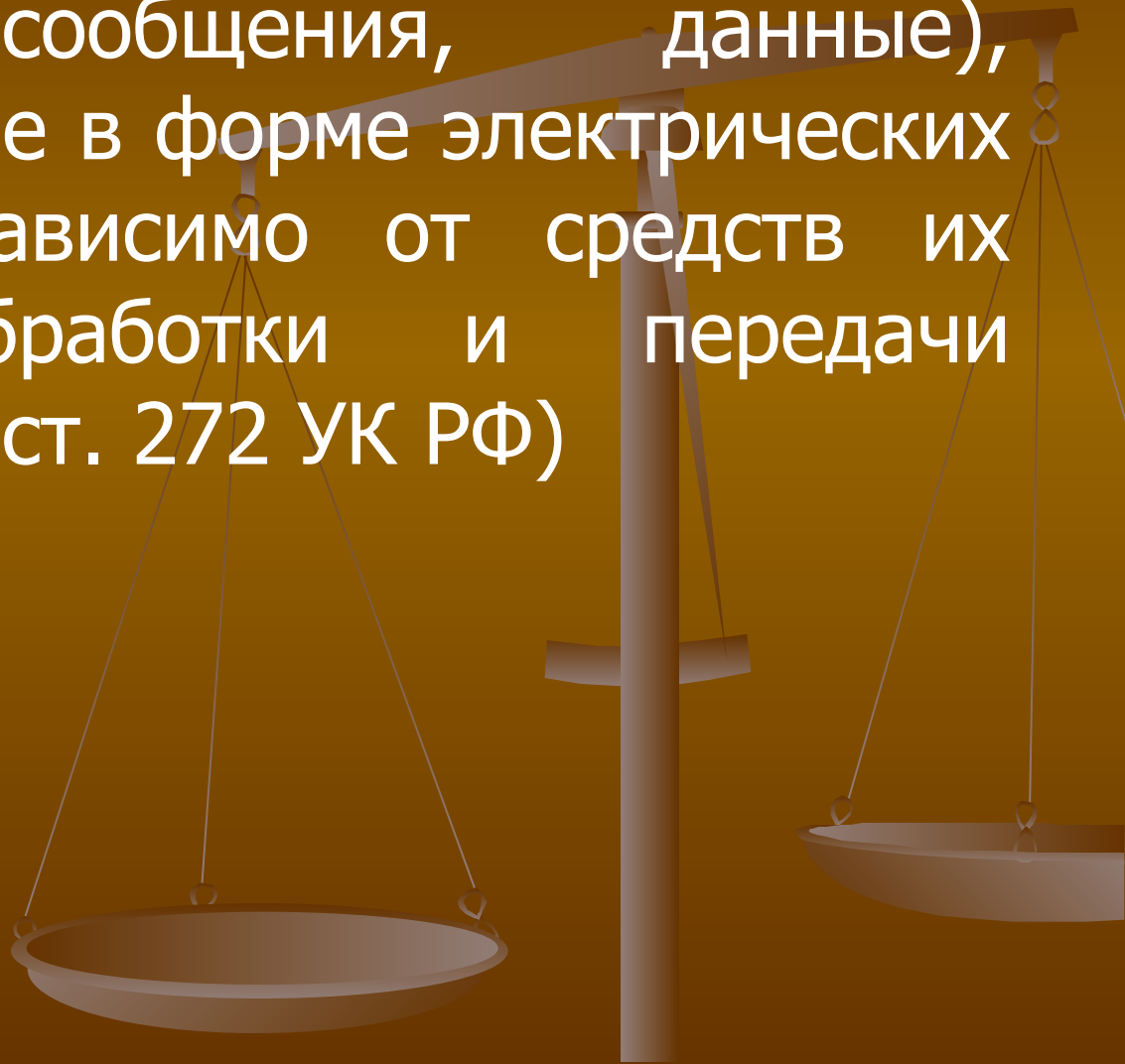
Особенности расследования преступлений в сфере компьютерной информации

Лекция (2 ч)

Компьютерная информация:

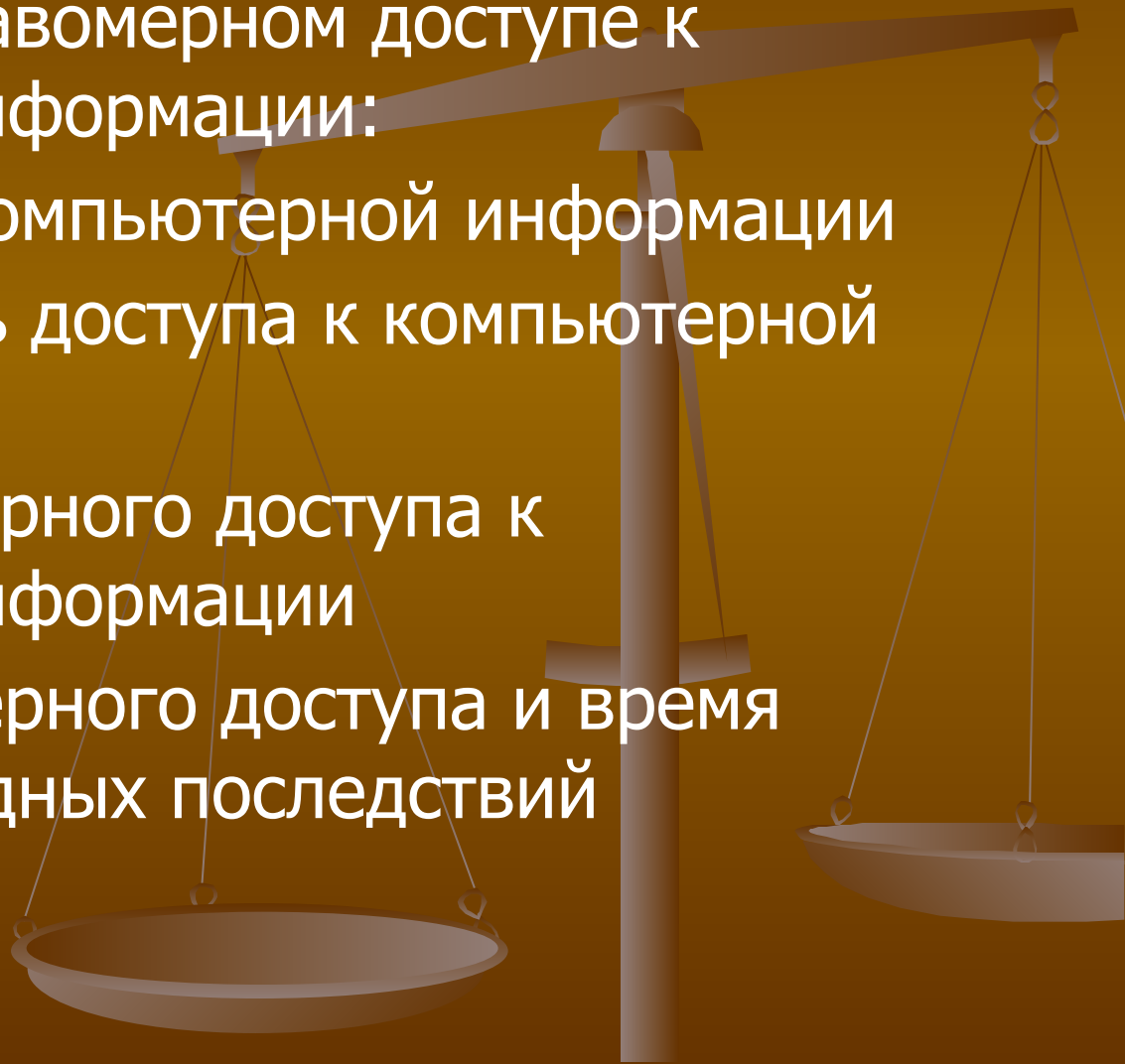
- сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (примечание к ст. 272 УК РФ)



