**с 22.11.20г. по 26.11.20г.**

**Дисциплина: Криминалистика**

***Составить конспект в тетрадь и выполнить задание для самостоятельного изучения***

**Тема: «Методика расследования преступлений в сфере компьютерной информации»**

**Основные вопросы:**

1. Общая характеристика преступлений в сфере компьютерной информации.

2. Криминалистическая характеристика преступлений в сфере компьютерной информации.

3. Особенности тактики отдельных следственных действий.

* + - 1. Действующим Уголовным кодексом Российской Федерации предусмотрена ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ), нарушение права эксплуатации компьютерной техники (ст. 274 УК РФ). Эти составы законодатель отнес к главе 28 УК РФ «Преступления в сфере компьютерной информации».

Компьютерная информация, будучи разновидностью информации вообще, в криминалистическом аспекте может быть определена как фактические данные, обработанные компьютерной системой и (или) передающиеся по телекоммуникационным каналам, а также доступные для восприятия, на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения уголовного или гражданского дела.

Специфика компьютерной информации проявляется в том, что она: 1) быстро обрабатываема и легко удаляема;

2) легко передается по телекоммуникационным каналам связи компьютерных сетей в любом объеме и на любое расстояние;

3) относительно обезличена, т.к. не всегда очевидна жесткая связь между ней и лицом, которое ее создает и использует;

4) может находиться лишь на машинном носителе, в самой ЭВМ, системе ЭВМ, сети ЭВМ.

*Мотивы совершения* рассматриваемых преступлений следующие: удовлетворение собственных амбиций создателя или пользователя рассматриваемой информации; получение информации, которую можно использовать в политических, военных и экономических целях; создание эффекта опасности, который можно использовать в целях воздействия на других лиц или организации; получение личных имущественных или неимущественных выгод; разрушение информационных систем и др.

2. Центральным элементом криминалистической характеристики преступлений в сфере компьютерной информации является способ преступления. Известны следующие ***способы их*** ***совершения***:

1) методы перехвата: подключение к компьютерным сетям; электронный поиск и прочие;

2) методы несанкционированного доступа: подключение к линии законного пользователя через Интернет; использование особой программы, применяемой в компьютерных центрах при сбоях в работе ЭВМ;

3) методы манипуляции: подмена данных; «троянский конь» - тайный ввод в чужую программу; «бомба» - тайное встраивание в программу набора команд, которые должны сработать (или срабатывают каждый раз при определенных условиях либо в определенные моменты времени (вирус «Чернобыль», который активизируется 26 апреля - в день аварии на АЭС);

4) моделирование процессов, в которые преступники хотят вмешаться, и планируемые методы совершения и сокрытия посягательства. Например, реверсивная модель, когда создается модель конкретной системы, в которую вводятся реальные исходные данные и учитываются планируемые действия. Из полученных результатов подбираются правдоподобные желательные. Затем, путем прогона модели назад к каналу, выясняют результаты и устанавливают, какие манипуляции с исходными данными нужно проводить. Таких операций может быть несколько. После этого остается только осуществить задуманное.

***Способы сокрытия*** преступлений в сфере компьютерной информации в значительной степени детерминированы способами их совершения. При непосредственном доступе сокрытие следов сводится к воссозданию обстановки, предшествующей совершению преступления, то есть уничтожению оставленных следов (следов пальцев рук на клавиатуре, кнопках дисководов и д.р.). При опосредованном доступе распространено программное сокрытие следов, состоящее в указании ложных телефонных номеров, паролей и анкетных данных лица, совершающего неправомерный доступ.

Наиболее распространенными способами программного сокрытия следов преступления в сети Интернет являются следующие:

1) использование ремейлеров (компьютеров, получающих сообщение и перенаправляющих его по адресу, указанному отправителем, в процессе чего информация об отправителе уничтожается, и конечный получатель лишен возможности установить автора сообщения);

2) использование в программах пересылки электронной почты вымышленного электронного адреса отправителя, а также второго электронного почтового ящика;

3) использование программ-анонимизаторов, которые в отличие от ремейлеров фактически осуществляют переадресацию электронной почты, направляя ее с другого компьютера, позволяют изменять данные об обратном адресе и службе электронной почты отправителя. При этом остается возможность установить электронный адрес компьютера отправителя.

***Орудиями*** совершения преступлений в сфере компьютерной информации являются средства компьютерной техники, в том числе и специальное программное обеспечение. Кроме того, средствами совершения преступлений являются: сетевое оборудование, телефонная сеть, машинные носители информации.

***Следы преступлений*** в сфере компьютерной информации можно разделить на два типа: традиционные следы-отображения («идеальные» следы, «материальные» следы-отображения, а также следы-вещества и следы-предметы) и нетрадиционные – компьютерно-технические следы.

К *традиционным* следам относятся какие-либо рукописные записи, распечатки и т.п., свидетельствующие о приготовлении и совершении преступления. «Материальные» следы могут остаться и на самой вычислительной технике (следы пальцев рук, микрочастицы на клавиатуре, дисководах, принтере и т.д.), а также на машинных носителях. «Идеальные» следы – это отражения события преступления и элементов механизма его совершения в сознании и памяти людей, имеющие психофизиологическую природу формирования и проявляющиеся в виде мысленных образов преступления в целом, отдельных его моментов и участников данного деяния.

*Компьютерно-технические* следы представляют собой результаты передачи и преобразования компьютерной информации, причинно связанные с событием преступления.

