

Лекция:

**Противодействие преступлениям
в сфере компьютерной информации**

Доцент кафедры прикладной информатики и информационной безопасности к.т.н., доцент Карпов Д.С.

Учебные вопросы

1. Нормативно-правовая основа противодействия преступлениям в сфере компьютерной информации в РФ
2. Расследование преступлений в сфере компьютерной информации
3. Правоприменительная практика в области противодействия преступлениям в сфере компьютерной информации

Перечень основных нормативно-правовых актов в области противодействия преступлениям в сфере компьютерной информации

1. Конституция Российской Федерации от 25.12.1993 года.
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон Российской Федерации от 28 декабря 2010 г. № 403-ФЗ «О Следственном комитете Российской Федерации».
4. Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности».
5. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции».
6. Уголовный кодекс Российской Федерации (№ 63-ФЗ от 13 июня 1996 года).
7. Уголовно-процессуальный кодекс Российской Федерации (№ 174-ФЗ от 18 декабря 2001 года).

Классификация компьютерных преступлений и преступлений, совершаемых с использованием новых информационных технологий

Несмотря на многообразие компьютерных преступлений, практически все способы их совершения имеют свои индивидуальные, присущие только им признаки, по которым их можно распознать и классифицировать по отдельным общим группам:

1. Неправомерный доступ к компьютерной информации:

- Преступления, совершаемые в отношении компьютерной информации, находящейся в компьютерах и глобальных компьютерных сетях или при обращении к ним.

- Преступления, совершаемые в отношении компьютерной информации, находящейся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (таких, как сервер, сотовый телефон, кассовый аппарат и т.п).

2. Изготовление или распространение вредоносных программ (вирусы, программы - взломщики и т.п.).

3. Нарушение авторских прав (компьютерное пиратство).

4. Мошенничество с использованием платежных карт.

5. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", а также средств связи, в том числе подвижной связи.

Вопрос 1

Нормативно-правовая основа противодействия преступлениям в сфере компьютерной информации в РФ

Статья 14. Понятие преступления

1. Преступлением признается виновно совершенное общественно опасное деяние, запрещенное настоящим Кодексом под угрозой наказания.
2. Не является преступлением действие (бездействие), хотя формально и содержащее признаки какого-либо деяния, предусмотренного настоящим Кодексом, но в силу малозначительности не представляющее общественной опасности.

Статья 15. Категории преступлений

1. В зависимости от характера и степени общественной опасности деяния, предусмотренные настоящим Кодексом, подразделяются на преступления небольшой тяжести, преступления средней тяжести, тяжкие преступления и особо тяжкие преступления.
2. Преступлениями **небольшой тяжести** признаются умышленные и неосторожные деяния, за совершение которых максимальное наказание, предусмотренное настоящим Кодексом, **не превышает трех лет лишения свободы**.
3. Преступлениями **средней тяжести** признаются умышленные деяния, за совершение которых максимальное наказание, предусмотренное настоящим Кодексом, **не превышает пяти лет лишения свободы**, и неосторожные деяния, за совершение которых максимальное наказание, предусмотренное настоящим Кодексом, превышает три года лишения свободы.
4. **Тяжкими преступлениями** признаются умышленные деяния, за совершение которых максимальное наказание, предусмотренное настоящим Кодексом, **не превышает десяти лет лишения свободы**.
5. **Особо тяжкими преступлениями** признаются умышленные деяния, за совершение которых настоящим Кодексом предусмотрено **наказание в виде лишения свободы на срок свыше десяти лет или более строгое наказание**.
6. С учетом фактических обстоятельств преступления и степени его общественной опасности суд вправе при наличии смягчающих наказание обстоятельств и при отсутствии отягчающих наказание обстоятельств изменить категорию преступления на менее тяжкую, но не более чем на одну категорию преступления при условии, что за совершение преступления, указанного в части третьей настоящей статьи, осужденному назначено наказание, не превышающее трех лет лишения свободы, или другое более мягкое наказание; за совершение преступления, указанного в части четвертой настоящей статьи, осужденному назначено наказание, не превышающее пяти лет лишения свободы, или другое более мягкое наказание; за совершение преступления, указанного в части пятой настоящей статьи, осужденному назначено наказание, ⁶ не превышающее семи лет лишения свободы.

Статья 205.6. Несообщение о преступлении

(введена Федеральным законом от 06.07.2016 N 375-ФЗ)

Несообщение в органы власти, уполномоченные рассматривать сообщения о преступлении, о лице (лицах), которое по достоверно известным сведениям готовит, совершает или совершило хотя бы одно из преступлений, предусмотренных статьями* 205, 205.1, 205.2, 205.3, 205.4, 205.5, 206, 208, 211, 220, 221, 277, 278, 279, 360 и 361 настоящего Кодекса, -

наказывается штрафом в размере до ста тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо принудительными работами на срок до одного года, либо лишением свободы на тот же срок.

Примечание. Лицо не подлежит уголовной ответственности за несообщение о подготовке или совершении преступления его супругом или близким родственником.

Статья 316. Укрывательство преступлений

Заранее не обещанное укрывательство особо тяжких преступлений -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо принудительными работами на срок до двух лет, либо арестом на срок до шести месяцев, либо лишением свободы на срок до двух лет.

Примечание. Лицо не подлежит уголовной ответственности за заранее не обещанное укрывательство преступления, совершенного его супругом или близким родственником.

*Статья 205. Террористический акт; Статья 206. Захват заложника; Статья 208. Организация незаконного вооруженного формирования или участие в нем; Статья 211. Угон судна воздушного или водного транспорта либо железнодорожного подвижного состава; Статья 220. Незаконное обращение с ядерными материалами или радиоактивными веществами; Статья 221. Хищение либо вымогательство ядерных материалов или радиоактивных веществ; Статья 277. Посягательство на жизнь государственного или общественного деятеля; Статья 278. Насильственный захват власти или насильственное удержание власти; Статья 279. Вооруженный мятеж; Статья 360. Нападение на лиц или учреждения, которые пользуются международной защитой; Статья 361. Акт международного терроризма

