

**Захарова Анастасия Владимировна**

Магистрант

**Направление** Юриспруденция

**Направление подготовки:** Уголовный процесс, криминалистика и судебная экспертиза, теория оперативно-розыскной деятельности

**Компьютерно-техническая экспертиза как один из видов экспертиз.**

**Ее особенности и задачи**

**Аннотация.** В статье описаны особенности проведения компьютерно-технической экспертизы как одной из основных экспертиз, проводимых при расследовании преступлений в сфере компьютерной информации.

**Ключевые слова:** интернет-технологии, эксперты, экспертизы, компьютерная информация

Особенности специфики расследования противоправных деяний, совершенных с использованием интернет-технологий, делает значимой необходимость использования особых действий в виде проведения экспертного анализа [3].

Категория рассматриваемых дел предопределяет необходимость непрерывного использования в процессе дознания специальной подготовки в области современных информационных технологий. Такие знания и навыки требуются как для получения улик и доказательств, так и для грамотного оформления документов в ходе следственного процесса, подготовленных с помощью компьютерной техники, и которые могут быть представленными в качестве доказательств.

Важную роль играет компьютерно-техническая экспертиза, проведение которой дает возможность успешно выполнить следующие задачи [1]:

– восстановить и отпечатать информацию из компьютера частично или в полном объеме (по ключевым словам, по определенным темам и т. п.),

хранящаяся на электронных носителях, и в том числе те, которые находятся в нетекстовом формате (например, в форме электронных таблиц, языков программирования, баз данных и других сложных форматах);

- восстановление информации, ранее размещенной в компьютере, впоследствии удаленной или модифицированной (измененной) по каким-то причинам;

- установление даты и время создания, модификации (изменения), копирования, уничтожения или стирания той или иной компьютерной информации (файлов, программ, документов и т. п.);

- подбор паролей, взлом защитных систем цифровых носителей и других средств хранения информации, дешифрование закодированной информации;

- изучение компьютерно-технических средств хранения информации на предмет наличия или отсутствия в них аппаратно-программных модификаций и модулей, которые предоставляют возможность проводить несанкционированное блокирование, уничтожение, копирование или изменение информации, вызывать сбои в работе системы электронно-технических устройств и в их сети (наличие «жучков», компьютерных вирусов, «закладок» и т. п.);

- установление авторства, средства (места) подготовки и способ изготовления документов (программ, файлов), находящихся на машинном носителе информации;

- выявление способов утечки конфиденциальной информации из компьютерных сетей, определенных технических средств хранения информации и мест их расположения; определение вероятных способов неправомерного доступа к носителям охраняемой законом конфиденциальной компьютерной информации;

- установление технического состояния, обнаружение неисправностей электронных носителей информации, определение степени их

износа, а также характерных признаков приспособления компьютерно-технических средств к конкретному пользователю;

- фактическая оценка уровня профессиональной подготовки фигурантов, которые проходят по делу в роли пользователя и в качестве программиста;

- выявление лиц, нарушавших правила эксплуатации компьютеров и их сетей;

- выяснение причин, вследствие которых стало возможно совершение правонарушения, в процессе которого использовались компьютерно-технические средства размещения информации.

В частности, компьютерно-техническая экспертиза обеспечивает решение следующих экспертных задач [2]:

- выявление свойств, качеств, статуса и особенностей использования технических компьютерных систем;

- установление особенностей разработки и использования программных продуктов (при установлении фактов использования программного обеспечения с нарушением авторских прав его разработчика);

- установление фактов использования того или иного оборудования при создании документов или совершении иных действий, имеющих отношение к преступлению;

- получение доступа к информации на носителях;

- исследования информации, созданной пользователем или программой для реализации информационных процессов;

- установление особенностей функционирования компьютерных средств, реализующих сетевую информационную технологию.

При установлении обстоятельств использования компьютерных средств:

1. Производилось ли подключение внешних носителей информации к представленному компьютеру? Производились ли какие-либо операции с файлами, имеющимися на внешнем носителе в момент подключения? Производилось ли копирование/удаление информации?

2. Использовался ли представленный компьютер в указанный период времени? Если да, то какие операции с компьютером были проведены в указанный период?

3. Изменялось ли системное время компьютера в указанный период?

При установлении фактов разработки и использования программного обеспечения [4]:

1. Содержится ли на представленном компьютере программное обеспечение «...»? Если да, то каковы время и источник его установки, какова версия программного обеспечения, является ли оно работоспособным?

2. Применялись ли при установке и использовании указанной программы средства защиты авторских прав? Если да, то какие именно средства?

3. Выполнялись ли в ходе установки представленного программного обеспечения действия, направленные на нейтрализацию средств защиты авторского права?

4. Соответствует ли разработанное программное обеспечение требованиям технического задания, а также иным нормативным и техническим документам?

5. Какова дата начала использования системы/оборудования?

При установлении обстоятельств создания и использования документов и баз данных[5]:

1. Имеются ли признаки того, что документ «...» был изготовлен при помощи компьютерных средств, представленных на исследование?

2. Содержатся ли в памяти компьютерных средств, представленных на исследование, следы изготовления документа «...»?

3. Имеются ли на представленных носителях информации сведения о создании документа «...»? Если да, то когда данный документ был создан, когда и какие изменения в него вносились, производилась ли печать документа?

4. Имеются ли в представленной базе данных сведения о документе «...»? Удалялся ли данный документ из базы данных?

5. Посредством какой учетной записи было проведено создание или удаление документа и когда?

6. Возможно ли восстановить информацию с представленного носителя/накопителя информации?

При установлении фактов использования сетевых технологий:

1. Осуществлялось ли посредством представленной компьютерной техники подключение к сети Интернет?

2. Какие логины и пароли использовались для подключения и работы в сети Интернет?

3. В какие временные периоды пользователь был подключен к сети Интернет?

4. Осуществлялись ли при помощи представленного оборудования вход на почтовый сервер «...» или переписка при помощи программ мгновенного обмена сообщениями? Если да, то каковы реквизиты отправителя и адресатов сообщений? Какие сообщения были приняты или отправлены, когда, от кого и кому?

5. Осуществлялся ли вход в банк-клиент в период с «...» по «...»? Если да, то сохранилась ли информация о создании и отправке платежного поручения № «...»?

### Литература

1. Вехов В.Б., Rogozin В.Ю. Методика расследования преступлений в сфере компьютерной информации / Криминалистика: учебник для среднего профессионального образования. Волгоград: ВА МВД России, 2015.

2. Катков С.А., Собецкий И.В., Фёдоров А.Л. Подготовка и назначение программно-технической экспертизы // Информационный бюллетень СК МВД России. 2015. №4 (85).

3. Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий: Автореф. дис. ... канд. юрид. наук. Ростов н/Д., 2017.

4. Номоконов В.А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2016. №1 (24).

5. Генеральная прокуратура Российской Федерации «О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий» [Электронный ресурс] // Режим доступа: <http://genproc.gov.ru> (дата обращения: 03.04.2019).

© Бюллетень магистранта 2019 год № 5