Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение

высшего образования
«Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)»

Университет имени О.Е. Кутафина (МГЮА)

Северо-Западный институт (филиал) Университета имени О.Е. Кутафина (МГЮА)

КАФЕДРА УГОЛОВНОГО ПРОЦЕССА И КРИМИНАЛИСТИКИ

КУРСОВАЯРАБОТА

по дисциплине Криминалистика

**Тема: Киберпреступления: криминалистическая характеристика и особенности расследования**

Выполнил: студент 4 курса
4 группы очной формы обучения
Будилов Андрей Михайлович

Проверил:

Вологда – 2016

**ОГЛАВЛЕНИЕ**

[**ВВЕДЕНИЕ** 3](#_Toc468523049)

[**ГЛАВА 1. КИБЕРПРЕСТУПЛЕНИЯ: КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ.** 6](#_Toc468523050)

[§ 1. Криминалистическая характеристика и классификация киберпреступлений 6](#_Toc468523051)

[§ 2. Составы киберпреступлений, закрепленные в Уголовном кодексе РФ 9](#_Toc468523052)

[3. Понятие и классификация виртуальных следов киберпреступлений 11](#_Toc468523053)

[**ГЛАВА 2. ТАКТИКА ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ НА ПЕРВОНАЧАТЕЛЬНОМ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ.** 13](#_Toc468523054)

[§ 1. Тактика проведения осмотра места происшествия 13](#_Toc468523055)

[§ 2. Обыск и выемка при расследовании киберпреступлений 16](#_Toc468523056)

[§ 3 Особенности проведения следственного эксперимента 20](#_Toc468523057)

[§ 4. Назначение и виды судебных экспертиз при расследовании киберпреступлений 22](#_Toc468523058)

[**ЗАКЛЮЧЕНИЕ** 27](#_Toc468523059)

[**СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ** 28](#_Toc468523060)

# **ВВЕДЕНИЕ**

Актуальность темы исследования, обосновывается тем, что число совершенных киберпреступлений возрастает и охватывает все новые и новые деяния. Преступность в сфере информационных технологий в текущих реалиях выступает одной из ключевых угроз национальной безопасности Российской Федерации в информационной сфере. Количество киберпреступлений напрямую зависит от числа интернет-пользователей. Расследование компьютерных преступлений обусловлено спецификой совершенных преступником действий, слабой теоретический проработкой вопроса методики организации расследования киберпреступлений, и индивидуальностью тактики производства следственных действий под отдельно взятое преступление; несомненно, влияет и недостаточная квалификация следователей для работы со специфическими источниками информации, представленной в виде электронных страниц, сайтов и т.д. В связи с ростом числа киберпреступлений, оформлением более профессиональных способов их совершения проблема изучения криминалистических особенностей расследования киберпреступлений является насущной.

**Степень разработанности проблемы другими авторами:** криминалистические особенности киберреступлений изучались многими авторами, вопросы касаемо выделения данных преступлений в отдельную группу в системе криминалистической классификации; описание методики их расследования; возможность использования виртуальных следов, и другие рассматривались В. Ю. Агибаловым, М. А. Бабаковой, В. Б. Веховым, А. С. Вражновым, А. А. Васильевым, Ю. В. Гаврилиным, В. В. Крыловым, В. А. Мещеряковым, Д.А. Илюшиным, В. В. Степановым, А. И. Семикаленовой, А. И. Усовым и другими.

**Объектом исследования** являются: криминалистическая характеристика киберпреступлений и особенности производства следственных действий по данной категории преступлений.

**Предметом** исследования является: закономерности совершения преступлений в киберпространстве и закономерности образования их следов; практика производства следственных действий; теоретические положения уголовного права, криминалистики и уголовного процесса в аспекте производства следственных действий.

**Целью исследования** является рассмотрение теоретических и практических аспектов киберпреступлений, их криминалистическая характеристика, изучение возможности использования виртуальных следов при расследовании киберпреступлений. Данная цель разрешается через связанные с ней задачи:

–провести криминалистическую классификацию киберпреступлений;

–охарактеризовать особенности тактики производства следственных действий при расследовании киберпреступлений;

–рассмотреть особенности назначения и виды судебных экспертиз при расследовании киберпреступлений.

**Методологическую основу составляют различные методы, в первую очередь** диалектический метод познания. Также, в работе использовались: общелогические методы, метод системного анализа и метод статистического сравнения, обобщение материала и др.

**Нормативную правовую основу исследования** составляют нормы международного права, Конституция Российской Федерации, Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, иные нормативно-правовые акты по исследуемой теме,

**Научная новизна** работы подтверждается комплексным изучением и анализом производства следственных действий при расследовании киберпреступлений на первоначальном этапе. Изучена криминалистическая классификация преступлений в киберпространстве.

**Теоретическая значимость** заключается в том, что сформулированные выводы могут быть основой для теоретических исследований в данной сфере.

**Практическая значимость** заключается в возможности применения выводов и предложений в практической деятельности органов предварительного расследования.

**Работа структурно** состоит из введения, двух глав, заключения и списка использованной литературы. Во введении обосновывается актуальность темы курсовой работы, ставятся цели и задачи исследования. В первой главе рассматриваются особенности криминалистической характеристики и классификация киберпреступлений и примеры киберпреступлений закрепленных в Уголовном кодексе РФ, а также рассмотрен вопрос виртуальных следов преступления Во второй главе курсовой работы рассматриваются отдельные следственные действия на первоначальном этапе расследования, такие как осмотр места происшествия, обыск (выемка) и следственный эксперимент, отдельно рассмотрен вопрос назначения и видов экспертиз. В заключении подводится итог проведенному исследованию.

