КАФЕДРА КРИМИНАЛИСТИКИ И ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ В ОВД

ЛЕКЦИЯ

по дисциплине «Расследование преступлений в сфере компьютерной информации»

Тема № 1

«Организационно-правовые основы раскрытия и расследования преступлений в сфере компьютерной информации и высоких технологий»

КАФЕДРА КРИМИНАЛИСТИКИ И ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ В ОВД

ЛЕКЦИЯ

по дисциплине «Расследование преступлений в сфере компьютерной информации»

Тема № 1

«Организационно-правовые основы раскрытия и расследования преступлений в сфере компьютерной информации и высоких технологий»

ПЛАН ЛЕКЦИИ

1. **Нормативные правовые акты,** используемые следователем при расследовании преступлений в сфере компьютерной информации: система и основные положения.
2. **Понятийный аппарат,** используемый следователем при расследовании преступлений в сфере компьютерной информации.
3. **Криминалистически значимые сведения** о преступлениях в сфере компьютерной информации.

Расследование преступлений в сфере компьютерной информации, в силу специфики объекта и предмета преступления, обусловливает использование следователем соответствующих нормативных правовых актов.

1) Конституция Российской Федерации

2) Соглашение от 1 июня 2001 г. «О сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации», г. Минск (ратифицирована Россией с оговоркой).

3) Уголовный кодекс РФ *(статьи 272 «Неправомерный доступ к компьютерной информации», 273 «Создание, использование и распространение вредоносных компьютерных программ» и 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»).*

4) Уголовно-процессуальный кодекс РФ *(статьи 81, 82, 166, 182 и 183).*

5) Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6) Федеральный закон РФ от 7 июля 2003 г. № 126-ФЗ «О связи».

Одновременно применяются иные федеральные законы, отдельные положения которых могут использоваться следователем при расследовании по уголовному делу (например, статья 13 *федерального* закона РФ от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»).

7) Указ Президента РФ от 15 января 2013 г. № 51с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

8) Постановление Правительства РФ от 21 апреля 2005 г. № 241 «О мерах по организации оказания универсальных услуг связи».

9) Приказ МВД РФ от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации».

10) Приказ МВД РФ № 786, Минюста РФ № 310, ФСБ РФ № 470, ФСО РФ № 454, ФСКН РФ № 333, ФТС РФ № 971 от 6 октября 2006 г. «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола».

ВОПРОС 2. Понятийный аппарат, используемый следователем при расследовании преступлений в сфере компьютерной информации

1. ***Информация*** – это сведения (сообщения, данные) независимо от формы их представления (статья 2 ФЗ «Об информации, информационных технологиях и о защите информации»).

Информация представляет содержание результата **процесса отражения**, **при котором один объект (отражаемый), взаимодействуя с другим объектом или субъектом (отражающим), вызывает изменения в его состоянии и тем самым передает ему часть сведений о собственном содержании.**

2. ***Компьютерная информация*** – это сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (примечание к статье 272 УК РФ).

3. ***Электронно-цифровой след*** – это любая криминалистически значимая информация (сведения, сообщения, данные), зафиксированная в электронно-цифровой форме с помощью электромагнитных взаимодействий либо передающаяся по каналам связи посредством электромагнитных сигналов (Вехов В.Б.).

4. Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (статья 2 ФЗ «Об информации, информационных технологиях и о защите информации»). Каждая сеть имеет аппаратно-программный и информационный

глобальной сети).

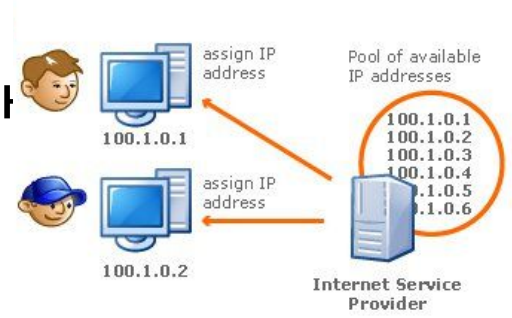
5. Персональный компьютер (оконечное оборудование, DTE) – это устройство (вычислительная система), способное выполнять заданную, четко определенную программой последовательность операций для манипулирования различными типами данных, проведения обработки и преобразования содержащейся в них информации.