Статья 20. Возраст, с которого наступает уголовная ответственность

1. Уголовной ответственности подлежит лицо, достигшее ко времени совершения преступления шестнадцатилетнего возраста.
2. Лица, достигшие ко времени совершения преступления четырнадцатилетнего возраста, подлежат уголовной ответственности за убийство (статья 105), умышленное причинение тяжкого вреда здоровью (статья 111), умышленное причинение средней тяжести вреда здоровью (статья 112), похищение человека (статья 126), изнасилование (статья 131), насильственные действия сексуального характера (статья 132), кражу (статья 158), грабеж (статья 161), разбой (статья 162), вымогательство (статья 163), неправомерное завладение автомобилем или иным транспортным средством без цели хищения (статья 166), умышленные уничтожение или повреждение имущества при отягчающих обстоятельствах (часть вторая статьи 167), террористический акт (статья 205), прохождение обучения в целях осуществления террористической деятельности (статья 205.3), участие в террористическом сообществе (часть вторая статьи 205.4), участие в деятельности террористической организации (часть вторая статьи 205.5), **несообщение о преступлении** (статья 205.6), захват заложника (статья 206), **заведомо ложное сообщение об акте терроризма** (статья 207), участие в незаконном вооруженном формировании (часть вторая статьи 208), угон судна воздушного или водного транспорта либо железнодорожного подвижного состава (статья 211), участие в массовых беспорядках (часть вторая статьи 212), хулиганство при отягчающих обстоятельствах (часть вторая и третья статьи 213), вандализм (статья 214), незаконные приобретение, передачу, сбыт, хранение, перевозку или ношение взрывчатых веществ или взрывных устройств (статья 222.1), **незаконное изготовление взрывчатых веществ или взрывных устройств** (статья 223.1), хищение либо вымогательство оружия, боеприпасов, взрывчатых веществ и взрывных устройств (статья 226), хищение либо вымогательство наркотических средств или психотропных веществ (статья 229), приведение в негодность транспортных средств или путей сообщения (статья 267), посягательство на жизнь государственного или общественного деятеля (статья 277), нападение на лиц или учреждения, которые пользуются международной защитой (статья 360), акт международного терроризма (статья 361).
3. Если несовершеннолетний достиг возраста, предусмотренного частями первой или второй настоящей статьи, но вследствие отставания в психическом развитии, не связанном с психическим расстройством, во время совершения общественно опасного деяния не мог в полной мере осознавать фактический характер и общественную опасность своих действий (бездействия) либо руководить ими, он не подлежит уголовной ответственности.

Раздел III. НАКАЗАНИЕ

Глава 9. ПОНЯТИЕ И ЦЕЛИ НАКАЗАНИЯ. ВИДЫ НАКАЗАНИЙ

Статья 43. Понятие и цели наказания

1. Наказание есть мера государственного принуждения, назначаемая по приговору суда. **Наказание применяется к лицу, признанному виновным в совершении преступления, и заключается в предусмотренных настоящим Кодексом лишении или ограничении прав и свобод этого лица.**

2. **Наказание применяется в целях восстановления социальной справедливости, а также в целях исправления осужденного и предупреждения совершения новых преступлений.**

Статья 44. Виды наказаний

Видами наказаний являются:

- а) штраф;
- б) лишение права занимать определенные должности или заниматься определенной деятельностью;
- в) лишение специального, воинского или почетного звания, классного чина и государственных наград;
- г) обязательные работы;
- д) исправительные работы;
- е) ограничение по военной службе;
- ж) утратил силу. - Федеральный закон от 08.12.2003 N 162-ФЗ;
- з) ограничение свободы;
 - з.1) принудительные работы;
- и) арест;
- к) содержание в дисциплинарной воинской части;
- л) лишение свободы на определенный срок;
- м) пожизненное лишение свободы;
- н) смертная казнь.

Статья 45. Основные и дополнительные виды наказаний

1. Обязательные работы, исправительные работы, ограничение по военной службе, принудительные работы, арест, содержание в дисциплинарной воинской части, лишение свободы на определенный срок, пожизненное лишение свободы, смертная казнь применяются только в качестве основных видов наказаний.

2. Штраф, лишение права занимать определенные должности или заниматься определенной деятельностью и ограничение свободы применяются в качестве как основных, так и дополнительных видов наказаний.

3. Лишение специального, воинского или почетного звания, классного чина и государственных наград применяется только в качестве дополнительных видов наказаний.

Статья 46. Штраф

1. Штраф есть денежное взыскание, назначаемое в пределах, предусмотренных настоящим Кодексом.
2. Штраф устанавливается в размере от пяти тысяч до пяти миллионов рублей или в размере заработной платы или иного дохода осужденного за период от двух недель до пяти лет либо исчисляется в величине, кратной стоимости предмета или сумме коммерческого подкупа, взятки или сумме незаконно перемещенных денежных средств и (или) стоимости денежных инструментов. Штраф в размере от пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период свыше трех лет может назначаться только в случаях, специально предусмотренных соответствующими статьями Особенной части настоящего Кодекса, за исключением случаев исчисления размера штрафа исходя из величины, кратной сумме коммерческого подкупа, взятки или сумме незаконно перемещенных денежных средств и (или) стоимости денежных инструментов. Штраф, исчисляемый исходя из величины, кратной сумме коммерческого подкупа, взятки или сумме незаконно перемещенных денежных средств и (или) стоимости денежных инструментов, устанавливается в размере до стократной суммы коммерческого подкупа, взятки или суммы незаконно перемещенных денежных средств и (или) стоимости денежных инструментов, но не может быть менее двадцати пяти тысяч рублей и более пятисот миллионов рублей.
3. Размер штрафа определяется судом с учетом тяжести совершенного преступления и имущественного положения осужденного и его семьи, а также с учетом возможности получения осужденным заработной платы или иного дохода. С учетом тех же обстоятельств суд может назначить штраф с рассрочкой выплаты определенными частями на срок до пяти лет.
4. Штраф в качестве дополнительного вида наказания может назначаться только в случаях, предусмотренных соответствующими статьями Особенной части настоящего Кодекса.
5. В случае злостного уклонения от уплаты штрафа, назначенного в качестве основного наказания, за исключением случаев назначения штрафа в размере, исчисляемом исходя из величины, кратной стоимости предмета или сумме коммерческого подкупа или взятки, штраф заменяется иным наказанием, за исключением лишения свободы. В случае злостного уклонения от уплаты штрафа в размере, исчисляемом исходя из величины, кратной стоимости предмета или сумме коммерческого подкупа или взятки, назначенного в качестве основного наказания, штраф заменяется наказанием в пределах санкции, предусмотренной соответствующей статьей Особенной части настоящего Кодекса. При этом назначенное наказание не может быть условным

Статья 47. Лишение права занимать определенные должности или заниматься определенной деятельностью

1. Лишение права занимать определенные должности или заниматься определенной деятельностью состоит в запрещении занимать должности на государственной службе, в органах местного самоуправления либо заниматься определенной профессиональной или иной деятельностью.

2. Лишение права занимать определенные должности или заниматься определенной деятельностью устанавливается на срок от одного года до пяти лет в качестве основного вида наказания и на срок от шести месяцев до трех лет в качестве дополнительного вида наказания. В случаях, специально предусмотренных соответствующими статьями Особенной части настоящего Кодекса, лишение права занимать определенные должности или заниматься определенной деятельностью устанавливается на срок до двадцати лет в качестве дополнительного вида наказания.