Обстоятельства, подлежащие установлению и доказыванию

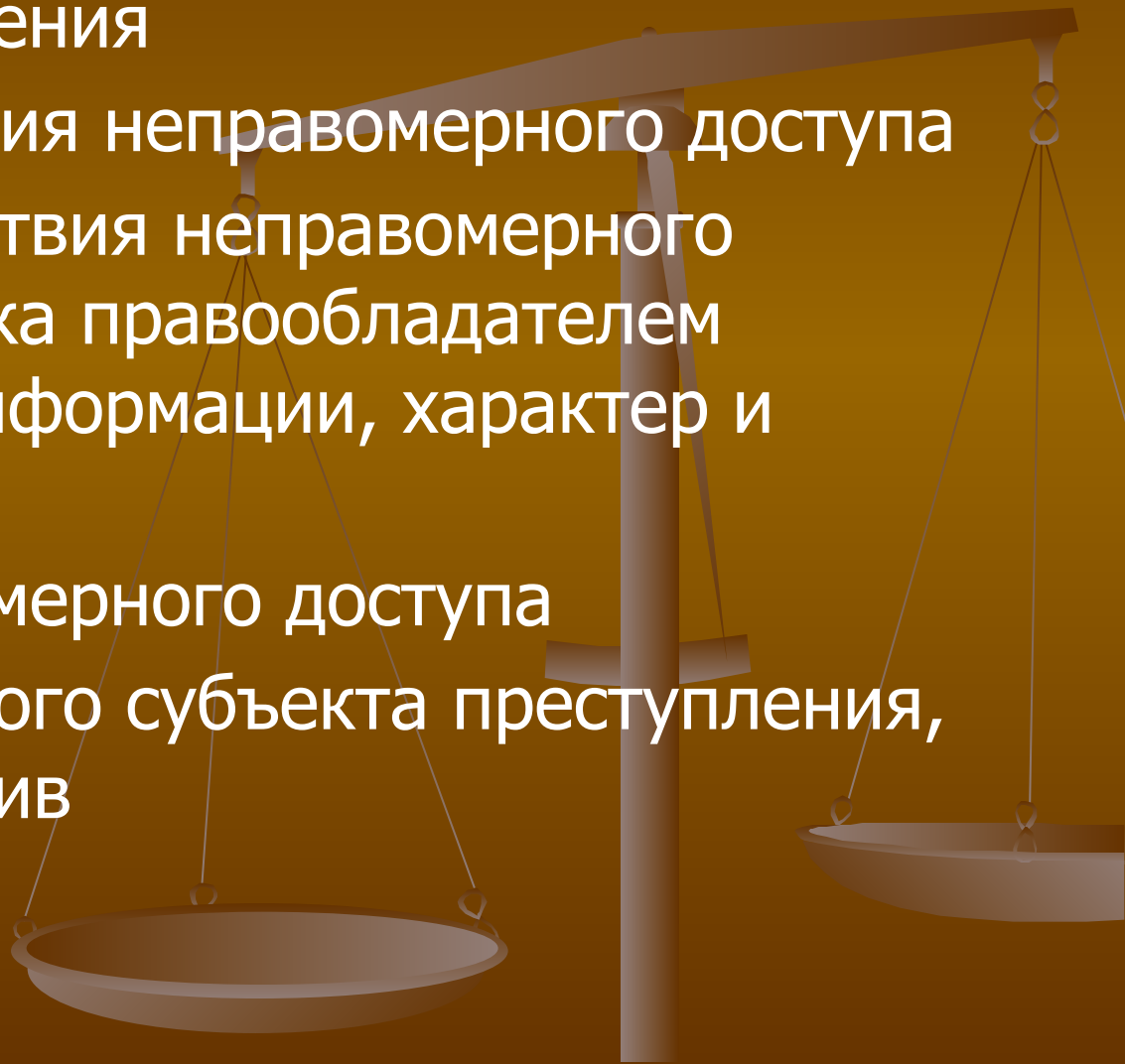
По делам о неправомерном доступе к компьютерной информации:

- Факт доступа к компьютерной информации
- Неправомерность доступа к компьютерной информации
- Место неправомерного доступа к компьютерной информации
- Время неправомерного доступа и время наступления вредных последствий