6. Сервер – это персональный компьютер, выделенный из группы компьютеров для выполнения какой-либо сервисной задачи без непосредственного участия человека. Сервер отличается от *рабочей станции* (персонального компьютера), чьи «интересы» он обслуживает. Отдельные сервисные задачи могут выполняться на рабочей станции параллельно с работой пользователя.

7. IP-адрес **(сетевой адрес) – это основной тип адресов в глобальной сети, обеспечивающий однозначную идентификацию отдельного узла. IP-адрес характеризует не отдельное аппаратное устройство, а сетевое соединение. IP-адрес состоит из двух частей (номера сети доступа и номера узла) и, как правило, предстает в виде четырех десятичных чисел значением от 0 до 255, разделенных точками (например, 198.168.0.6).**

IP-адрес может быть статический (определятся сетевому соединению на постоянной основе из множества имеющихся у администратора сети доступа в ручном или автоматическом режиме) или

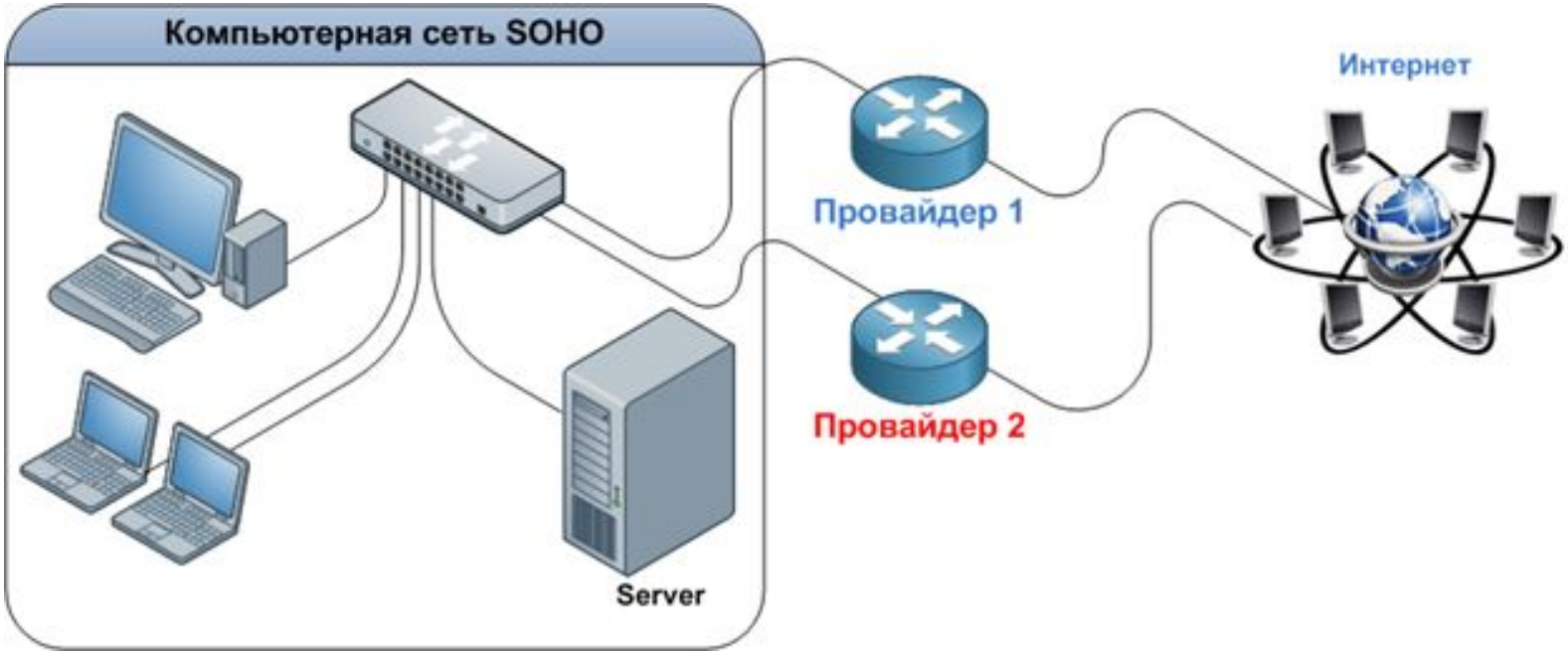
сетевому соединени



8. Доменное имя – это обозначение символами, предназначенное для адресации сайтов в глобальной сети в целях обеспечения доступа к информации, размещенной в данной сети (в настоящее время сети Интернет, статья 2 ФЗ «Об информации, информационных технологиях и о защите информации»).