3. Лишение права занимать определенные должности или заниматься определенной деятельностью может назначаться в качестве дополнительного вида наказания и в случаях, когда оно не предусмотрено соответствующей статьей Особенной части настоящего Кодекса в качестве наказания за соответствующее преступление, если с учетом характера и степени общественной опасности совершенного преступления и личности виновного суд признает невозможным сохранение за ним права занимать определенные должности или заниматься определенной деятельностью.

4. В случае назначения этого вида наказания в качестве дополнительного к обязательным работам, исправительным работам, ограничению свободы, а также при условном осуждении его срок исчисляется с момента вступления приговора суда в законную силу. В случае назначения лишения права занимать определенные должности или заниматься определенной деятельностью в качестве дополнительного вида наказания к аресту, содержанию в дисциплинарной воинской части, принудительным работам, лишению свободы оно распространяется на все время отбывания указанных основных видов наказаний, но при этом его срок исчисляется с момента их отбытия.

Статья 48. Лишение специального, воинского или почетного звания, классного чина и государственных наград

При осуждении за совершение тяжкого или особо тяжкого преступления с учетом личности виновного суд может лишить его специального, воинского или почетного звания, классного чина и государственных наград.

Статья 49. Обязательные работы

1. Обязательные работы заключаются в выполнении осужденным **в свободное от основной работы или учебы время** бесплатных общественно полезных работ. Вид обязательных работ и объекты, на которых они отбываются, определяются органами местного самоуправления по согласованию с уголовно-исполнительными инспекциями.

2. Обязательные работы устанавливаются на срок от шестидесяти до четырехсот восьмидесяти часов и отбываются не свыше четырех часов в день.

3. В случае злостного уклонения осужденного от отбывания обязательных работ они заменяются **принудительными работами или лишением свободы**. При этом время, в течение которого осужденный отбывал обязательные работы, учитывается при определении срока принудительных работ или лишения свободы из расчета один день принудительных работ или один день лишения свободы за восемь часов обязательных работ.

4. Обязательные работы не назначаются лицам, признанным инвалидами первой группы, беременным женщинам, женщинам, имеющим детей в возрасте до трех лет, военнослужащим, проходящим военную службу по призыву, а также военнослужащим, проходящим военную службу по контракту на воинских должностях рядового и сержантского состава, если они на момент вынесения судом приговора не отслужили установленного законом срока службы по призыву.

Статья 50. Исправительные работы

1. Исправительные работы назначаются осужденному, имеющему основное место работы, а равно не имеющему его. **Осужденный, имеющий основное место работы, отбывает исправительные работы по основному месту работы.** Осужденный, не имеющий основного места работы, отбывает исправительные работы в местах, определяемых органами местного самоуправления по согласованию с уголовно-исполнительными инспекциями, но в районе места жительства осужденного.
2. Исправительные работы устанавливаются на срок от двух месяцев до двух лет.
3. **Из заработной платы осужденного к исправительным работам производятся удержания в доход государства в размере, установленном приговором суда, в пределах от пяти до двадцати процентов.**
4. В случае злостного уклонения осужденного от отбывания исправительных работ суд может заменить неотбытое наказание принудительными работами или лишением свободы из расчета один день принудительных работ или один день лишения свободы за три дня исправительных работ.
5. Исправительные работы не назначаются лицам, признанным инвалидами первой группы, беременным женщинам, женщинам, имеющим детей в возрасте до трех лет, военнослужащим, проходящим военную службу по призыву, а также военнослужащим, проходящим военную службу по контракту на воинских должностях рядового и сержантского состава, если они на момент вынесения судом приговора не отслужили установленного законом срока службы по призыву.

Статья 51. Ограничение по военной службе

1. Ограничение по военной службе назначается осужденным военнослужащим, проходящим военную службу по контракту, на срок от трех месяцев до двух лет в случаях, предусмотренных соответствующими статьями Особенной части настоящего Кодекса за совершение преступлений против военной службы, а также осужденным военнослужащим, проходящим военную службу по контракту, вместо исправительных работ, предусмотренных соответствующими статьями Особенной части настоящего Кодекса.

2. Из денежного довольствия осужденного к ограничению по военной службе производятся удержания в доход государства в размере, установленном приговором суда, но не свыше двадцати процентов. Во время отбывания этого наказания осужденный не может быть повышен в должности, воинском звании, а срок наказания не засчитывается в срок выслуги лет для присвоения очередного воинского звания.

Статья 53. Ограничение свободы

1. Ограничение свободы заключается в установлении судом осужденному следующих ограничений: не уходить из места постоянного проживания (пребывания) в определенное время суток, не посещать определенные места, расположенные в пределах территории соответствующего муниципального образования, не выезжать за пределы территории соответствующего муниципального образования, не посещать места проведения массовых и иных мероприятий и не участвовать в указанных мероприятиях, не изменять место жительства или пребывания, место работы и (или) учебы без согласия специализированного государственного органа, осуществляющего надзор за отбыванием осужденными наказания в виде ограничения свободы, в случаях, предусмотренных законодательством Российской Федерации. При этом суд возлагает на осужденного обязанность являться в специализированный государственный орган, осуществляющий надзор за отбыванием осужденными наказания в виде ограничения свободы, от одного до четырех раз в месяц для регистрации. Установление судом осужденному ограничений на изменение места жительства или пребывания без согласия указанного специализированного государственного органа, а также на выезд за пределы территории соответствующего муниципального образования является обязательным.

2. Ограничение свободы назначается на срок от двух месяцев до четырех лет в качестве основного вида наказания за преступления небольшой тяжести и преступления средней тяжести, а также на срок от шести месяцев до двух лет в качестве дополнительного вида наказания к принудительным работам или лишению свободы в случаях, предусмотренных соответствующими статьями Особенной части настоящего Кодекса.

3. В период отбывания ограничения свободы суд по представлению специализированного государственного органа, осуществляющего надзор за отбыванием осужденными наказания в виде ограничения свободы, может отменить частично либо дополнить ранее установленные осужденному ограничения.

4. Надзор за осужденным, отбывающим ограничение свободы, осуществляется в порядке, предусмотренном уголовно-исполнительным законодательством Российской Федерации, а также издаваемыми в соответствии с ним нормативными правовыми актами уполномоченных федеральных органов исполнительной власти.

5. В случае злостного уклонения осужденного от отбывания ограничения свободы, назначенного в качестве основного вида наказания, суд по представлению специализированного государственного органа, осуществляющего надзор за отбыванием осужденными наказания в виде ограничения свободы, может заменить неотбытую часть наказания принудительными работами или лишением свободы из расчета один день принудительных работ за два дня ограничения свободы или один день лишения свободы за два дня ограничения свободы.