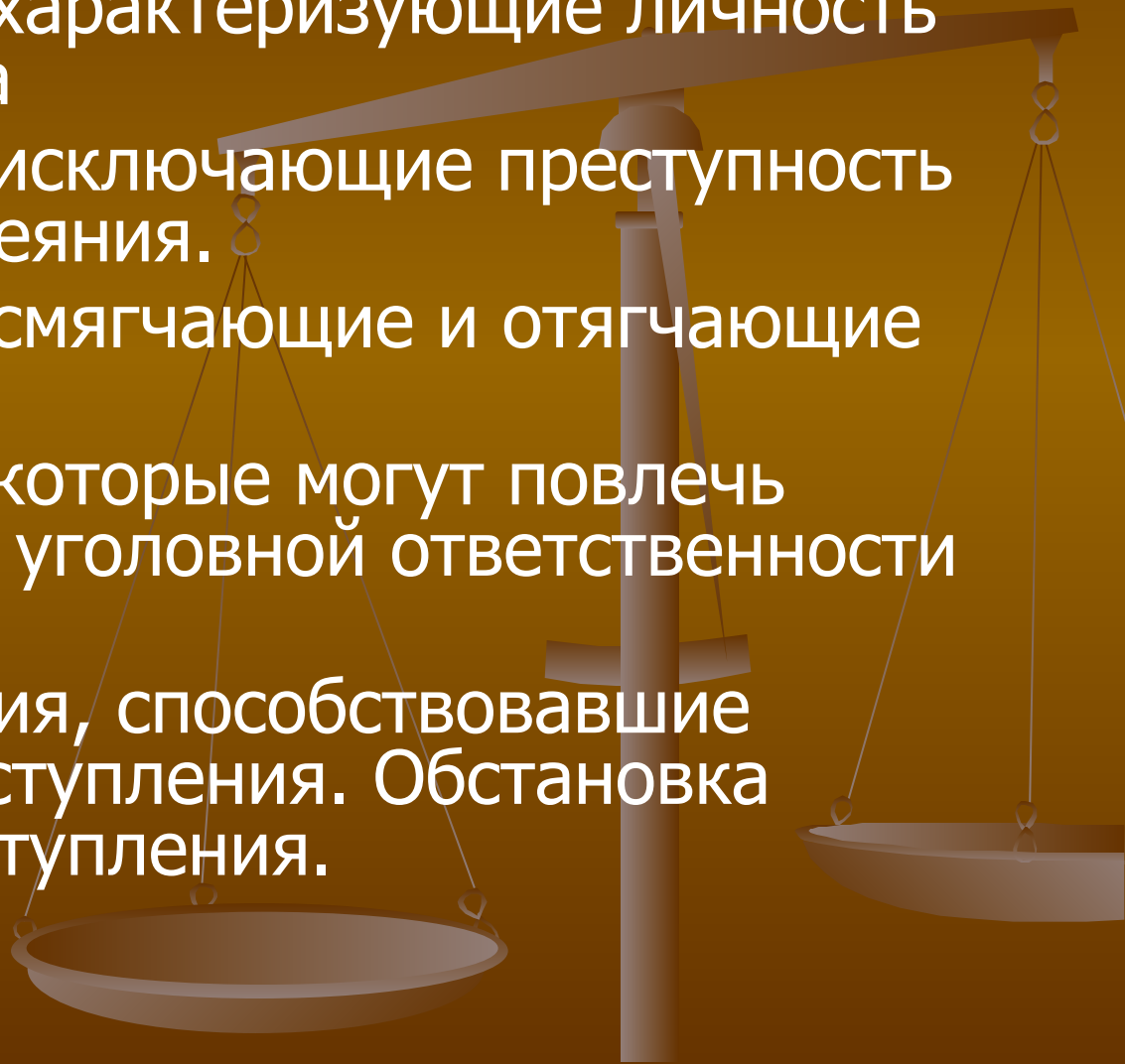
Обстоятельства, подлежащие установлению и доказыванию

- Орудия преступления
- Способ совершения неправомерного доступа
- Вредные последствия неправомерного доступа, их оценка правообладателем компьютерной информации, характер и размер вреда
- Субъект неправомерного доступа
- Виновность каждого субъекта преступления, форма вины, мотив



Обстоятельства, подлежащие установлению и доказыванию

- Обстоятельства, характеризующие личность каждого субъекта
- Обстоятельства, исключающие преступность и наказуемость деяния.
- Обстоятельства, смягчающие и отягчающие наказание
- Обстоятельства, которые могут повлечь освобождение от уголовной ответственности и наказания.
- Причины и условия, способствовавшие совершению преступления. Обстановка совершения преступления.



Обстоятельства, подлежащие установлению и доказыванию

При расследовании создания, использования и распространения вредоносных программ для ЭВМ

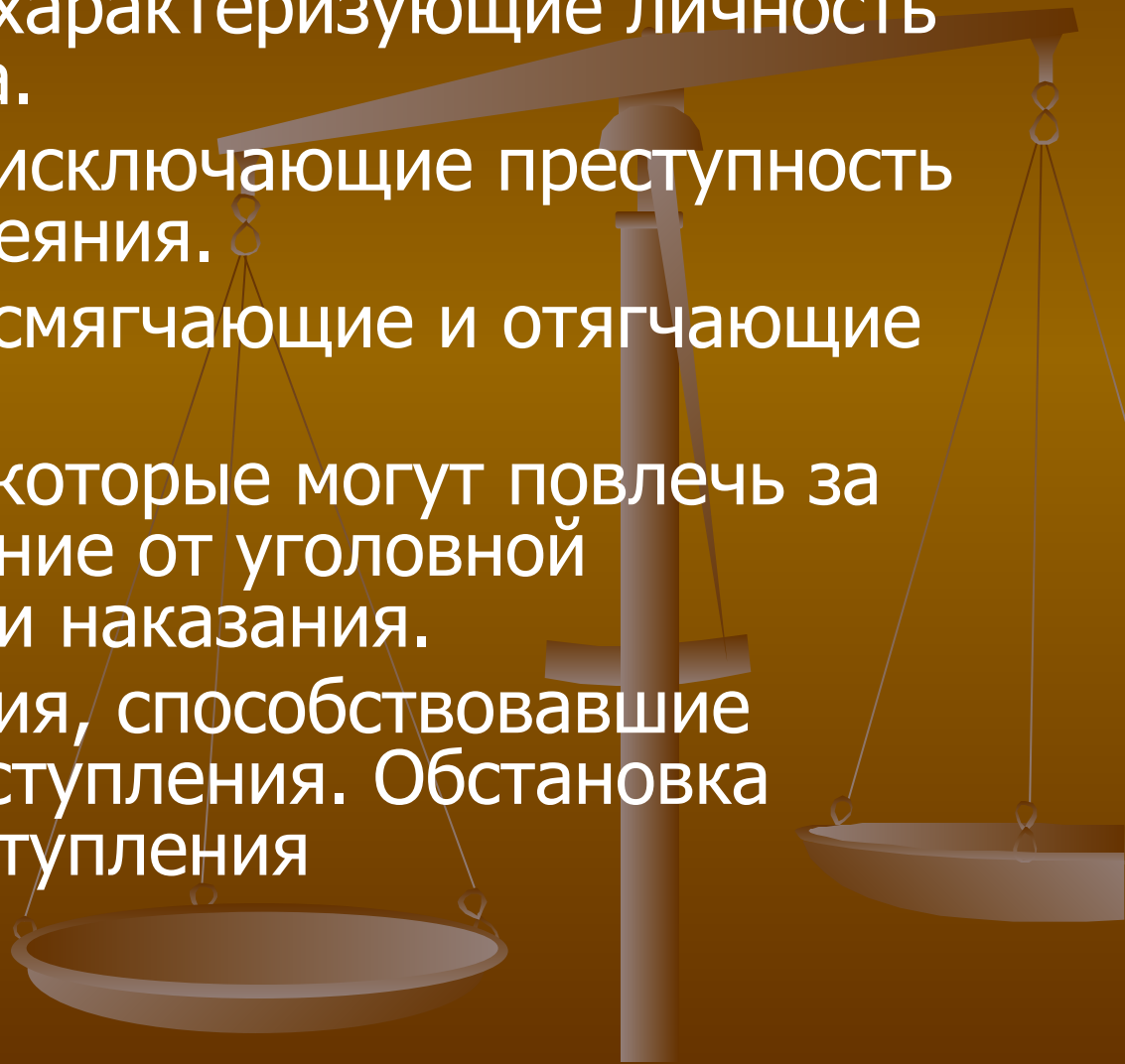
- Факт и способ создания, распространения или использования вредоносной программы для ЭВМ или иной компьютерной информации
- Вредные последствия, причиненные преступлением
- Физические и(или) юридические лица, потерпевшие от преступления