# **ГЛАВА 1. КИБЕРПРЕСТУПЛЕНИЯ: КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ**

## § 1. Криминалистическая характеристика и классификация киберпреступлений

Киберпреступление – это общественно опасное деяние, совершаемое в киберпространстве, посягающее на общественную безопасность, собственность, права человека, другие охраняемые законом отношения, необходимым элементом механизма подготовки, совершения, сокрытия и отражения которого является компьютерная информация, выступающая в роли предмета или средства преступления.[[1]](#footnote-1)

Под криминалистической характеристикой понимается совокупность наиболее характерной криминалистически значимой информации о признаках и свойствах такого ряда преступлений, способной служить основанием для выдвижения версий о событии преступления и личности преступника, позволяющей верно оценить ситуации, возникающие в процессе раскрытия и расследования компьютерных преступлений, обусловливающей применение соответствующих методов, приемов и средств. Киберпреступления характеризуются высокой латентностью, сложностью сбора доказательств и процесса доказывания, широким спектром криминалистическизначимых признаков, отсутствием единой программы борьбы с киберпреступлениями и отсутствием обобщенной судебной и следственной практики по делам данной категории.

Необходимо выделить криминалистически значимые элементы характеристики киберпреступлений, такие как: способ совершения преступления; особенности следовой информации и обстановки совершения преступления; личностная характеристика преступника; особенности непосредственного предмета преступного посягательства.

Криминалистическая классификация преступлений активно применяется в ходе следственной деятельности, так как помогает обеспечить правильное понимание сути событий, выбор и применение криминалистических методик расследования отдельных видов киберпреступлений. На основе положений Конвенции Совета Европы о киберпреступности можно выделить пять групп киберпреступлений: Во-первых, преступления посягающие на конфиденциальность, целостность и недоступность компьютерных данных и систем, например: несанкционированный доступ, незаконный перехват, вмешательство в базы данных и в систему. Во-вторых, преступления, связанные с использованием компьютера как средства совершения противозаконных действий, например, компьютерное мошенничество. В-третьих, преступления, связанные с размещением данных в сети «Интернет». В-четвертых, преступления, связанные с нарушением авторских и смежных прав, при этом установление таких правонарушений Конвенцией отнесено к компетенции национальных законодательств государств. В-пятых преступления, связанные с распространением в сети «Интернет» расистских и ксенофобских материалов. Многообразие киберпреступлений требует их систематизации по различным основаниям. Криминалистическая классификация должна исходить из соблюдения правил и принципов логического деления не самих объектов реальной действительности, а объёма их понятий. Д.А. Ильюшин выделяет следующие виды киберпреступлений:

1) Неправомерное подключение к информационно-телекоммуникационной сети Интернет.

2) Создание, использование и распространение сетевых вредоносных программ.

3) Незаконное изготовление, хранение, распространение, рекламирование и (или) публичная демонстрация информации, запрещённой к свободному обороту, совершённое с использованием сети Интернет.

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

5) Компьютерное мошенничество.

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.[[2]](#footnote-2)

По предмету преступного посягательства преступления подразделяются на преступления, имеющие материальный предмет посягательства, и преступления, не имеющие такового. По численности субъектов преступления – совершённые одним лицом; группой лиц.

В. А. Мещеряков классифицирует преступления в сфере компьютерной информации по объекту преступного посягательства – компьютерной информаций. На основе этого критерия выделяет следующие виды:

1. Уничтожение (разрушение) компьютерной информации.

2. Неправомерное завладение компьютерной информацией или нарушение исключительного права на её использование:

1. Неправомерное завладение алгоритмом (методом) преобразования компьютерной информации;
2. Неправомерное завладение совокупностью сведений, документов – нарушение исключительного права владения;
3. Неправомерное завладение компьютерной информацией как товаром.

3. Действия или бездействие по созданию компьютерной информации с заданными свойствами:

1. Распространение по телекоммуникационным каналам информационно-вычислительных сетей компьютерной информации, наносящей ущерб абонентам;
2. Разработка и распространение компьютерных вирусов и прочих вредоносных программ для ЭВМ.

4. Неправомерная модификация компьютерной информации:

1. Неправомерная модификация компьютерной информации как совокупности фактов, сведений;
2. Неправомерная модификация компьютерной информации как алгоритма;
3. Неправомерная модификация компьютерной информации как товара с целью воспользоваться её полезными свойствами. [[3]](#footnote-3)

Формирование теории криминалистической классификации киберпреступлений способствует наиболее правильному выбору тактики и методики расследования киберпреступлений, с практической точки зрения криминалистическая классификация необходима для гарантии всесторонности и полноты расследования. Дальнейшая разработка теоретических основ криминалистической классификации киберпреступлений обусловлена потребностями криминалистической теории и практики выявления и расследования преступлений в сфере высоких технологий.

