СЛЕДСТВЕННЫЕ СИТУАЦИИ НАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ УДАЛЕННЫМ ОБРАЗОМ

Вит.В. Поляков, А.В. Куракин
Алтайский государственный университет, г. Барнаул

При расследовании компьютерных преступлениях, совершаемых удаленным образом, особое внимание уделяется обнаружению следов преступления и других вещественных доказательств, а также выявлению иных значимых для дела обстоятельств. Компьютерную технику и устройства связи, которые представляют интерес для расследования, в криминалистических целях можно подразделить по следующим группам признаков:

- по виду собственности;
- по виду мобильности;
- по характеру построения канала связи;
- по энергозависимости устройства, в котором хранится информация.

Данная классификация представлена в таблице 1.

Таблица 1. Классификация компьютерной техники и устройств связи

1. По виду собственности	1.1. Личные
	1.2. Публичные
2. По виду мобильности средств совершения преступлений	2.1. Мобильные
	2.2. Стационарные
3. По характеру построения канала связи	3.1. Прямой канал соединения
	3.2. Опосредованный канал соединения
4. По обнаружению компьютерной информации в энергозависимой части устройства	4.1. Энергонезависимые устройства
	4.2. Энергозависимые устройства

Описанная классификация позволяет более эффективно акцентировать внимание следствия на поиск имеющих отношение к преступлению следов-последствий, позволяет выявить возможных участников сетевого обмена информацией и дает возможность смоделировать различные ситуации. Рассмотрим в качестве примера ситуации, возникающие при выделенных признаках.

Ситуации для первой группы возможны в двух вариантах личные устройства связи принадлежат пользователям на праве собственности и, как правило, содержат следы владельца устройства (характерные идентификационные признаки личности) – рис. 1; публичные устройства связи позволяют ими воспользоваться на праве пользования при конкретных условиях и обстоятельствах, обычно они содержат следы общения разных личностей (наличие идентификационных признаков, принадлежащих разным лицам в конкретные периоды времени) – рис. 2.

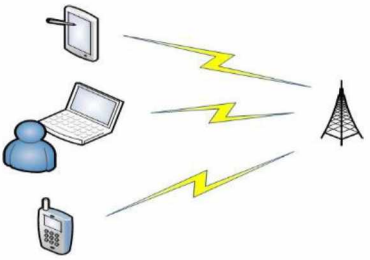

Рис. 1. Личные устройства

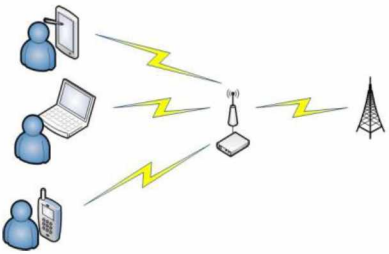

Рис. 2. Публичные устройства.

Ситуации для второй группы возможны в двух вариантах: когда средства удаленного совершения преступлений были мобильными, находясь в рабочем состоянии, меняли свое местонахождение – рис. 3, и стационарные устройства, имевшие постоянное местонахождение – рис. 4. Типичная следовая картина при использовании мобильных или стационарных устройств будет отличаться.

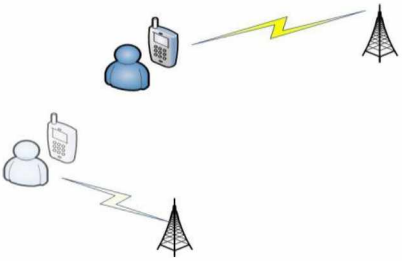

Рис. 3. Мобильные устройства.

Рис. 4. Стационарные устройства.

Ситуации для третьей группы возможны в следующих вариантах: прямой канал соединения с наличием следов технического сетевого соединения и взаимодействия сетевого оборудования – рис. 5. В этом случае возможна передача и получение пакетов информации, содержащих различные данные об отправителе, его компьютерной технике и программном обеспечении, о личная переписке и иных следов удаленного общения пользователей. Опосредованный канал соединения отличается наличием следов сетевого взаимодействия не только у соединяющихся устройств, но и на компьютерной технике посредников соединения: роутерах, маршрутизаторах, шлюзах, серверах и ином сетевом оборудовании – рис. 6.

Рис. 5. Прямой канал связи.

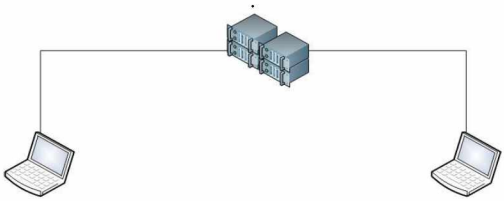

Рис. 6. Опосредованный канал связи.