Обстоятельства, подлежащие установлению и доказыванию

- Место совершения преступления
- Время создания, использования, распространения вредоносных программ, время наступления вредных последствий
- Орудия преступления
- Субъект преступления, наличие преступной группы, распределение ролей между ее участниками
- Виновность каждого субъекта преступления, форма вины, мотив преступной деятельности

Обстоятельства, подлежащие установлению и доказыванию

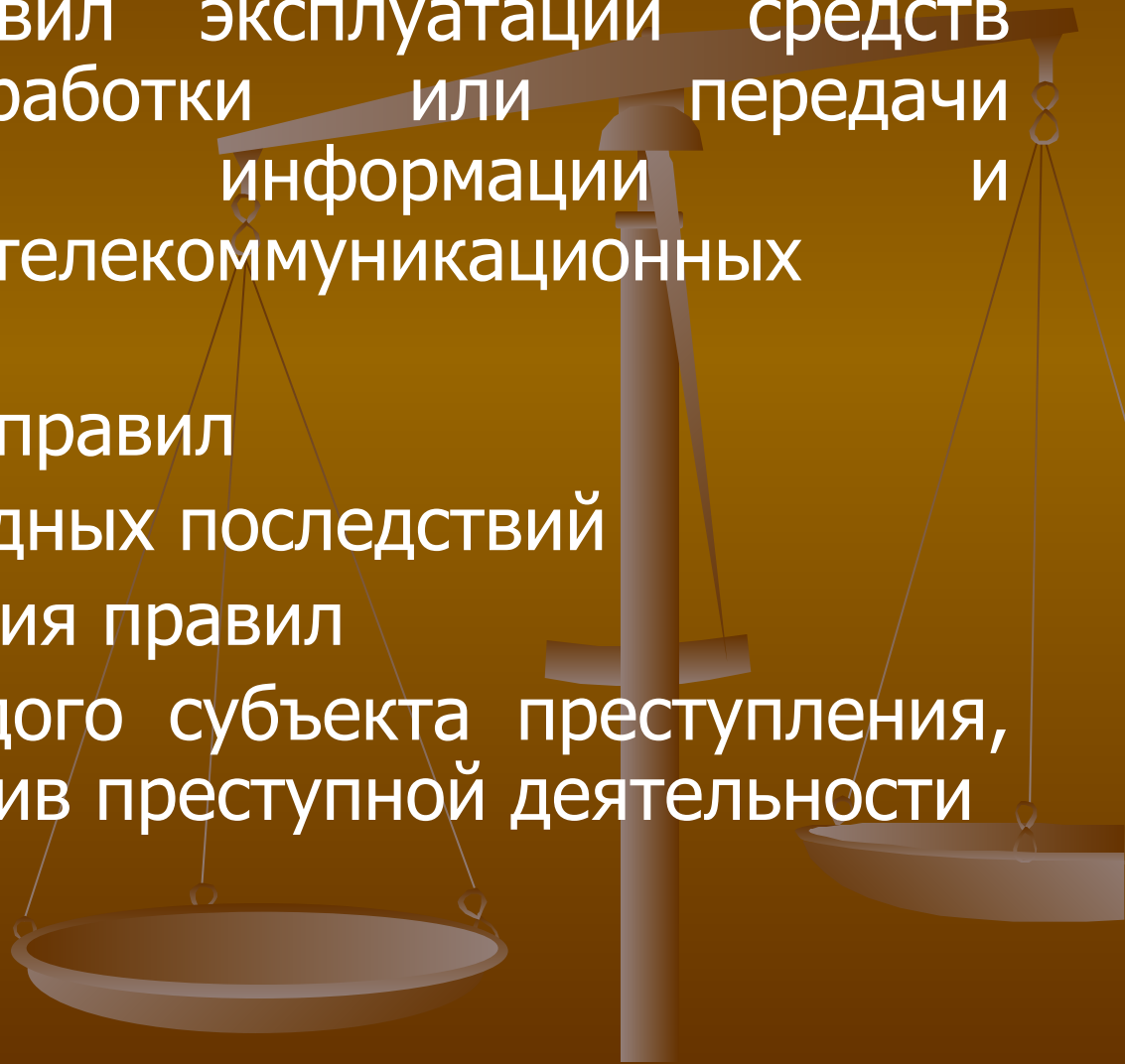
- Обстоятельства, характеризующие личность каждого субъекта.
- Обстоятельства, исключающие преступность и наказуемость деяния.
- Обстоятельства, смягчающие и отягчающие наказание.
- Обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания.
- Причины и условия, способствовавшие совершению преступления. Обстановка совершения преступления



Обстоятельства, подлежащие установлению и доказыванию

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

- Факт нарушения правил
- Наступление вредных последствий
- Субъект нарушения правил
- Виновность каждого субъекта преступления, форма вины, мотив преступной деятельности