## § 2. Составы киберпреступлений, закрепленные в Уголовном кодексе РФ

Российское законодательство не содержит понятия киберпреступления. В свою очередь, Уголовном кодексе РФ (далее - УК РФ) есть глава 28 «Преступления в сфере компьютерной информации», в которую включены общественно опасные деяния, предусмотренные ст.: 272 Неправомерный доступ к компьютерной информации; ст. 273 Создание, использование и распространение вредоносных компьютерных программ; ст. 274 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Кроме преступлений в сфере компьютерной информации, к киберпреступлениям относятся и другие деяния, предусмотренные в УК РФ:, например ст. 128.1 «Клевета»; ст. 137 «Нарушение неприкосновенности частной жизни»; ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»; ст. 146 «Нарушение авторских и смежных прав»; ст. 159.6 «Мошенничество в сфере компьютерной информации»; ст.171 «Незаконное предпринимательство»; ст.183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»; ст. 205.1 «Содействие террористической деятельности»; ст. 205.2 «Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма»; ст. 207 «Заведомо ложное сообщение об акте терроризма»; ст. 242.1 «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних»; ст. 276 «Шпионаж»; ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства»; ст. 283.1 «Незаконное получение сведений, составляющих государственную тайну»; ст. 319 «Оскорбление представителя власти» и др.[[4]](#footnote-4)

Объединяет приведенные виды преступлений фигурирование при их совершении компьютерной информации как элемента взаимодействия и отражения механизмов подготовки, совершения и сокрытия этих преступных деяний, а также выступающей в роли предмета или средства преступления.

Под компьютерной информацией применительно к процессу доказывания понимаются фактические данные, обработанные компьютерной системой и (или) передающиеся по телекоммуникационным каналам, доступные для восприятия человеком, на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение по делу. Данный вид информации фиксируется в файле, машинной распечатке или на различных электронных носителях.[[5]](#footnote-5)

##  3. Понятие и классификация виртуальных следов киберпреступлений

Киберпреступления характеризуются специфической картиной следов, на месте происшествия одновременно с обычными следами имеют место быть виртуальные следы, находящиеся в памяти электронных устройств.

Виртуальные следы представляют собой следы совершения любых действий в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей. В. Мещеряков под виртуальными следами понимает «любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации. Данные следы занимают условно промежуточную позицию между материальными и идеальными следами» [[6]](#footnote-6)

Категория компьютерных следов остается в памяти, как компьютерных, так и в памяти иных цифровых устройств. Так, В. Агибаловым считает, что в результате электронно-цифрового отражения на материальном носителе фиксируется образ из цифровых значений параметров формальной математической модели наблюдаемого реального физического явления.

А. Волеводз выдвинул классификацию виртуальных следов на основании непосредственного физического носителя следов:

1. Следы на жестком диске, магнитной ленте, оптическом диске, на дискете;
2. Следы в оперативных запоминающих устройствах ЭВМ, периферийных устройств, компьютерных устройств связи и сетевых устройств;
3. Следы в проводных и других электромагнитных системах и сетях связи.[[7]](#footnote-7)

Л.Б. Красновой предложена классификация виртуальных следов по механизму следообразования на первичные и вторичные следы. Первичные формирует непосредственное воздействие пользователя с использованием какой-либо информационной технологии, а вторичные – в результате воздействия технологических процессов без участия человека.[[8]](#footnote-8)

Любые действия с высокоточными устройствами оставляют свой след в их памяти. Наиболее явными в данном случае выступают следы в памяти компьютера, которые подразделяются на следы включения и выключения, а также следы различных операций с содержимым памяти, следы действий с программами и сведения о работе в сети Интернет, локальных и иных сетях.

Виртуальные следы являются доказательствами совершения или планирования преступления конкретным лицом или группой лиц. Они указывают на уровень профессионализма преступника.

На первоначальном этапе фиксации виртуальных следов производится описание в протоколе, сведений о том в памяти какого устройства обнаружены виртуальные следы; кому принадлежит устройство; имеет ли устройство выход в сеть Интернет, локальные и иные сети; оперативная система устройства в каких файлах и какие обнаружены следы; когда файл был создан, изменен. Затем выполняется фотографирование экрана с выведенной информацией о свойствах исследуемых файлов, журналов администрации. После чего происходит изъятие для исследования объекта с виртуальными следами.**[[9]](#footnote-9)**

# **ГЛАВА 2. ТАКТИКА ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ НА ПЕРВОНАЧАТЕЛЬНОМ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ**

## § 1. Тактика проведения осмотра места происшествия

В соответствии с правилами ст. 176 УПК РФ, осмотр места происшествия (далее – ОМП) производится в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела.[[10]](#footnote-10) Обнаружение, фиксация и изъятие виртуальных следов киберпреступления сопряжены с временными и техническими трудностями, поэтому помимо общих требований порядка проведения ОМП, установленных в ст. 177 УПК РФ, необходимо учитывать и специфику данного рода преступлений. При производстве ОМП возникает необходимость осмотра информационных объектов задействованных в преступлении. Распознавать и фиксировать приходится не материальные объекты, а кибернетическое пространство, образованное средствами вычислительной сети, сегментом локальной сети или глобальной сети Интернет, а также всевозможными цифровыми носителями компьютерной информации, в котором могут находиться виртуальные следы. Осмотр места совершения преступления в киберпространстве связан с необходимостью обнаружения таких следов, для восприятия которых требуется специальное аппаратное обеспечение и подготовительные действия.