6. Ограничение свободы не назначается военнослужащим, иностранным гражданам, лицам без гражданства, а также лицам, не имеющим места постоянного проживания на территории РФ.

Статья 53.1. Принудительные работы

1. Принудительные работы применяются как альтернатива лишению свободы в случаях, предусмотренных соответствующими статьями Особенной части настоящего Кодекса, за совершение преступления небольшой или средней тяжести либо за совершение тяжкого преступления впервые.
2. Если, назначив наказание в виде лишения свободы, суд придет к выводу о возможности исправления осужденного без реального отбывания наказания в местах лишения свободы, он постановляет заменить осужденному наказание в виде лишения свободы принудительными работами. При назначении судом наказания в виде лишения свободы на срок более пяти лет принудительные работы не применяются.
3. Принудительные работы заключаются в привлечении осужденного к труду в местах, определяемых учреждениями и органами уголовно-исполнительной системы.
4. Принудительные работы назначаются на срок от двух месяцев до пяти лет.
5. Из заработной платы осужденного к принудительным работам производятся удержания в доход государства, перечисляемые на счет соответствующего территориального органа уголовно-исполнительной системы, в размере, установленном приговором суда, и в пределах от пяти до двадцати процентов.
6. В случае уклонения осужденного от отбывания принудительных работ они заменяются лишением свободы из расчета один день лишения свободы за один день принудительных работ.
7. Принудительные работы не назначаются несовершеннолетним, лицам, признанным инвалидами первой или второй группы, беременным женщинам, женщинам, имеющим детей в возрасте до трех лет, женщинам, достигшим пятидесятипятилетнего возраста, мужчинам, достигшим шестидесятилетнего возраста, а также военнослужащим.

Статья 54. Арест*

1. Арест заключается в содержании осужденного в условиях строгой изоляции от общества и устанавливается на срок от одного до шести месяцев. В случае замены обязательных работ или исправительных работ арестом он может быть назначен на срок менее одного месяца.
2. Арест не назначается лицам, не достигшим к моменту вынесения судом приговора восемнадцатилетнего возраста, а также беременным женщинам и женщинам, имеющим детей в возрасте до четырнадцати лет.
3. Военнослужащие отбывают арест на гауптвахте.

Статья 55. Содержание в дисциплинарной воинской части

1. Содержание в дисциплинарной воинской части назначается военнослужащим, проходящим военную службу по призыву, а также военнослужащим, проходящим военную службу по контракту на должностях рядового и сержантского состава, если они на момент вынесения судом приговора не отслужили установленного законом срока службы по призыву. Это наказание устанавливается на срок от трех месяцев до двух лет в случаях, предусмотренных соответствующими статьями Особенной части настоящего Кодекса за совершение преступлений против военной службы, а также в случаях, когда характер преступления и личность виновного свидетельствуют о возможности замены лишения свободы на срок не свыше двух лет содержанием осужденного в дисциплинарной воинской части на тот же срок.
2. При содержании в дисциплинарной воинской части вместо лишения свободы срок содержания в дисциплинарной воинской части определяется из расчета один день лишения свободы за один день содержания в дисциплинарной воинской части.

*В целях исполнения данного наказания предусмотрено создание арестных домов. Однако, на сегодняшний день их так и не создали, поэтому данный вид наказания, суды не применяют.

Статья 56. Лишение свободы на определенный срок

1. Лишение свободы заключается в изоляции осужденного от общества путем направления его в колонию-поселение, помещения в воспитательную колонию, лечебное исправительное учреждение, исправительную колонию общего, строгого или особого режима либо в тюрьму. Наказание в виде лишения свободы может быть назначено осужденному, совершившему впервые преступление небольшой тяжести, только при наличии отягчающих обстоятельств, предусмотренных статьей 63 настоящего Кодекса*, за исключением преступлений, предусмотренных частью первой статьи 228, частью первой статьи 231 и статьей 233 настоящего Кодекса, или только если соответствующей статьей Особенной части настоящего Кодекса лишение свободы предусмотрено как единственный вид наказания.

2. Лишение свободы устанавливается на срок от двух месяцев до двадцати лет.

3. Утратила силу. - Федеральный закон от 08.12.2003 N 162-ФЗ.

4. За исключением случаев, предусмотренных частью пятой настоящей статьи, при частичном или полном сложении сроков лишения свободы при назначении наказаний по совокупности преступлений максимальный срок лишения свободы не может быть более двадцати пяти лет, а по совокупности приговоров - более тридцати лет.

5. В случае совершения хотя бы одного из преступлений, предусмотренных статьями 205, 205.1, 205.2, 205.3, 205.4, 205.5, частями третьей и четвертой статьи 206, частью четвертой статьи 211, статьями 277, 278, 279, 353, 356, 357, 358, 360 и 361 настоящего Кодекса, при частичном или полном сложении сроков лишения свободы при назначении наказаний по совокупности преступлений максимальный срок лишения свободы не может быть более тридцати лет, а по совокупности приговоров - более тридцати пяти лет.

* Отягчающими обстоятельствами признаются: а) рецидив преступлений;

б) наступление тяжких последствий в результате совершения преступления;

в) совершение преступления в составе группы лиц, группы лиц по предварительному сговору, организованной группой или преступного сообщества (преступной организации);

г) особо активная роль в совершении преступления ...

Статья 57. Пожизненное лишение свободы

1. Пожизненное лишение свободы устанавливается за совершение особо тяжких преступлений, посягающих на жизнь, а также за совершение особо тяжких преступлений против здоровья населения и общественной нравственности, общественной безопасности, половой неприкосновенности несовершеннолетних, не достигших четырнадцатилетнего возраста.

2. Пожизненное лишение свободы не назначается женщинам, а также лицам, совершившим преступления в возрасте до восемнадцати лет, и мужчинам, достигшим к моменту вынесения судом приговора шестидесятипятилетнего возраста.

Статья 59. Смертная казнь

1. Смертная казнь как исключительная мера наказания может быть установлена только за особо тяжкие преступления, посягающие на жизнь.

2. Смертная казнь не назначается женщинам, а также лицам, совершившим преступления в возрасте до восемнадцати лет, и мужчинам, достигшим к моменту вынесения судом приговора шестидесятипятилетнего возраста.

2.1. Смертная казнь не назначается лицу, выданному Российской Федерации иностранным государством для уголовного преследования в соответствии с международным договором Российской Федерации или на основе принципа взаимности, если в соответствии с законодательством иностранного государства, выдавшего лицо, смертная казнь за совершенное этим лицом преступление не предусмотрена или неприменение смертной казни является условием выдачи либо смертная казнь не может быть ему назначена по иным основаниям.