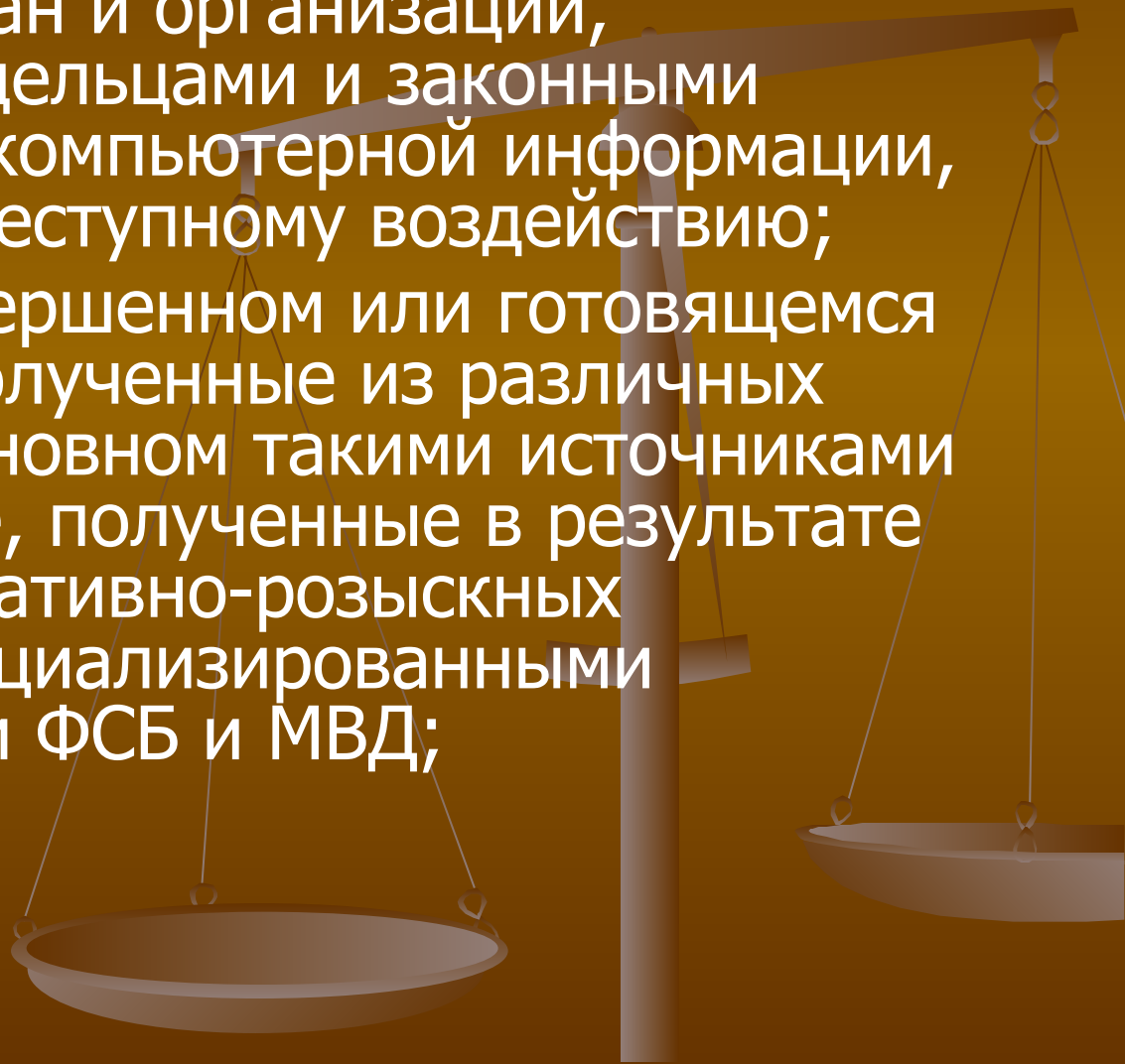


Обстоятельства, подлежащие установлению и доказыванию

- Обстоятельства, характеризующие личность каждого субъекта.
- Место и время нарушения правил эксплуатации.
- Обстоятельства, исключающие преступность и наказуемость деяния.
- Обстоятельства, смягчающие и отягчающие наказание
- Обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания.
- Причины и условия, способствовавшие совершению преступления. Обстановка совершения преступления.