При проведении осмотра места происшествия возможно применение противодействия со стороны преступника или группы лиц. Преступник всеми усилиями будет препятствовать установлению обстоятельств совершенного им преступления в связи с тем, что изначально преступление спланировано и совершено так, чтобы оно не было выявлено. Поэтому следователь должен, по возможности, обеспечить тайну проведения осмотра места происшествия при расследовании киберпреступлений. Однако, лица совершившие преступления в сфере информационных технологий, как правило, опытные пользователи и пользователи-специалисты с высоким интеллектуальным уровнем и могут выявить постороннее вмешательство в их деятельность. С целью исключения данного тактического риска при расследовании киберпреступлений необходимо:

– ограничить, а в отдельных случаях сделать невозможным, вход и выход с компьютеров, на которых имеется информация;

– продолжать деятельность в глобальной сети с тем, чтобы не привлекать к действиям, направленным на расследование преступления, излишнего внимания;

– определить последовательность действий, по расследованию преступления, так, чтобы действия по отношению к лицам, по поводу которых есть сомнения, что они будут хранить тайну, были совершены в последнюю очередь после формирования доказательственной базы;

– следственные действия, связанные с изъятием или выемкой, проводить в то время, когда можно избежать присутствия большого количества очевидцев;

– к проведению следственных действий в качестве понятых желательно привлекать лиц, не связанных с деятельностью конкретного юридического лица, или, если это физическое лицо незнакомо последнему;

– осуществлять постоянный контроль всех исходящих и входящих сообщений из конкретного подразделения занятого расследованием преступления в сфере компьютерной информации;

– выявить дефекты в системе защиты информации в устройстве, принадлежащему потерпевшему;

– выявить скрытые угрозы для системы информации, хранящейся на компьютере, на котором была изменена или уничтожена информация. [[11]](#footnote-11)

Для того чтобы следователь был уверен в сохранении следов и необходимой информации по преступлению и мог избежать уничтожения или повреждения искомой информации, необходимо чётко спланировать рассматриваемое следственное действие, а также подготовиться к нему.

Для эффективного проведения осмотра компьютерной техники, если это возможно, следователю необходимо провести подготовительные мероприятия. Необходимо изучить схему расположения удалённых устройств и связь между ними, а также выяснить наличие электронных охранных средств, произвести работу по извлечению необходимой, криминалистически значимой информации, расшифровать файлы, которые содержат доказательственную базу данных, и найти, а также извлечь прочие виртуальные следы.

Для обнаружения виртуальных следов должен быть проведён осмотр технического средства, материального носителя компьютерной информации с целью обнаружения типовыми стандартными средствами и приёмами виртуальных следов с последующим изготовлением копии информационного содержания носителя и назначения экспертного исследования. В связи с этим следователь должен позаботиться о материально-техническом обеспечении осмотра, что позволит собрать максимальное количество информации, относимой к расследованию преступления.

К стандартным средствам и приёмами для обнаружения виртуальных следов можно отнести:

– специальные программы

– программно-аппаратные средства для криминалистического исследования компьютерных носителей информации «EnCase Forensic Edition»

– технические средства.

Если следователь посчитает нужным привлечь понятых для осмотра места происшествия киберпреступления, то они должны обладать знаниями и являться сами пользователями компьютерной техники.

После окончания выявления и изъятия материальных следов необходим осмотр компьютера и киберпространства, задействованного в совершении киберпреступления. Необходимо посмотреть, в каком состоянии находится компьютер. В случае, если компьютер выключен, его необходимо оставить в выключенном состоянии, для того чтобы избежать возможного уничтожения информации. Необходимо осмотреть общий внешний вид компьютера, на наличие на нем: механических повреждений; пометок, специальных знаков, пломб и прочего. Установить с участием специалиста: вид, назначение и технические возможности компьютера.

Осмотр работающего компьютера должен начинаться с осмотра изображения на экране дисплея. Далее следователь, с участием специалиста, в случае, если на компьютере запущена не относящаяся к киберпреступлению программа, то она останавливается. Специалист выясняет, какая операционная система установлена на компьютере, какие используются протоколы связи, службы доступа к файлам и сети, как локальной, так и сети Интернет. Исследует информацию в компьютере и в той части киберпространства, которая была задействована в совершении преступления. Затем обнаруженные виртуальные следы, электронные документы и иную значимую информацию для дела, специалист фиксирует и изымает. При необходимости, если это рекомендует специалист, может изыматься весь компьютер или компьютерный блок.

## § 2. Обыск и выемка при расследовании киберпреступлений

Общие основания и порядок проведения обыска и выемки установлены статьями 182 и 183 УПК РФ. Так, согласно ст. 182 УПК РФ, основанием производства обыска является наличие достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться орудия, оборудование или иные средства совершения преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела. В соответствии со ст. 183 УПК РФ определённые предметы и документы, имеющие значение для уголовного дела, при необходимости могут быть изъяты. [[12]](#footnote-12)

При расследовании киберпреступлений при производстве следственных действий, направленных на получение виртуальной информации, проведение обыска и выемки имеет свои особенности. Производство обыска (выемки) при расследовании рассматриваемых преступлений, связано с получением доказательств о способе совершения преступления, обусловленного использованием компьютерной техники и телекоммуникационных сетей. Главной целью производства обыска при расследовании киберпреступления является обнаружение и изъятие компьютерной техники, на которой остались следы киберпреступления, компьютерной информации, касающейся как самого киберпреступления и лиц, совершивших это преступление, предметы, являющиеся результатом преступления и (или) документы, содержащие важную информацию для дела.

Результативность обыска при расследовании киберпреступлений во многом обусловлена тщательной подготовкой к его производству. Так, на подготовительном этапе обыска следователю необходимо:

1. Провести анализ исходной информации, определить вид, содержание компьютерной информации, предположительно находящейся у преступника; выяснить, на каких материальных носителях может храниться искомая информация; какая компьютерная техника, относящаяся к совершенному преступлению, может находиться в месте обыска.