10. Интернет-провайдер (оператор связи) – это юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии (статья 2 ФЗ «О связи»).

11. Провайдер хостинга – это лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к глобальной сети (в настоящее время сети Интернет, статья 2 ФЗ «Об информации, информационных технологиях и о защите информации»).


Компьютерная сеть SOHO
Server
Провайдер 1
Провайдер 2
Интернет

Вопрос 3. Криминалистически значимые сведения о преступлениях в сфере компьютерной информации

Криминалистически значимые сведения о неправомерном доступе к компьютерной информации (на примере составе преступления, предусмотренного статьей 272 УК РФ):

1. Способ непосредственного совершения преступления в сфере компьютерной информации, в том числе орудие и средство совершения преступления:

1) непосредственный доступ к персональному компьютеру.

2) опосредованное подключение к персональному компьютеру:

а) путем преодоления технической защиты:

– подключение к линии связи легального пользователя, перехват его сигнала и доступ к ПК после окончания

– подключение к персональному компьютеру легального пользователя путем **подбора паролей** (перебором с помощью специальной программы, интеллектуальным подбором с помощью «словарей» наиболее распространенных паролей);

– подключение к персональному компьютеру легального пользователя с **использованием паролей, сообщенных легальным пользователем** (например, преступник представляется системным администратором или работником банка и просит сообщить пароль);

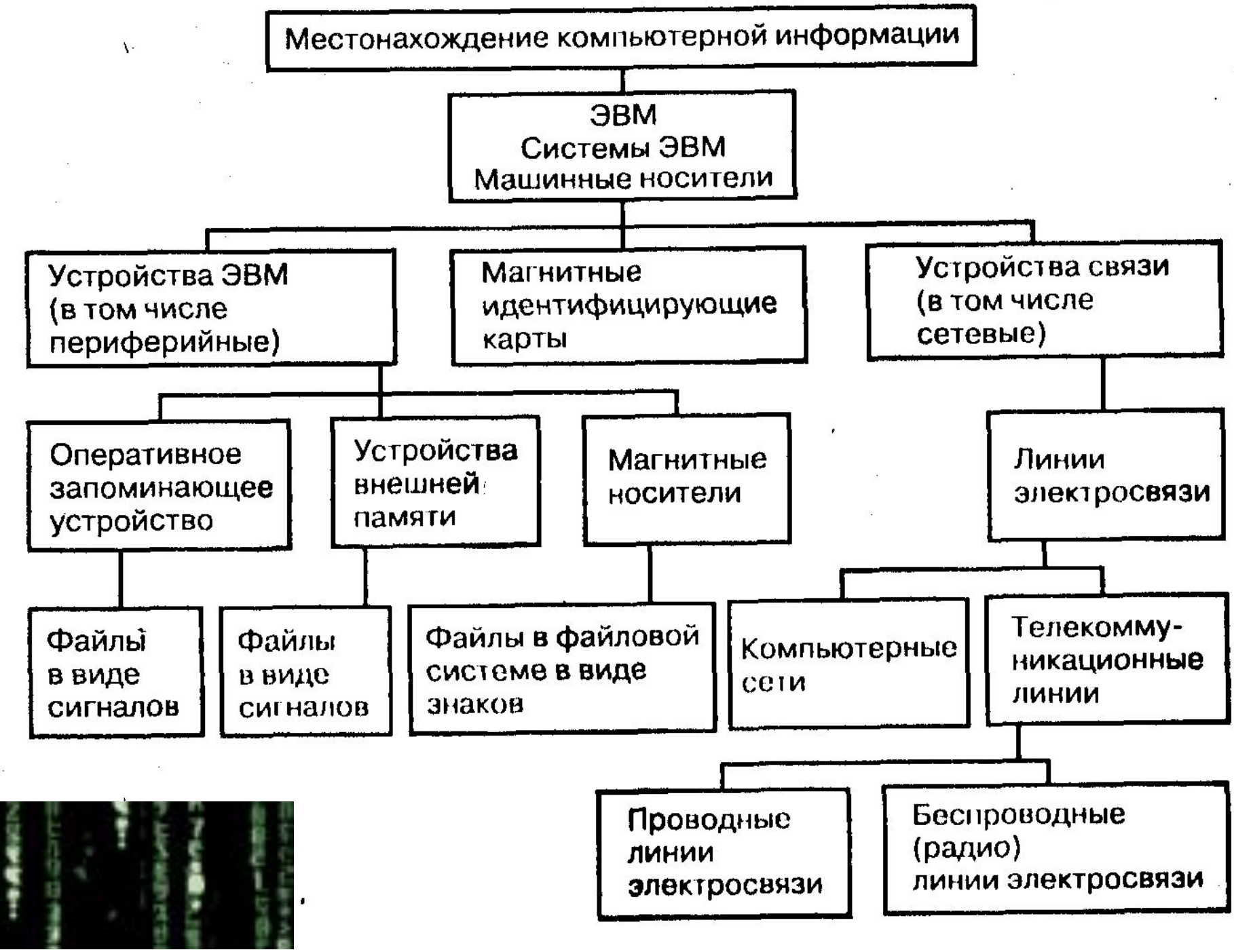
– получение удаленного доступа к чужой локальной, в том числе частной виртуальной, сети путем автоматического перебора абонентских номеров с последующим соединением с тем или иным