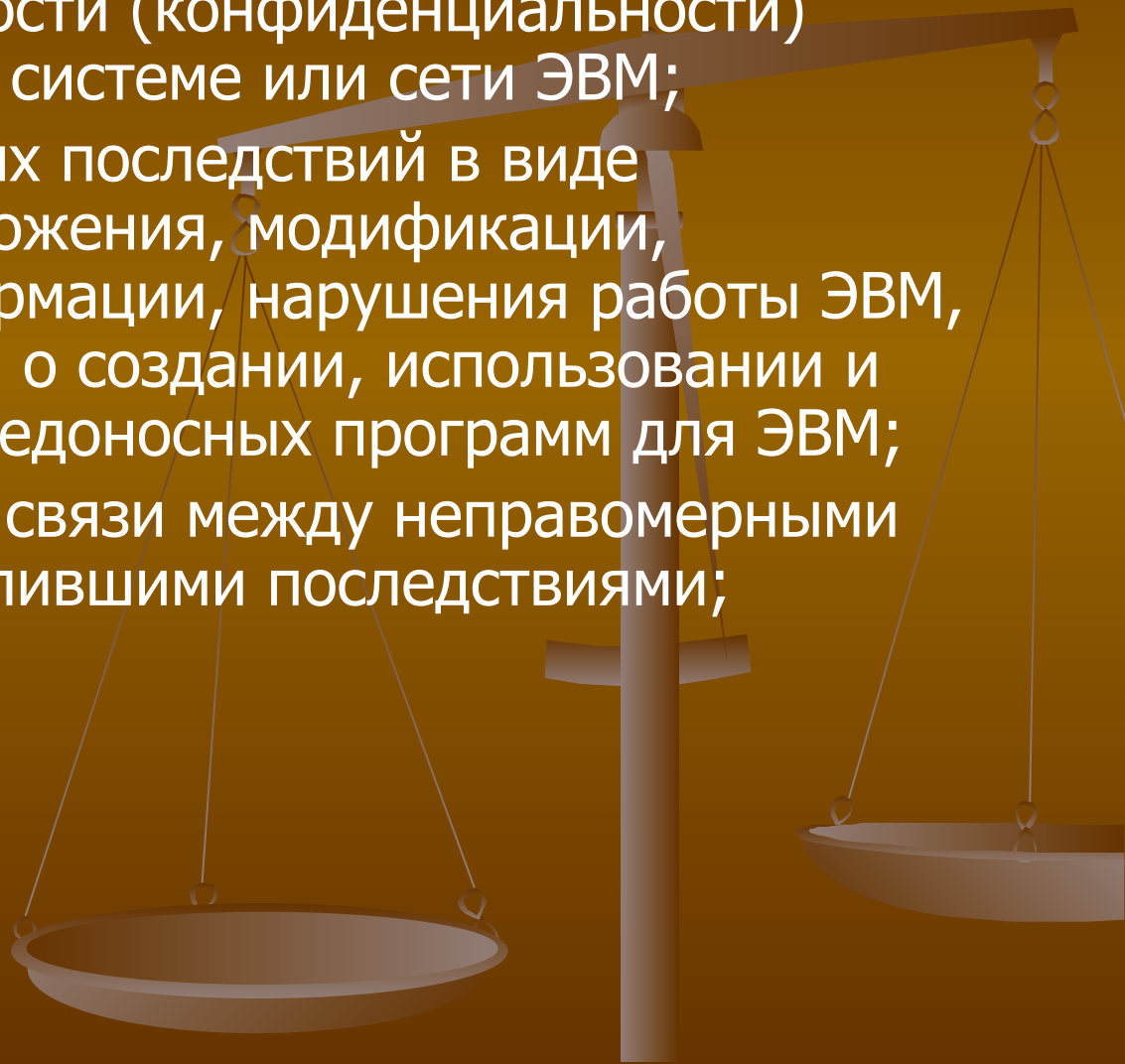
Поводы для возбуждения уголовного дела

- заявления граждан и организаций, являющихся владельцами и законными пользователями компьютерной информации, подвергшейся преступному воздействию;
- сообщения о совершенном или готовящемся преступлении, полученные из различных источников. В основном такими источниками являются данные, полученные в результате проведения оперативно-розыскных мероприятий специализированными подразделениями ФСБ и МВД;
- явка с повинной



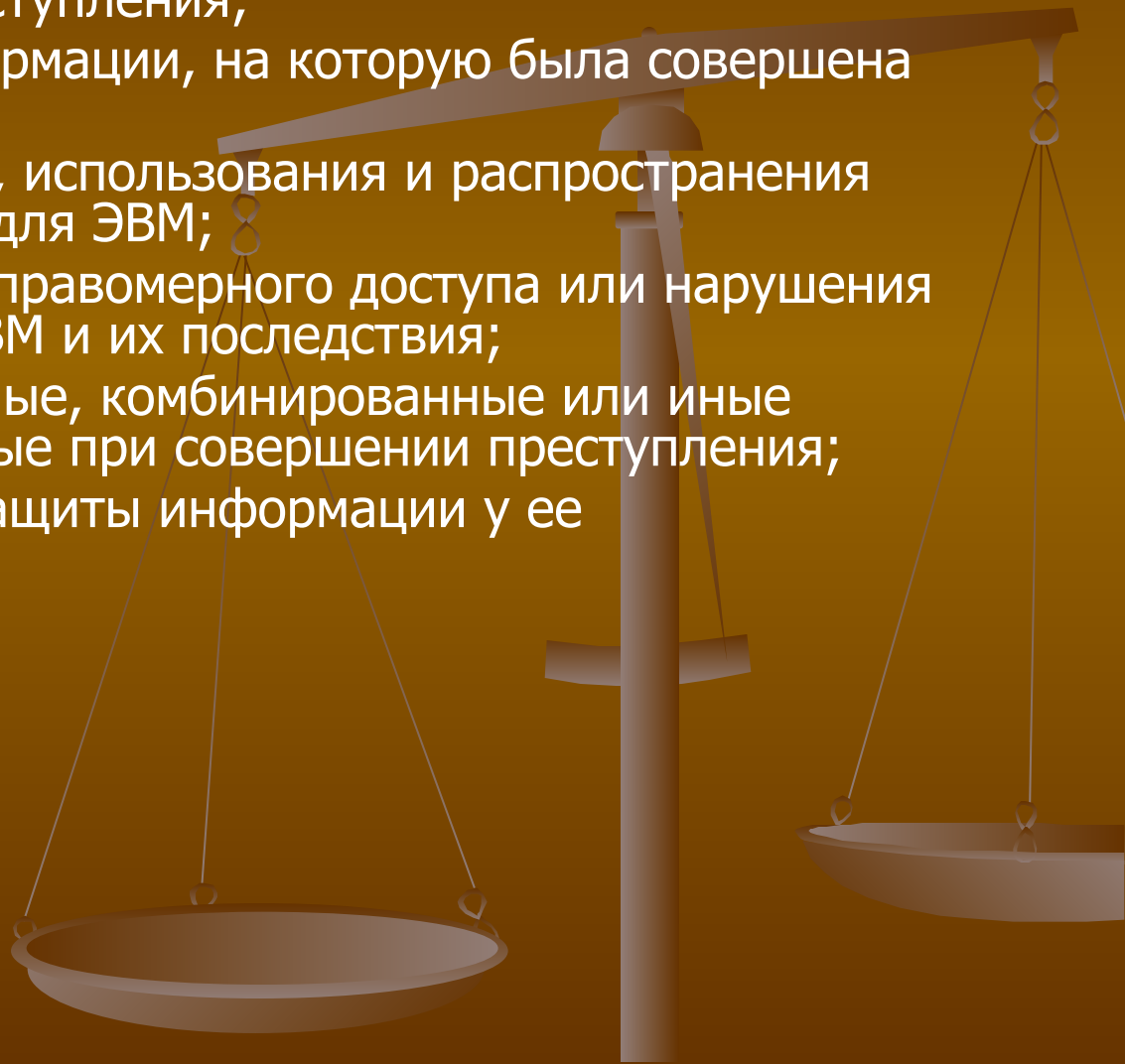
В ходе проверки должны найти подтверждение факты

- нарушения целостности (конфиденциальности) информации в ЭВМ, системе или сети ЭВМ;
- наступления вредных последствий в виде копирования, уничтожения, модификации, блокирования информации, нарушения работы ЭВМ, за исключением дел о создании, использовании и распространении вредоносных программ для ЭВМ;
- наличия причинной связи между неправомерными действиями и наступившими последствиями;
- размер ущерба.