Они остаются на машинных носителях информации и отражают изменения в хранящейся в них информации (по сравнению с исходным состоянием). Речь идет о следах модификации информации (баз данных, программ, текстовых файлов, файлов-отчетов и протоколов работы, системного реестра, учетных записей пользователей сети Интернет и др.), находящиеся на жестких дисках ЭВМ, дискетах, магнитных лентах, лазерных и магнитооптических дисках, флэш-картах. Кроме того, магнитные носители могут нести следы уничтожения или модификации информации (удаление из каталогов имен файлов, стирание или добавление отдельных записей, физическое разрушение или размагничивание носителей). Компьютерно-техническими следами являются также результаты работы антивирусных и тестовых программ. Данные следы могут быть выявлены при изучении компьютерного оборудования, протоколов работы антивирусных программ, программного обеспечения. Для их выявления необходимо участие специалистов.

***Предметом преступного посягательства*** при совершении рассматриваемых преступлений является компьютерная информация. Последняя, как вид информации вообще, представляет собой сведения, знания или набор команд, предназначенные для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинном носителе, которые имеют собственника, установившего правила их использования.

***Типовой портрет*** лица, совершающего преступления в сфере компьютерной информации, также специфичен. Преступления в сфере компьютерной информации совершают: а) лица, состоящие в трудовых отношениях с предприятием, организацией, учреждением, фирмой или компанией, где совершено преступление; б) граждане, не состоящие в правоотношениях с предприятием, организацией, учреждением, фирмой или компанией, где совершено преступление.

Особую категорию лиц, совершающих преступления в сфере компьютерной информации, составляют хакеры (от анг. to haсk – рубить, кромсать) – специалисты в сфере вычислительной техники, осуществляющие негативные действия в области систем компьютерной связи, информационных технологий. Их деятельность направлена на получение доступа к компьютерной информации, для чего они используют различные способы «взлома», обхода защиты и проникновения в сеть. В результате они похищают и заменяют данные, модифицируют файлы, блокируют работу сети и выводят из строя программное оборудование, предназначенное для поиска «слабых мест» в системе защиты и др.

3. Тактика отдельных следственных действий преступлений в сфере расследования компьютерной информации имеет свои особенности. Прежде всего, перед началом обыска или осмотра принимаются меры, которые предотвратят возможное повреждение или уничтожение информации. Для этого следует обеспечить контроль за бесперебойным электроснабжением ЭВМ в момент осмотра (обыска), удалить всех посторонних лиц с территории, на которой производится осмотр или обыск, прекратить дальнейший доступ к компьютерным средствам; принять меры к тому, чтобы оставшиеся лица не имели возможности прикасаться к средствам вычислительной техники и к источникам электропитания. Если на объекте находятся взрывчатые, легковоспламеняющиеся, едкие вещества, посторонние источники электромагнитого излучения и другие предметы и аппаратура, способные привести к аварии ЭВМ, эвакуировать их. Осмотр или обыск целесообразно производить с участием специалиста по информационно-компьютерным технологиям. Желательно и в качестве понятых (если они вообще необходимы) приглашать квалифицированных пользователей ЭВМ.

Не следует ограничиваться поиском информации только в компьютере; необходимо внимательно осмотреть имеющуюся документацию, вплоть до записей на клочках бумаги, поскольку программисты часто, не надеясь на свою память, оставляют записи о паролях, изменениях конфигурации системы, особенностях построения информационной базы компьютера. Многие пользователи хранят копии своих файлов на дискетах во избежание утраты их при выходе компьютера из строя. Поэтому любые обнаруженные носители информации должны быть изъяты и изучены. Производство осмотра или обыска в помещениях, где находится много компьютерных устройств, работает множество людей, сопряжено со значительными трудностями. В частности, лица, в отношении которых расследуется подобные уголовные дела, часто оказывают серьезное противодействие.

Условиями успеха в этом случае являются: собирание информации об объекте осмотра или обыска; составление плана осмотра или обыска с детальной регламентацией задач каждого участника; определение соответствующего состава следственно-оперативной группы; обеспечение группы необходимыми специальными техническими средствами.

Одним из ключевых следственных действий является допрос представителя фирмы-провайдера. Перед допросом необходимо довести до сведения допрашиваемого некоторые основные понятия и определения, используемые в юридической науке, поскольку они могут не совпадать со сходной технической терминологией, что может вызвать недопонимание и разночтение. У представителя провайдера необходимо получить копии учредительных документов и лицензии на право предоставления услуг связи. Это можно оформить протоколом выемки. Также необходимо получить протоколы работы в сети Интернет абонента с именем, присвоенным потерпевшему, с указанием времени работы и суммы денежных средств, списанных со счета указанного абонента. Эти данные сопоставляются с заключением компьютерно-технической экспертизы. Совпадение протоколов работы в сети, ведущихся у провайдера и на компьютере подозреваемого, нередко используется при формулировании фабулы обвинения.

При расследовании преступлений в сфере компьютерной информации назначаются и проводятся различные экспертизы, в том числе традиционные криминалистические экспертизы, экспертизы веществ и материалов, экономические экспертизы и др. Назначение и проведение перечисленных экспертиз особых затруднений не вызывают, что касается экспертиз собственно компьютерно-технических, то они относятся к разряду новых и их назначение и проведение вызывают значительные сложности.

Комплекс экспертиз, назначаемых при расследовании неправомерного доступа к компьютерной информации, будет меняться и зависеть от способа и в целом механизма преступления.

В компьютерно-технической экспертизе как самостоятельном роде судебных экспертиз, относящемся к классу инженерно-технических, выделяют следующие виды: аппаратно-компьютерную экспертизу; программно-компьютерную экспертизу; компьютерно-сетевую экспертизу.