3. Смертная казнь в порядке помилования может быть заменена пожизненным лишением свободы или лишением свободы на срок двадцать пять лет.

Статья 58. Назначение осужденным к лишению свободы вида исправительного учреждения

1. Отбывание лишения свободы назначается:

а) лицам, осужденным за преступления, совершенные по неосторожности, а также лицам, осужденным к лишению свободы за совершение умышленных преступлений небольшой и средней тяжести, ранее не отбывавшим лишение свободы, - в колониях-поселениях. С учетом обстоятельств совершения преступления и личности виновного суд может назначить указанным лицам отбывание наказания в исправительных колониях общего режима с указанием мотивов принятого решения;

б) мужчинам, осужденным к лишению свободы за совершение тяжких преступлений, ранее не отбывавшим лишение свободы, а также женщинам, осужденным к лишению свободы за совершение тяжких и особо тяжких преступлений, в том числе при любом виде рецидива, - в исправительных колониях общего режима;

в) мужчинам, осужденным к лишению свободы за совершение особо тяжких преступлений, ранее не отбывавшим лишение свободы, а также при рецидиве или опасном рецидиве преступлений, если осужденный ранее отбывал лишение свободы, - в исправительных колониях строгого режима;

г) мужчинам, осужденным к пожизненному лишению свободы, а также при особо опасном рецидиве преступлений - в исправительных колониях особого режима.

2. Мужчинам, осужденным к лишению свободы за совершение особо тяжких преступлений на срок свыше пяти лет, а также при особо опасном рецидиве преступлений отбывание части срока наказания может быть назначено в тюрьме, при этом суд засчитывает время содержания осужденного под стражей до вступления в законную силу обвинительного приговора в срок отбывания наказания в тюрьме.

3. Лицам, осужденным к лишению свободы, не достигшим к моменту вынесения судом приговора восемнадцатилетнего возраста, отбывание наказания назначается в воспитательных колониях.

4. Изменение вида исправительного учреждения осуществляется судом в соответствии с уголовно-исполнительным законодательством Российской Федерации.

ОСОБЕННАЯ ЧАСТЬ

Раздел VII. ПРЕСТУПЛЕНИЯ ПРОТИВ ЛИЧНОСТИ

Глава 19. Преступления против конституционных прав и свобод человека и гражданина

Статья 137. Нарушение неприкосновенности частной жизни

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

Статья 138.1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации

Статья 146. Нарушение авторских и смежных прав

Статья 147. Нарушение изобретательских и патентных прав

РАЗДЕЛ VIII. ПРЕСТУПЛЕНИЯ В СФЕРЕ ЭКОНОМИКИ

ГЛАВА 21. Преступления против собственности

Статья 159. Мошенничество

Статья 159.3. Мошенничество с использованием платежных карт

Статья 159.6. Мошенничество в сфере компьютерной информации

Глава 22. Преступления в сфере экономической деятельности

Статья 171.2. Незаконная организация и проведение азартных игр

Статья 185.3. Манипулирование рынком

Статья 185.6. Неправомерное использование инсайдерской информации

Статья 187. Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов

РАЗДЕЛ VIII. ПРЕСТУПЛЕНИЯ ПРОТИВ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ И ОБЩЕСТВЕННОГО ПОРЯДКА

Глава 25. Преступления против здоровья населения и общественной нравственности

Статья 228.1. Незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества

Статья 242. Незаконное изготовление и оборот порнографических материалов или предметов

Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних

Статья 242.2. Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов

Глава 28. Преступления в сфере компьютерной информации

Статья 272. Неправомерный доступ к компьютерной информации

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Раздел X. ПРЕСТУПЛЕНИЯ ПРОТИВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Глава 29. Преступления против основ конституционного строя и безопасности государства

Статья 280. Публичные призывы к осуществлению экстремистской деятельности

Статья 280.1. Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации

Статья 282. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства

Статья 158. Кража

1. Кража, то есть тайное хищение чужого имущества, - наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо **лишением свободы на срок до двух лет**.

2. Кража, совершенная:

а) группой лиц по предварительному сговору;

б) с незаконным проникновением в помещение либо иное хранилище;

в) с причинением значительного ущерба гражданину;

г) из одежды, сумки или другой ручной клади, находившихся при потерпевшем, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо **лишением свободы на срок до пяти лет** с ограничением свободы на срок до одного года или без такового.

Примечания. 1. Под хищением в статьях настоящего Кодекса понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.

2. Значительный ущерб гражданину в статьях настоящей главы, за исключением части пятой статьи 159, определяется с учетом его имущественного положения, но не может составлять менее пяти тысяч рублей.

...

4. Крупным размером в статьях настоящей главы, за исключением частей шестой и седьмой статьи 159, статей 159.1, 159.3, 159.5 и 159.6, признается стоимость имущества, превышающая двести пятьдесят тысяч рублей, а особо крупным - один миллион рублей.

Статья 158. Кража (продолжение)

3. Кража, совершенная:

- а) с незаконным проникновением в жилище;
- б) из нефтепровода, нефтепродуктопровода, газопровода;
- в) в крупном размере, -

наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до полутора лет или без такового, либо **лишением свободы на срок до шести лет** со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Кража, совершенная:

- а) организованной группой;
- б) в особо крупном размере, -

наказывается **лишением свободы на срок до десяти лет** со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Статья 159. Мошенничество

1. Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо **лишением свободы на срок до двух лет.**

2. Мошенничество, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо **лишением свободы на срок до пяти лет** с ограничением свободы на срок до одного года или без такового.

Статья 159. Мошенничество (продолжение)

3. Мошенничество, совершенное лицом с использованием своего служебного положения, а равно в крупном размере, -

наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо **лишением свободы на срок до шести лет** со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Мошенничество, совершенное организованной группой либо в особо крупном размере или повлекшее лишение права гражданина на жилое помещение, -

наказывается **лишением свободы на срок до десяти лет** со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Статья 159.3. Мошенничество с использованием платежных карт
(введена Федеральным законом от 29.11.2012 N 207-ФЗ)

1. Мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации, -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо **арестом на срок до четырех месяцев.**

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо **лишением свободы на срок до четырех лет** с ограничением свободы на срок до одного года или без такового.

Статья 159.3. Мошенничество с использованием платежных карт
(введена Федеральным законом от 29.11.2012 N 207-ФЗ)

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в крупном размере, -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо **лишением свободы на срок до пяти лет** со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются **лишением свободы на срок до десяти лет** со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Статья 159.6. Мошенничество в сфере компьютерной информации
(введена Федеральным законом от 29.11.2012 N 207-ФЗ)

1. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо **арестом на срок до четырех месяцев**.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо **лишением свободы на срок до четырех лет** с ограничением свободы на срок до одного года или без такового.