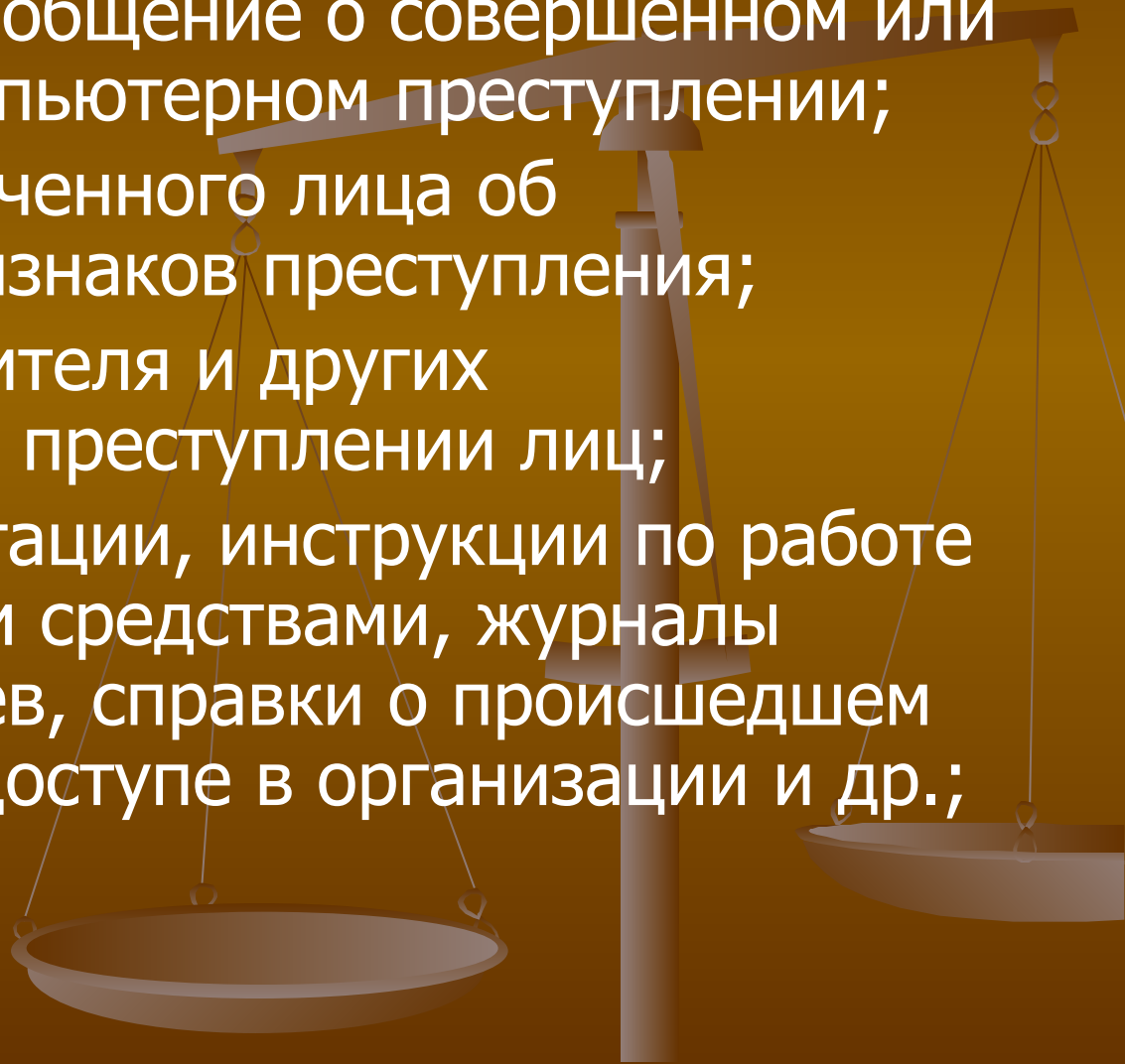
В процессе проверки заявления или сообщения следует принять меры к установлению

- время совершения преступления;
- место нахождения информации, на которую была совершена атака;
- время и место создания, использования и распространения вредоносных программ для ЭВМ;
- способы совершения неправомерного доступа или нарушения правил эксплуатации ЭВМ и их последствия;
- технические, программные, комбинированные или иные средства, использованные при совершении преступления;
- способы преодоления защиты информации у ее правообладателя;
- субъект преступления.



К моменту возбуждения уголовного дела материал проверки должен содержать:

- заявление или сообщение о совершенном или готовящемся компьютерном преступлении;
- рапорт уполномоченного лица об обнаружении признаков преступления;
- объяснения заявителя и других осведомлённых о преступлении лиц;
- правила эксплуатации, инструкции по работе с компьютерными средствами, журналы регистрации сбоев, справки о происшедшем неправомерном доступе в организации и др.;