2. Собрать информацию о месте проведения обыска (выемки): точный адрес этого места; характеристика строения; планировка помещений; есть ли телефонная связь, работающий модем; есть ли локальная и (или) глобальная сети; подключена ли беспроводная сеть Wi-Fi; соединена ли компьютерная техника между собой локальной сетью; где находится система электропитания; место прокладки телекоммуникационных кабелей.

Эту информацию можно получить как из материалов уголовного дела, так и из иных источников, например, для выяснения информации о подключении к телекоммуникационным услугам (телефонная сеть, сеть Интернет, беспроводная сеть Wi-Fi, локальная сеть и прочее), можно обратиться к оператору связи, обслуживающему интересующий адрес.

3. Изучить личность обыскиваемого и лиц, проживающих либо работающих совместно с ним в одном помещении. Важно получить информацию о его навыках работы с компьютерной техникой и телекоммуникационными сетями, профессиональных знаниях, о месте работы и должности.

4. Подготовить материально-техническое обеспечение, что предварительно согласовывается со специалистом, который будет оказывать содействие при производстве обыска.

5. Подобрать участников обыска (выемки). Обязательными участниками производства обыска при расследовании киберпреступлений являются специалист и понятые. Специалиста следователь должен подобрать, исходя из цели обыска Понятые должны быть подобраны с учетом наличия у них навыков работы с компьютерной техникой и телекоммуникационными сетями. Понятыми, например, в этом случае могут стать студенты профильных ВУЗов и факультетов, например, вычислительной математики и кибернетики. [[13]](#footnote-13)

После выполнения всех подготовительных действий следователю необходимо незамедлительно приступить к производству обыска (выемки).

По прибытии на место обыска и выемки, войдя в помещение, следователь должен ознакомить обыскиваемого с постановлением и судебным решением о производстве обыска (выемки) и предложить добровольно выдать искомые предметы. В случае отказа следователю необходимо всех лиц, находящихся в обыскиваемом помещении, собрать в одном месте и незамедлительно запретить доступ к компьютерной технике.

Поисковые мероприятия при производстве обыска делятся на две стадии: обзорную и детальную. При производстве обзорной и детальной стадий следователь должен придерживаться как общих тактических положений производства обыска (выемки), так и учитывать отдельные специфические особенности, присущие киберпреступлениям.

При производстве обыска (выемки) при расследовании киберпреступлений следует выделить ряд особенностей:

На обзорной стадии необходимо:

1. Провести осмотр всего помещения. В связи с тем, что искомый объект находится в форме компьютерной информации, в первую очередь нужно обратить внимание на компьютерную технику, находящуюся в помещении, на ее расположение, состояние, а также на состояние телекоммуникационных сетей. При осмотре помещения следует произвести поиск портативных запоминающих устройств, в том числе замаскированных.

2. Необходимо определить подключение компьютера к локальным и телекоммуникационным сетям. Если в обыскиваемом помещении компьютеров несколько, то с помощью специалиста определить базовый и начать обыск с него.

3. На компьютере необходимо проверить наличие средств защиты информации, вирусных программ и удалённого доступа. В случае их наличия, следует отключить специальные средства защиты информации, первую очередь автоматически уничтожающие всю информацию при несанкционированном доступе, а также блокировать на компьютере удалённый доступ.

4. При осмотре компьютера, определить: какая операционная система установлена: какие были выполнены операции и какие использовались программы, начиная с включения компьюте. Изображение на экране компьютера необходимо снять на видео (либо с помощью скриншота), в случае необходимости, выполняемые программы остановить.

5. При осмотре работающего компьютера: с помощью специалиста в случае, если нет угрозы уничтожения компьютерной информации, следует провести поиск компьютерной информации, имеющей значения для расследуемого преступления, в осматриваемом компьютере. Поиск проводится, исходя из известных сведений об искомой информации.

После проведения осмотра компьютера он по всем правилам выключается, упаковывается и изымается.

При осмотре неработающего компьютера: зафиксировать его месторасположение, а также его периферийных устройств; определить и зафиксировать соединения компьютера с телекоммуникационными сетями, периферийным оборудованием и иными устройствами; разъединить устройства с компьютером и подготовить для упаковки и изъятия.

6. При обнаружении на месте обыска (выемки) мобильного телефона, смартфона или планшетного компьютера для поиска в них нужной информации, относящейся к расследуемому преступлению, совместно со специалистом

В случае, когда нет возможности предварительно исследовать информацию в мобильном устройстве, устройство необходимо изъять.

После производства обыска (выемки) вся обнаруженная компьютерная техника, содержащая искомую информацию по расследуемому киберпреступлению, перед изъятием должна быть правильно упакована и опечатана. По окончании обыска (выемки) составляется протокол следственного действия и описи к нему.

## § 3 Особенности проведения следственного эксперимента

В соответствии со ст. 181 УПК РФ в целях проверки и уточнения данных, имеющих значение для уголовного дела, а также для установления их достоверности и получения новых доказательств, следователь вправе произвести следственный эксперимент путём воспроизведения действий, а также обстановки или иных обстоятельств определённого события. При этом проверяется возможность восприятия каких-либо фактов, совершения определённых действий, наступления какого-либо события, а также выявляются последовательность происшедшего события и механизм образования следов. [[14]](#footnote-14)

Следственный эксперимент необходим для устранения сомнений, в знаниях подозреваемого (обвиняемого) в области телекоммуникационных систем и компьютерной техники. В случае необходимости проверки времени подготовки, совершения и сокрытия преступления, получения доказательств совершения преступления лицом с использованием конкретной компьютерной технологии.