Статья 159.6. Мошенничество в сфере компьютерной информации (продолжение)
(введена Федеральным законом от 29.11.2012 N 207-ФЗ)

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в крупном размере, -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо **лишением свободы на срок до пяти лет** со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются **лишением свободы на срок до десяти лет** со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок **до двух лет**, либо **лишением свободы на тот же срок**.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок **до четырех лет**, либо арестом на срок до шести месяцев, либо **лишением свободы на тот же срок**.

Примечания 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации (продолжение)

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок **до пяти лет**, либо **лишением свободы** на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия* или создали угрозу их наступления, - наказываются **лишением свободы на срок до семи лет**.

*определяются следователем и судом в каждом конкретном случае. К ним могут быть отнесены гибель людей, причинение вреда их здоровью, срыв или остановка деятельности предприятия и др.

Неправомерный доступ к компьютерной информации (ст. 272)

Статья 272 УК предусматривает ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, в ЭВМ или сети ЭВМ), **если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем.**

Преступное деяние должно состоять в **неправомерном** доступе к охраняемой законом компьютерной информации..... при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

Неправомерным признается доступ к защищенной компьютерной информации лица, не обладающего правами на получение и работу с данной информацией, либо компьютерной системой.

Важным является **наличие причинной связи между** несанкционированным доступом и наступлением предусмотренных статьей 272 последствий...

Неправомерный доступ к компьютерной информации должен осуществляться *умышленно*. Совершая это преступление, лицо сознает, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность наступления указанных в законе последствий, **желает** и **сознательно** допускает их наступление либо относится к ним безразлично.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо **лишением свободы на срок до пяти лет** со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются **лишением свободы на срок до семи лет**.

Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273)

Статья предусматривает уголовную ответственность **за создание программ для ЭВМ или их модификацию, заведомо приводящие к несанкционированному уничтожению, блокированию и модификации**, либо копированию информации, нарушению работы информационных систем, а **равно использование и распространение таких программ или машинных носителей с такими программами.**

Под созданием вредоносных программ в смысле ст. 273 УК РФ понимаются программы специально разработанные для нарушения нормального функционирования компьютерных программ.

Для привлечения к ответственности по 273 ст. необязательно наступление каких-либо отрицательных последствий для владельца информации, **достаточен сам факт создания программ или внесение изменений в существующие программы**, заведомо приводящих к негативным последствиям, перечисленным в статье.

Под **использованием** программы понимается выпуск в свет, воспроизведение, распространение и иные действия по их введению в оборот.

Уголовная ответственность по этой статье возникает **уже в результате создания программы**, независимо от того использовалась эта программа или нет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами **на срок до двух лет, либо лишением свободы на тот же срок.**

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, -

наказывается принудительными работами **на срок до пяти лет либо лишением свободы на тот же срок.**

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274)

Статья 274 УК устанавливает **ответственность за нарушение правил эксплуатации** ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, **если это деяние причинило существенный вред.**

Данная уголовная норма не содержит конкретных технических требований и отсылает к ведомственным инструкциям и правилам, определяющим порядок работы, которые должны устанавливаться специально уполномоченным лицом и доводиться до пользователей.

Между фактом нарушения и наступившим существенным вредом **должна быть установлена причинная связь и полностью доказано, что наступившие последствия являются результатом именно нарушения правил эксплуатации.**

Преступник должен совершать свое деяния **умышленно**, он сознает, что нарушает правила эксплуатации, предвидит возможность или неизбежность неправомерного воздействия на информацию и причинение существенного вреда, желает или сознательно допускает причинение такого вреда или относится к его наступлению безразлично.

Статья 146. Нарушение авторских и смежных прав

1. Присвоение авторства (плагиат), если это деяние причинило крупный ущерб автору или иному правообладателю, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до одного года, либо **арестом на срок до шести месяцев**.

2. Незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере, - наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами **на срок до двух лет, либо лишением свободы на тот же срок**.

3. Деяния, предусмотренные частью второй настоящей статьи, если они совершены:

- а) утратил силу. - Федеральный закон от 08.12.2003 N 162-ФЗ;
- б) группой лиц по предварительному сговору или организованной группой;
- в) в особо крупном размере;
- г) лицом с использованием своего служебного положения, -

наказываются принудительными работами на срок до пяти лет либо **лишением свободы на срок до шести лет** со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет или без такового.

Примечание. Деяния, предусмотренные настоящей статьей, признаются совершенными в крупном размере, если стоимость экземпляров произведений или фонограмм либо стоимость прав на использование объектов авторского права и смежных прав превышают сто тысяч рублей, а в особо крупном размере - один миллион рублей.

Статья 171.2. Незаконные организация и проведение азартных игр

(введена Федеральным законом от 20.07.2011 N 250-ФЗ)

1. Организация и (или) проведение азартных игр с использованием игрового оборудования вне игорной зоны, **либо с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет"**, а также средств связи, в том числе подвижной связи, либо без полученного в установленном порядке разрешения на осуществление деятельности по организации и проведению азартных игр в игорной зоне, сопряженные с извлечением дохода в крупном размере, -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до четырех лет, либо **лишением свободы на срок до трех лет.**

2. Те же деяния:

а) сопряженные с извлечением дохода в особо крупном размере;

б) совершенные организованной группой, -

наказываются штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет либо **лишением свободы на срок до шести лет** со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет либо без такового.

Примечания. Крупным размером в статьях настоящей главы признается стоимость имущества, превышающая двести пятьдесят тысяч рублей, а особо крупным - один миллион рублей.

"Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ

Статья 242. Незаконные изготовление и оборот порнографических материалов или предметов

1. Незаконные изготовление и (или) перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование порнографических материалов или предметов -

наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо принудительными работами **на срок до двух лет, либо лишением свободы на тот же срок.**

2. Распространение, публичная демонстрация или рекламирование порнографических материалов или предметов среди несовершеннолетних либо вовлечение несовершеннолетнего в оборот порнографической продукции, совершенные лицом, достигшим восемнадцатилетнего возраста, -

наказываются **лишением свободы на срок от двух до пяти лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до десяти лет либо без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные:

а) группой лиц по предварительному сговору или организованной группой;

б) с использованием средств массовой информации, **в том числе информационно-телекоммуникационных сетей (включая сеть "Интернет");**

в) с извлечением дохода в крупном размере, -

наказываются **лишением свободы на срок от двух до шести лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пятнадцати лет либо без такового.