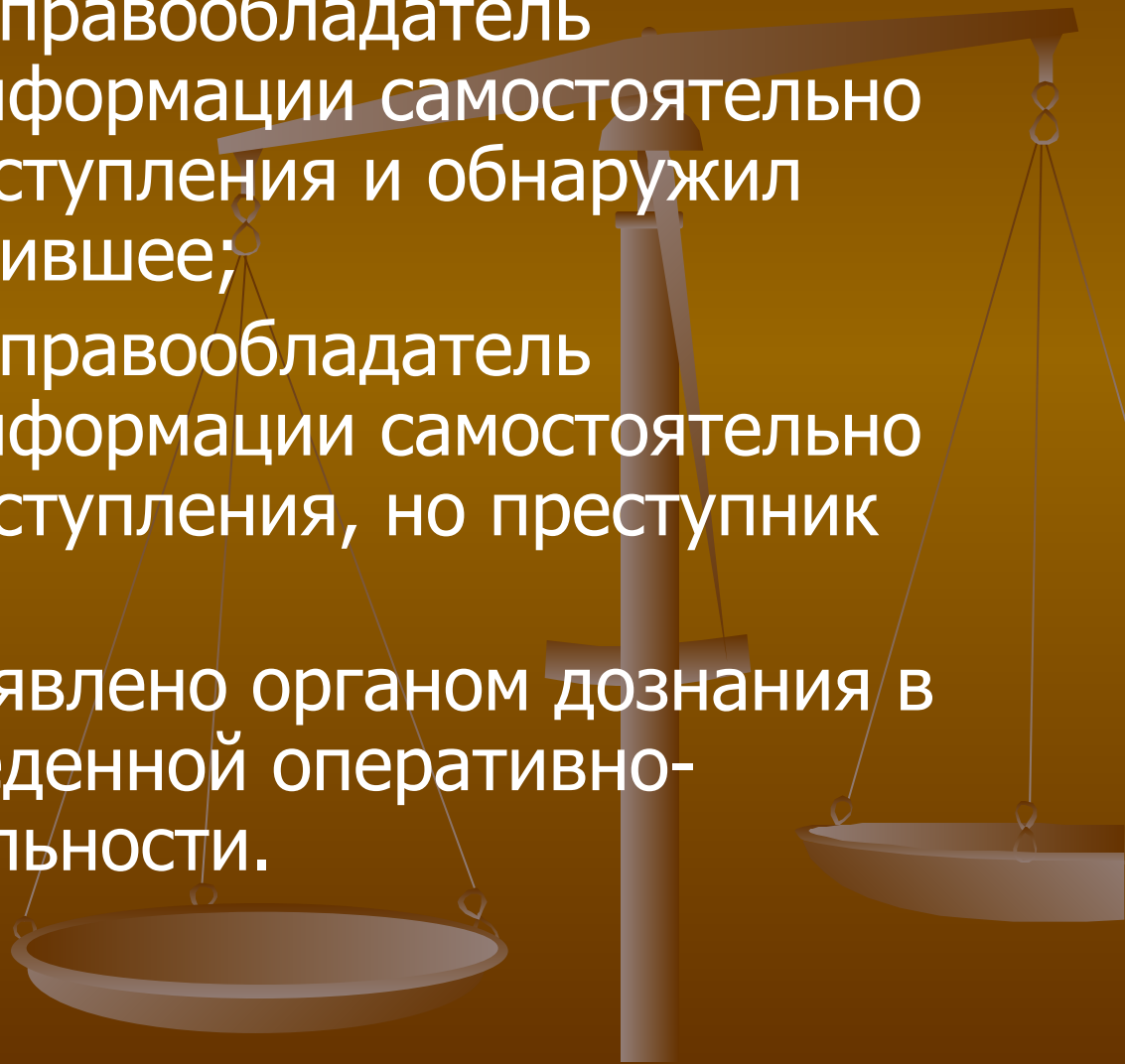


К моменту возбуждения уголовного дела материал проверки должен содержать:

- документы, подтверждающие распространение вредоносных программ через торговые предприятия;
- материалы органов, осуществлявших ОРД: протоколы проверочных закупок носителей с вредоносными программами, оперативного наблюдения, перехвата и регистрации информации электронной почты, оперативных экспериментов и других оперативно-розыскных мероприятий, проводимых по данному факту, стенограммы прослушивания телефонных переговоров и иных сообщений, перехвата информации с иных каналов связи, свидетельствующие о неправомерной деятельности подозреваемых лиц и других оперативно-розыскных мероприятий, проводившихся в ходе ОРД;
- постановление начальника органа, осуществляющего ОРД, о рассекречивании полученной информации;
- постановление начальника органа, осуществляющего ОРД, о представлении результатов ОРД дознавателю, органу дознания или следователю

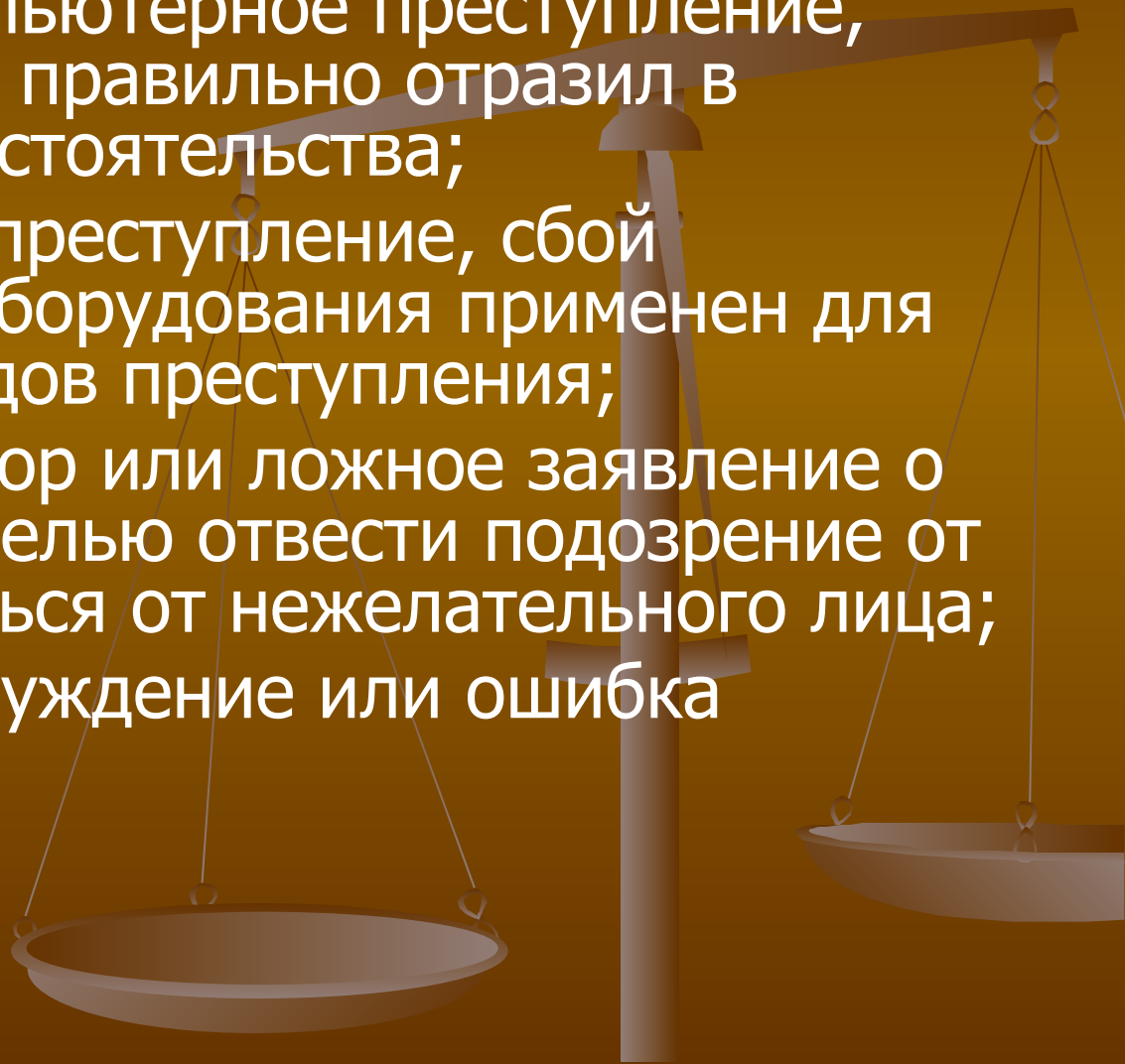
Типичные следственные ситуации

- собственник или правообладатель компьютерной информации самостоятельно выявил факт преступления и обнаружил лицо, его совершившее;
- собственник или правообладатель компьютерной информации самостоятельно выявил факт преступления, но преступник неизвестен;
- преступление выявлено органом дознания в результате проведенной оперативно-розыскной деятельности.



Типичные версии о событии:

- имело место компьютерное преступление, правообладатель правильно отразил в заявлении его обстоятельства;
- совершено иное преступление, сбой компьютерного оборудования применен для запутывания следов преступления;
- имеет место оговор или ложное заявление о преступлении с целью отвести подозрение от себя или избавиться от нежелательного лица;
- имеет место заблуждение или ошибка заявителя.



Типичные следственные действия

- Осмотр места происшествия
- Обыск и выемка
- Допросы: свидетелей-очевидцев, подозреваемого, обвиняемого, потерпевшего
- Назначение судебных экспертиз