Виды следственного эксперимента проводимого при расследовании киберпрестулений зависят от способов совершения преступления. Могут быть проведены следственные эксперименты: по проверке возможности подключения компьютерной техники и совершения действий с использованием определённой криминальной (компьютерной) технологии; по проверке подбора паролей, идентификационных кодов и установлению периода времени для данного подбора; по проверке возможности подключения к компьютерной сети и использования криминальной технологии; по проверке возможности электромагнитного перехвата; по установлению периода времени, необходимого на отключение технических средств защиты информации и времени для модификации, копирования информации; по проверке возможности совершения определённых действий в киберпространстве. Перед производством следственного эксперимента необходимо проведение подготовительных мероприятий:

1. Выяснение технических условий на момент совершения киберпреступления и их воссоздание.

Главным из условий сходства с моментом совершения преступления при проведении следственного эксперимента при расследовании киберпреступлений является использование подлинного или аналогичного технического средства, которым мог пользоваться преступник.

По общему правилу, нет необходимости восстанавливать обстановку помещения при производстве следственного эксперимента, поскольку обстановка в реальности не влияет на киберпространство. Однако, в случае, если необходимо провести следственный эксперимент для проверки возможности доступа к компьютерной информации, связанного с проникновением преступника в помещение, где установлены средства компьютерной техники, реконструкция необходима.

2. Согласовать содержание действий со специалистом в области тех информационных технологий, с помощью которых было совершено преступление. Специалист сможет правильно разъяснить, какие необходимо произвести действия во время следственного эксперимента, чтобы достичь преступного результата.

3. Необходимо заранее подготовить все научно-технические средства, компьютерную технику и другие технические средства, которые будут необходимы для проведения следственного эксперимента. Технические средства для следственного эксперимента подбираются в соответствии с материалами дела и показаниями допрашиваемых лиц.

4. Определить круг участников следственного эксперимента понятые должны располагать навыками работы на компьютере; возможно участие переводчика, педагога. По усмотрению следователя, в следственном действии может принимать участие обвиняемый, потерпевший, свидетель и специалист, участие в данном случае специалиста способствует разъяснению содержания действия. В случае если лицо захочет ввести следователя в заблуждение специалист способен и предупредить об этом. [[15]](#footnote-15)

## § 4. Назначение и виды судебных экспертиз при расследовании киберпреступлений

Основной формой использования специальных знаний по киберпреступлениям является судебная экспертиза. В зависимости от обстоятельств дела могут быть назначены следующие виды компьютерно-технической экспертизы: аппаратно-компьютерная; программно-компьютерная; информационно-компьютерная; компьютерно-сетевая экспертиза.

Аппаратно-компьютерная экспертиза исследует аппаратные средства компьютерной системы – материальные носители информации. К объектам аппаратно-компьютерной экспертизы относятся: персональные компьютеры; периферийные устройства; сетевые аппаратные средства; комплектующие.

Программно-компьютерная экспертиза – исследование программного обеспечения компьютерной системы; информационно-компьютерная – поиск, обнаружение, анализ и оценка информации, подготовленной пользователем или созданной программами для организации информационных процессов в компьютерной системе; компьютерно-сетевая экспертиза – решение аппаратных, программных и информационных аспектов установления фактов и обстоятельств по делам (объекты функционируют в сети).

В настоящее время в рамках компьютерно-технической экспертизы формируется новый вид – компьютерно-техническая экспертиза устройств сотовой связи, к объектам исследования которой можно отнести: мобильные телефоны, смартфоны, планшетные компьютеры, sim-карты, а также комплектующие и т. п.

Однако, в настоящее время нет единого подхода как к названию компьютерно-технической экспертизы, так и к пределам компетенции экспертов. Производство экспертизы поручается специализированным экспертным учреждениям, как Министерства юстиции РФ, так и Министерства внутренних дел России, которые по-разному именуют в ведомственных документах подобные экспертизы.

В Министерстве юстиции Российской Федерации этот вопрос регламентирован приказом от 27.12.2012 г. № 237. Данный вид экспертизы именуется как «компьютерно-техническая экспертиза».[[16]](#footnote-16)

В МВД России вопрос регулируется приказом от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации». Для обозначения подобной экспертизы используется термин «компьютерная экспертиза», предметом исследования которой является исследование компьютерной информации.[[17]](#footnote-17)

Программно-компьютерная экспертиза назначается для исследования программного обеспечения компьютерной системы. Компьютерно-сетевая экспертиза - решение аппаратных, программных и информационных аспектов установления фактов и обстоятельств по делам (объекты функционируют в сети).

Информационно-компьютерная экспертиза – это экспертное исследование, направленное на поиск, обнаружение, анализ и оценку информации, подготовленной пользователем или созданной программами для организации информационных процессов в компьютерной системе.

Судебная компьютерно-техническая экспертиза при расследовании киберпреступлений зачастую назначается на первоначальном этапе расследования, когда уже проведены осмотр места происшествия, обыск и выемка, однако, информации для дальнейшего расследования недостаточно.