Место совершения преступления и наступления последствий совпадает в случае непосредственного доступа к ПК, зачастую не совпадает в случае опосредованного доступа к ПК, может присутствовать несколько мест реализации преступного умысла (при одновременной работе нескольких ПК и др.).

Время совершения преступления носит технологический характер.

Потерпевшими выступают зачастую коммерческие организации, реже – физические лица. Сведения о потерпевшем находятся в прямой зависимости от предмета преступления.

Предмет преступления – компьютерная информация в виде персональных данных пользователя, сведений для идентификации пользователя в компьютерной системе, сведений конфиденциального характера, легального программного обеспечения пользователя (есть позиция, согласно которой у названных преступлений фактически отсутствует предмет).


Местонахождение компьютерной информации
ЭВМ
Системы ЭВМ
Машинные носители
Устройства ЭВМ (в том числе периферийные)
Магнитные идентифицирующие карты
Устройства связи (в том числе сетевые)
Оперативное запоминающее устройство
Устройства внешней памяти
Магнитные носители
Линии электросвязи
Файлы в виде сигналов
Файлы в виде сигналов
Файлы в файловой системе в виде знаков
Компьютерные сети
Телекоммуникационные линии
Проводные линии электросвязи
Беспроводные (радио) линии электросвязи

Механизм следообразования включает следообразующую и следовоспринимающую поверхности.

Данные поверхности могут иметь различную природу:

- **физическую** (например, контакт преступника с поверхностью банкомата);

- **логическую** (например, взаимодействие вредоносной программы с операционной системой ПК) или смешанную (например, введение преступником ранее похищенного ПИН-кода на клавиатуре банкомата


Вредоносные программы
Вирусы, черви, троянские и хакерские программы
Шпионское, рекламное программное обеспечение
Web-черви
Загрузочные вирусы
Почтовые черви
Потенциально опасное программное обеспечение
Файловые вирусы
Троянские утилиты удаленного администрирования
Макровирусы
Рекламные программы
Троянские программы-шпионы
Сетевые атаки
Руткиты
Утилиты взлома удаленных компьютеров
Методы борьбы:
антивирусные программы, межсетевой экран, своевременное обновление системы безопасности операционной системы и приложений, проверка скриптов в браузере

Преступление совершается ***лицами*** двух групп:

1) лица, состоящие в **трудовых отношениях с организацией, пострадавшей от преступления** (примерно 55%; обслуживающие ПК или компьютерную сеть, пользователи ПК, администрация организации);

2) **лица, не состоящие в указанных отношениях** (45%; лица, занимающиеся проверкой финансово-хозяйственной деятельности пострадавшей организации; обслуживающие ПК или компьютерную сеть, связанные с ПК или сетью пострадавшей организации).

Спасибо за внимание!