модули поиска: Перефразирования по Интернету, Шаблонные фразы, Интернет Плюс, Сводная коллекция РГБ, Диссертации НББ, Кольцо вузов, Цитирование, eLIBRARY.RU, СПС ГАРАНТ, Перефразирования по eLIBRARY.RU, Сводная коллекция ЭБС, Медицина, Переводные заимствования (RuEn), ИПС Адилет, Библиография, Переводные заимствования по eLIBRARY.RU (EnRu), Переводные заимствования по Интернету (EnRu), Переводные заимствования издательства Wiley (RuEn), Патенты СССР, РФ, СНГ, СМИ России и СНГ, Модуль поиска "ЮУрГУ", Издательство Wiley, Переводные заимствования

ЗАИМСТВОВАНИЯ	САМОЦИТИРОВАНИЯ	ЦИТИРОВАНИЯ	ОРИГИНАЛЬНОСТЬ
26,83%	0%	8,34%	64,83%