Ситуации для четвертой группы могут быть подразделены на два вида, когда компьютерная информация находится в энергонезависимой части устройства (информации сохраняется после отключения электропитания), и в энергозависимой части устройства (информации безвозвратно удаляется после отключения электропитания). Криминалистически значимая компьютерная информация может быть обнаружена в обоих случаях, однако сбор ее необходимо начинать с энергозависимой части устройств. Это объясняется риском ее утраты в связи с возможными действиями по сокрытию следов преступления и противодействию расследованию со стороны преступников, установивших механизмы уничтожения информации при определенных условиях, отправляющих команды удаленно или действующих иными способами [2]. Потеря следов-последствий возможна также в результате стихийных бедствий, сбоев в работе компьютерной техники или ненамеренных действий третьих лиц, а также ошибок следствия, например, когда без достаточных причин отключается электроэнергия на месте происшествия или на конкретной компьютерной технике. В связи с этим для предотвращения риска утраты криминалистически значимой компьютерная информация первоначально делается слепок оперативной памяти и осуществляется фиксация информации, например, отображаемой на экране устройства.

Важным шагом в расследовании дистанционных компьютерных преступлений является знание того, каким образом осуществлялась коммуникация между устройствами связи. Обычно в поводах и основаниях для возбуждения уголовных дел данной категории бывает известно по крайней мере одно устройство с возможными следами преступления, совершенного с применением сетевых технологий. Установить иные устройства, участвовавшие в передаче данных по телекоммуникационным сетям связи, бывает достаточно затруднительно. В этих случаях целесообразно исследовать возможности применения комбинации рассмотренных выше признаков.

В качестве примера рассмотрим комбинацию из первой, второй и третьей групп. Результаты соответствующих ситуаций можно представить в виде таблицы 2, из которой следует, что возможно восемь комбинаций соединения рассматриваемых признаков. Содержание таблицы 2 может рассматриваться как представление типичных ситуаций первоначального этапа расследования компьютерных преступлений, совершенных удаленным образом.

Таблица 2. Ситуации, выделяемые в зависимости от комбинаций признаков

	Личное устройство		Общественное устройство	
	Мобильное	Стационарное	Мобильное	Стационарное
Прямой канал	+	+	+	+
Опосредованный канал	+	+	+	+

Личным мобильным устройством может служить смартфон, мобильный телефон, ноутбук, использующийся одним лицом; стационарным личным устройством выступает персональный компьютер, установленный дома или на работе, не меняющий свое местоположение в зависимости от времени. Примером мобильных публичных устройств связи могут служить общественные точки доступа к сети Wi-Fi на транспорте, примером стационарах публичных устройств - Wi-Fi роутеры в интернет-кафе.

Коммуникация личного устройства связи с иными устройствами через общественную точку доступа реализует опосредованный тип соединения, так как следы соединения между устройствами будут присутствовать не только на устройствах абонентов соединения, но и на устройстве точки доступа.

В качестве другого примера можно выделить ситуации для конкретного канала связи, который, как было показано, может быть прямым или опосредованным. В этом случае реализуется шестнадцать возможных комбинаций признаков, что проиллюстрировано в виде таблицы 3. , то есть осуществляемым через компьютерную технику, выполняющую посредническую роль, как например, работают большинство мессенджеров, социальные сети, при общении в которых следы остаются не только на конечных устройствах пользователей, но и на промежуточных устройствах.

Таблица 3. Ситуации для двух устройств с конкретным каналом связи.

		Личное		Общественное	
		Мобильное	Стационарное	Мобильное	Стационарное
Личное	Мобильное	+	+	+	+
	Стационарное	+	+	+	+
Общественное	Мобильное	+	+	+	+
	Стационарное	+	+	+	+

Выявляя конкретные комбинации электронно-цифровых следов компьютерных преступлений, совершаемых с помощью удаленного доступа, можно оценивать их в качестве основы для конкретных следственных ситуаций, выделение которых на начальном этапе расследования помогает правильно выдвигать

криминалистические версии и производить их проверку, а по соответствующим ситуациям применять наиболее удачный алгоритм их разрешения.

Публикация подготовлена в рамках поддержанного РФФИ научного проекта 16-33-01160-ОГН.

Библиографический список

1. Гавло, В.К. Ситуационный подход в криминалистике по делам о компьютерных преступлениях / В.К. Гавло, В.В. Поляков // Научно-методические и нормативные материалы и документы IV Пленума СибРОУМО по образованию в области информационной безопасности : матер. Пленума и документы конференции : сб. статей : Томск – Барнаул – Белокуриха, 8-13 июня 2010 г. – Томск : «В-Спектр», 2010. – С. 186 - 187.

2. Поляков, В.В. Некоторые сложности расследования компьютерных преступлений / В.В. Поляков, С.А. Лапин // Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях : матер. Междунар. научн.-практ. конф. (Тюмень, 1-2 ноября 2013 г.). – Тюмень, 2013. – Вып. 10, Ч. 2. – С. 208-211.

3. Гавло, В.К. Следовая картина преступлений, связанных с неправомерным доступом к компьютерной информации с помощью удаленно расположенной ЭВМ, и ее значение для производства судебных компьютерно - технических экспертиз / В.К. Гавло, В.В. Поляков // Теория и практика судебных экспертиз в современных условиях : сб. матер. Междунар. науч.-практ. конф. – М. : ТК Велби, Изд-во Проект, 2007. – С. 471 - 475.