Примечание. Доходом в крупном размере в настоящей статье, а также в статье 242.1 настоящего Кодекса признается доход в сумме, превышающей пятьдесят тысяч рублей.

Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних

1. Изготовление, приобретение, хранение и (или) перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних -

наказываются **лишением свободы на срок от двух до восьми лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пятнадцати лет либо без такового.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные:

а) в отношении лица, не достигшего четырнадцатилетнего возраста;

б) группой лиц по предварительному сговору или организованной группой;

в) с извлечением дохода в крупном размере;

г) **с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть "Интернет")**, -

наказываются **лишением свободы на срок от трех до десяти лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пятнадцати лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Статья 242.2. Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов

(введена Федеральным законом от 29.02.2012 N 14-ФЗ)

1. Фото-, кино- или видеосъемка несовершеннолетнего в целях изготовления и (или) распространения порнографических материалов или предметов либо привлечение несовершеннолетнего в качестве исполнителя для участия в зрелищном мероприятии порнографического характера, совершенные лицом, достигшим восемнадцатилетнего возраста, -

наказываются **лишением свободы на срок от трех до десяти лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пятнадцати лет либо без такового.

2. Те же деяния, совершенные:

а) в отношении двух или более лиц;

б) группой лиц по предварительному сговору или организованной группой;

в) в отношении лица, не достигшего четырнадцатилетнего возраста;

г) **с использованием информационно-телекоммуникационных сетей (включая сеть "Интернет")**, -

наказываются **лишением свободы на срок от восьми до пятнадцати лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двадцати лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Статья 30. Приготовление к преступлению и покушение на преступление

1. Приготовлением к преступлению признаются приискание, изготовление или приспособление лицом средств или орудий совершения преступления, приискание соучастников преступления, сговор на совершение преступления либо иное умышленное создание условий для совершения преступления, если при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам.

2. Уголовная ответственность наступает за приготовление только к тяжкому и особо тяжкому преступлениям.

3. Покушением на преступление признаются умышленные действия (бездействие) лица, непосредственно направленные на совершение преступления, если при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам.

Статья 66. Назначение наказания за неоконченное преступление

1. При назначении наказания за неоконченное преступление учитываются обстоятельства, в силу которых преступление не было доведено до конца.

2. Срок или размер наказания за приготовление к преступлению не может превышать половины максимального срока или размера наиболее строгого вида наказания, предусмотренного соответствующей статьей Особенной части настоящего Кодекса за оконченное преступление.

3. Срок или размер наказания за покушение на преступление не может превышать трех четвертей максимального срока или размера наиболее строгого вида наказания, предусмотренного соответствующей статьей Особенной части настоящего Кодекса за оконченное преступление.

4. Смертная казнь и пожизненное лишение свободы за приготовление к преступлению и покушение на преступление не назначаются.

Статья 42. Исполнение приказа или распоряжения

1. Не является преступлением причинение вреда охраняемым уголовным законом интересам лицом, действующим во исполнение обязательных для него приказа или распоряжения. Уголовную ответственность за причинение такого вреда несет лицо, отдавшее незаконные приказ или распоряжение.

2. Лицо, совершившее умышленное преступление во исполнение заведомо незаконных приказа или распоряжения, несет уголовную ответственность на общих основаниях. Неисполнение заведомо незаконных приказа или распоряжения исключает уголовную ответственность.

Вопрос 2

Расследование преступлений в сфере компьютерной информации

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

ОБЪЕКТОМ преступлений, предусмотренных статьями 272 - 274 УК, являются общественные отношения в сфере охраны целостности компьютерной информации, материальных или иных интересов ее собственников.

СУБЪЕКТОМ указанных преступлений может быть вменяемое лицо, достигшее 16 лет.

Субъект ст. 274 УК - специальный, им может быть только лицо, имеющее доступ к ЭВМ, их системе или сети.

ПРЕДМЕТОМ данных преступлений является охраняемая законом информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

В тех случаях, когда компьютерная аппаратура является предметом преступлений против собственности, ее хищение, уничтожение или повреждение подлежит квалификации, соответственно, по ст.ст. 158-168 УК.

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

Неправомерность доступа - воздействие либо использование определенным лицом такой компьютерной информации, доступ к которой или внесение в нее изменений запрещен, либо ограничен действующими законами и другими нормативными актами.

Уничтожение, блокирование, модификация и копирование компьютерной информации - соответствующие действия с ней на носителе информации, произведенные командой пользователя, осуществляющего неправомерный доступ. Обязательным условием для наступления ответственности за данное деяние состоит в наличии прямой причинной связи между совершенными действиями и наступившими последствиями.

Использование своего служебного положения возможно со стороны лица, которое организует неправомерный доступ к охраняемой законом компьютерной информации, используя для этого приданные ему властные полномочия в отношении лиц, имеющих доступ к ЭВМ, системе ЭВМ или их сети (например, отдает распоряжение соответствующим работникам о внесении изменений в компьютерную информацию), т.е. он неправомерно воздействует на компьютерную информацию не сам лично, а через своих подчиненных. Использование служебного положения предполагает совершение виновным таких действий, которые находятся в пределах его служебной компетенции, однако выполняются им с нарушением установленного законом или другим нормативным актом порядка их осуществления.

Имеющим доступ к ЭВМ, системе ЭВМ или их сети будет признано лицо, в чьи служебные обязанности входит работа с данными устройствами, либо их обслуживание. По роду своих занятий эти лица могут находиться в помещении, где расположена компьютерная техника. Они могут иметь право доступа к компьютерной информации, либо не иметь такового.

Создание программ - процесс, включающий в себя разработку алгоритма, написание программы в кодах языка программирования.

Внесение изменений - любая модификация кодов программы.

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

Несанкционированное уничтожение, блокирование, модификация и копирование - соответствующие действия с информацией на ее носителе, произведенное любым другим способом, кроме как по команде пользователя.

Нарушение правил эксплуатации - невыполнение или в ненадлежащее исполнение инструкций и других документов, регламентирующих условия и правила использования, установки, обслуживания, ремонта и транспортировки средств вычислительной техники и носителей машинной информации.

Правила эксплуатации ЭВМ различных модификаций предусматриваются технической документацией на данное изделие. В соответствии с ними в каждом учреждении, использующем компьютерную технику, разрабатываются внутренние правила ее эксплуатации, которые утверждаются приказами и доводятся до сведения всех лиц, имеющих доступ к ЭВМ, системе ЭВМ или их сети.

Существенный вред и тяжкие последствия - оценочные признаки, определяются следователем и судом в каждом конкретном случае и зависят от многих показателей, относящихся к последствиям воздействия на информацию, применяемым техническим средствам, к содержанию информации, степени повреждения и т.д. В любом случае существенный вред должен быть менее значительным, чем тяжкие последствия, к которым могут быть отнесены гибель людей, причинение вреда их здоровью, срыв или остановка деятельности предприятия и др.