После принятия решения о производстве экспертизы возникает необходимость указать разновидность судебной компьютерно-технической экспертизы. Хотя, ряд ученных считают, что следователю достаточно определить род экспертизы, а эксперт после анализа вопросов и оценки объектов укажет на конкретный вид экспертизы.

Информационное взаимодействие следователя и эксперта происходит в двух направлениях: следователь обеспечивает эксперта заданием и необходимой для его исполнения информацией, эксперт передаёт информацию об обстоятельствах, по которым были поставлены вопросы.

Важным элементом назначения экспертизы является определение экспертной задачи. Она основана на фактических данных, которые эксперту следует установить. Экспертными задачами являются идентификационные задачи, направленные на установление единого источника происхождения исследуемого объекта, и диагностические задачи, направленные на установление технических характеристик исследуемого объекта.

Корректный перечень вопросов к СКТЭ, должен соответствовать ряду критериев:

Во-первых, вопросы не должны быть правовыми, затрагивать стоимость объекта исследования и перевода текста, переписки и т.д.

Во-вторых, вопросы должны быть технического характера Однако, вопрос может касаться разъяснения компьютерных терминов.

В-третьих, вопросы должны быть составлены, исходя из задач исследования (идентификационные или диагностические).

Для составления корректного перечня вопросов для СКТЭ следователю необходимо согласовать составленные им вопросы со специалистом.

Упаковка внешнего носителя информации должна быть опечатана по местам вскрытия упаковки. Если это внутренний носитель информации, являющийся частью спецтехники, его необходимо, по возможности, отделить от техники и также подготовить к передаче эксперту, либо передать вместе с оборудованием, которое необходимо упаковать и опечатать.

Также необходимо собрать и оформить в соответствии с процессуальными нормами сравнительные образцы и иные материалы. Сравнительные образцы могут быть собраны во время производства осмотра места происшествия, обыска или выемки. Сравнительные образцы оформляются таким же образом, как и объект исследования.

Следователь также должен выбрать экспертное учреждение, которое будет проводить СКТЭ. В случае, отсутствия в государственных экспертных учреждениях необходимого специалиста, следователь на основании ст. 57 УПК РФ вправе привлечь в качестве эксперта любое лицо, обладающее специальными знаниями в области компьютерных технологий, компьютерной техники, телекоммуникационных сетей. Это могут быть специалисты предприятий, учреждений, научно-исследовательских и учебных заведений, а также специалисты, имеющие опыт практической работы в этих областях знаний.

Постановление о назначении компьютерно-технической экспертизы по общему правилу назначения судебной экспертизы, в соответствии со ст. 195 УПК РФ должно содержать наиболее полную информацию по уголовному делу и по исследуемому объекту; документы, сведения о которых могут содержаться на машинных носителях, представляемых на исследование; сведения, которые могут быть использованы при восстановлении и (или) поиске экспертом информации (например, названия фирм и организаций, фамилии клиентов, предполагаемые номера счетов, название логинов и паролей доступа в сеть; обстоятельства уголовного дела). По возможности следует ознакомить эксперта с уголовным делом полностью.

# **ЗАКЛЮЧЕНИЕ**

Подводя итог всему вышесказанному можно сделать вывод, что киберпреступелния по своей сути относятся к преступлениям высокого интеллектуального уровня, следовательно, и борьба с ним должна осуществляться квалифицированными специалистами в сфере информационных технологий.

Поэтому важной задачей является повышение уровня специальной криминалистической подготовки следователей, проводящих расследование данного рода преступлений. Необходимо учитывать особенности тактики производства следственных действий, направленных на получение виртуальной информации, поскольку виртуальные следы, зачастую не подлежат непосредственному восприятию человеком, и для обнаружения требуется специальное аппаратное обеспечение. Следовательно, работники органов предварительного расследования и привлекаемые специалисты должны иметь высокий уровень материально-технического оборудования для грамотного выявления и пресечения киберпреступлей. Также при производстве следственных действий необходим подбор понятых, обладающих навыками работы в компьютерной сфере. Можно сделать вывод о том, что при расследовании киберпреступлений необходимо использовать специальные знания и привлекать соответствующих специалистов в области компьютерной криминалистики, информатики и других.

Для большинства следователей раскрытие киберпреступлений является сложной задачей, что обусловлено:

- недостаточностью методических рекомендаций, инструкция, правил по организации расследования данного вида преступлений;

- незначительным опытом работы следователей со специфическими источниками доказательственной информации.

Таким образом, по итогам своей работы можно сделать вывод о выполнении поставленных задач и целей. Выделены некоторые проблемы и предложены пути их решения, которые требуют дальнейшей проработки.

**СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ**

Нормативные правовые акты

1. «Конвенция о преступности в сфере компьютерной информации» (ETS N 185) [рус., англ.](Заключена в г. Будапеште 23.11.2001)[Электронный ресурс]. // URL: http://uristu.com/library/konventsii/konvenciy\_773/ (дата обращения: 19.10.2016)

2. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 06.07.2016) [Электронный ресурс]. // URL: <https://rg.ru/2007/11/12/ukrf-dok.html> (дата обращения: 19.10.2016)

3. «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ (ред. от 06.07.2016)(с изм. и доп., вступ. в силу с 01.09.2016)[Электронный ресурс]. // URL: http://www.consultant.ru/document/cons\_doc\_LAW\_34481/ (дата обращения: 19.10.2016)

Литература

1. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе / В. Ю. Агибалов. – М.: Юрлитинформ, 2012. – 182 с.

Вехов В.Б. Особенности организации и тактика осмотра места происшествия при расследовании преступлений в сфере компьютерной информации // Российский следователь, 2004. – № 7.

Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. 2007. № 2. С. 17 - 25.

Илюшин, Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: Дис. … канд. юрид. наук: 12.00.09 / Илюшин Денис Анатольевич. – Волгоград, 2008. – 233 с.

Ищенко Е.П. Новые информационные технологии обеспечения раскрытия и расследования преступлений [Электронный ресурс]. // URL: http://www.studfiles.ru/preview/2801191/page6/3 (дата обращения: 10.10.2016)

Косынкин А. А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии предварительного расследования / А. А. Косынкин // Российский следователь. – 2012. – № 2

Мещеряков В.А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста: научный журнал. 2013. N 5 (10). С. 265 - 270.

Мирошников Б.Н. Борьба с киберпреступлениями – одна из составляющих информационной безопасности Российской Федерации [Электронный ресурс]. // URL: http://www.crime-research.ru/articles/ Mirosh1 (дата обращения: 12.10.2016)

1. Образцов В.А. // Криминалистика. Учебник. 2-е изд.- М.: Юрист, 2002.
2. Поляков, В. В. К вопросу о назначении компьютерно-технической экспертизы, объектом которой является смартфон по преступлениям в сфере компьютерной информации: Сб. м-лов криминалистических чтений / В. В. Поляков; А. В. Шебалин; под ред. Ю. Л. Бойко. – Барнаул, 2013
3. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы / Т. Л. Тропина; отв. ред. А. А. Номоконов. – Владивосток: Изд-во Дальневост. ун-та, 2009. – 240 с.
4. Тактика следственных действий: учебное пособие / Под ред. В. И. Комиссарова. – Саратов: СГАП, 2000. – 202 с.
5. Федотов Н.Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с.
6. Чекунов И.Г., Шумов Р.Н. Современное состояние киберпреступности в Российской Федерации // Российский следователь. 2016. N 10.
7. Шевченко Е.С. Актуальные проблемы расследования киберпреступлений // Эксперт-криминалист. 2015. № 3.
1. Шевченко, Е. С. О криминалистической трактовке понятия «киберпреступность» // Информационное право. 2014. № 3 (39). С. 29 – 32. [↑](#footnote-ref-1)
2. Илюшин, Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг интернет… С. 87 – 88. [↑](#footnote-ref-2)
3. Мещеряков, В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В. А. Мещеряков. – Воронеж: Изд-во Воронеж. гос. ун-та, 2002. – С. 94 – 119. [↑](#footnote-ref-3)
4. . «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 06.07.2016) [Электронный ресурс]. // URL: <https://rg.ru/2007/11/12/ukrf-dok.html> (дата обращения: 10.10.2016) [↑](#footnote-ref-4)
5. Криминалистика.Учебник для вузов / Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р. , Под ред. Белкина Р. С. М.: НОРМА, 2000. [↑](#footnote-ref-5)
6. Мещеряков, В. А. Следы преступлений в сфере высоких технологий / В. А. Мещеряков // Библиотека криминалиста. – 2013. – № 5 (10). – С. 265 – 269 [↑](#footnote-ref-6)
7. Волеводз А.Г. Противодействие компьютерным преступлениям. М., 2002. С. 159 - 160. [↑](#footnote-ref-7)
8. Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: Автореф. дис. канд. юрид. наук. Воронеж, 2005. С. 17 [↑](#footnote-ref-8)
9. Смушкин А.Б. «Виртуальные следы в криминалистике»// «Законность», 2012. - № 8. [↑](#footnote-ref-9)
10. ст. 176 Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 06.07.2016)(с изм. и доп., вступ. в силу с 01.09.2016) Электронный ресурс// URL: http://www.consultant.ru/document/cons\_doc\_LAW\_34481/ [↑](#footnote-ref-10)
11. Косынкин, А. А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии предварительного расследования / А. А. Косынкин // Российский следователь. – 2012. – № 2 [↑](#footnote-ref-11)
12. ст. 183 «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ (ред. от 06.07.2016)(с изм. и доп., вступ. в силу с 01.09.2016)[Электронный ресурс]. // URL: http://www.consultant.ru/document/cons\_doc\_LAW\_34481/ (дата обращения: 19.10.2016) [↑](#footnote-ref-12)
13. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: Дис. … канд. юрид. наук: 12.00.12 – Москва, 2016 . – 249 с. [↑](#footnote-ref-13)
14. ст. 181 «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ (ред. от 06.07.2016)(с изм. и доп., вступ. в силу с 01.09.2016)[Электронный ресурс]. // URL: http://www.consultant.ru/document/cons\_doc\_LAW\_34481/ (дата обращения: 19.10.2016) [↑](#footnote-ref-14)
15. Преступления в сфере компьютерной информации: квалификация и дока­зывание: Учеб. пособие / Под ред. Ю.В. Гаврилина. - М.: ЮИ МВД РФ, 2003. - 245 с. [↑](#footnote-ref-15)
16. Приказ Минюста от 27.12.2012 г. № 237 «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» [Электронный ресурс]. // URL: http://minjust.ru/node/114672 (дата обращения: 19.10.2016) [↑](#footnote-ref-16)
17. Приказ МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» [Электронный ресурс]. // URL: http://www.consultant.ru/document/cons\_doc\_LAW\_55315/ (дата обращения: 19.10.2016) [↑](#footnote-ref-17)