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

Для преступлений в сфере компьютерной информации общим предметом является именно информация. Она может храниться как на носителе информации вне ЭВМ - дискете, флэш-накопителе, лазерном компакт-диске и т.д., так и на жестком диске (винчестере) в электронно-вычислительной машине, разновидностью которой является персональный компьютер, а также в системе и сети ЭВМ на сервере (компьютере большой мощности, предназначенном для централизованного хранения и обработки информации в сети компьютеров).

Важно учитывать, что **следователь, в силу специфики своей деятельности, не может обладать достаточно глубокими знаниями и навыками специалиста в области компьютерной техники, которые требуются при исследовании механизма совершения преступления, и может совершить неисправимые ошибки в ходе обследования технической аппаратуры, снятия необходимой информации или изъятия вещественных доказательств.**

Поэтому, все эти действия необходимо выполнять в присутствии и с помощью специалиста. Участие соответствующего специалиста необходимо также и при производстве допросов, на которых выясняются технические аспекты совершенного преступления.

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

Следует отметить, что **неправомерный доступ к компьютерной информации, внесение в ЭВМ, в систему ЭВМ или их сеть вредоносных программ, нарушение правил эксплуатации ЭВМ, их системы или сети связаны прежде всего с аналогичным для всех составов этой группы проникновением, при котором преступниками совершаются практически одни и те же технические операции.**

Поэтому, среди общих обстоятельств, подлежащих установлению при расследовании указанных преступлений, **необходимо в обязательном порядке выяснить:**

1. Характеристику объекта, где совершено преступление:

- технические и конструктивные особенности помещений, связанные с установкой и эксплуатацией вычислительной техники (специальное оборудование полов, потолков и окон, каналы кабельных и вентиляционных шахт, установка и фактическое состояние устройств кондиционирования воздуха, система электропитания и иные особенности);
- особенности установки средств комплекса вычислительной техники (сосредоточены в одном месте или расположены в различных помещениях);
- связь компьютеров между собой посредством локально-вычислительной сети (ЛВС), устройств телекоммуникации и состояние линий связи;
- структура, конфигурация сети ЭВМ и внешних информационных связей;
- режим работы.

2. Состав вычислительного комплекса:

- тип, модель, тип и размер энергонезависимых носителей информации и другие характеристики компьютеров;
- наличие и типы периферийных устройств;
- состав и аппаратура организации локальной вычислительной сети;
- наличие, модель и характеристики устройств телекоммуникации;
- используемое программное обеспечение;
- использование программно-аппаратных средств защиты;

3. Организацию работы со средствами вычислительной техники.

...

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

4. Способы преодоления программной и аппаратной защиты:

- подбор ключей и паролей;
- предварительное хищение ключей и паролей;
- отключение средств защиты;
- использование несовершенства средств защиты;
- разрушение средств защиты;
- использование специальных программных средств.

5. Содержание и назначение информации, подвергшейся воздействию.

6. **Количественные и качественные характеристики информации** (объем, включая примерный объем архивной информации, возможность использовать без инсталляции (установки), ключевых дискет и аппаратных ключей-паролей, способ шифрования).

Кроме того, подлежат выяснению обстоятельства, характерные для того или иного вида преступлений данной категории. К таким обстоятельствам относятся:

- режим и фактическое состояние охраны;
- наличие и техническая характеристика охранной сигнализации, вид охранной техники;
- технические средства, использованные при совершении преступления;
- режим доступа к средствам вычислительной техники;
- разграничение доступа к средствам вычислительной техники и машинным носителям;
- организация доступа к ресурсам ЭВМ, сети ЭВМ (в т.ч. по устройствам телекоммуникации), к кодам, паролям и другой идентифицирующей информации;
- организация противовирусной защиты;
- наличие разработанных правил эксплуатации ЭВМ и документации об ознакомлении с ними.

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

ОСМОТР МЕСТА ПРОИСШЕСТВИЯ

2.1. Подготовка к осмотру места происшествия.

При осмотре места происшествия следователь обязательно должен использовать помощь незаинтересованных специалистов в области установки и функционирования средств электронно-вычислительной техники, программирования, а также специалиста-криминалиста.

Прежде чем приступить к осмотру места происшествия, следователь и участники следственно-оперативной группы должны знать и соблюдать общие правила обращения с вычислительной техникой и носителями информации. Несоблюдение этих правил может привести к потере важной для расследования информации и нанесению материального ущерба, вызванного этими действиями.

2.1.1. Общие правила обращения с вычислительной техникой и носителями информации.

2.1.1.1. Все включения (выключения) компьютеров и других технических средств производятся только специалистом или под его руководством;

2.1.1.2. Применение средств криминалистической техники - магнитных искателей, ультрафиолетового осветителя, инфракрасного преобразователя, во избежание разрушения носителей информации и микросхем памяти ЭВМ, должно быть согласовано со специалистом;

2.1.1.3. Исключение попадания мелких частиц и порошков на рабочие части компьютеров (разъемы, дисковод, вентилятор и др.);

2.1.1.4. При работе с магнитными носителями информации запрещается прикасаться руками к рабочей поверхности дисков, подвергать их электромагнитному воздействию, сгибать, хранить без специальных конвертов (пакетов, коробок);

2.1.1.5. Диапазон допустимых температур при хранении и транспортировке должен варьироваться в температурных пределах от 0 до +50 градусов Цельсия;

2.1.1.6. Со всеми непонятными вопросами, затрагивающими терминологию, устройство и функционирование вычислительной техники необходимо обращаться только к специалисту.

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

ОСМОТР МЕСТА ПРОИСШЕСТВИЯ (продолжение)

2.2. Производство осмотра места происшествия.

Осмотр места происшествия следует начать с **запрещения доступа к средствам вычислительной техники всем лицам, работающим на объекте.**

Принять меры к выявлению и изъятию следов рук, оставшихся на защелках дисководов, кнопках включения питания, участках корпуса около винтов крепления крышки корпуса, клавишах клавиатуры и мыши, разъемах портов и сетевых плат, а также на кнопках печатных устройств. Кроме того, нельзя исключать возможности доступа в помещение, где находится компьютерная техника и информация посторонними лицами путем взлома, подбора ключей, в т.ч. паролей к электронным замкам, на которых также могут остаться следы. При осмотре кабельных соединений ЛВС требуется убедиться в их целостности, отсутствии следов подключения нештатной аппаратуры.

В связи с возможностью совершения преступлений по сетям телекоммуникации и ЛВС необходимо **установить и зафиксировать в протоколе осмотра расположение** всех компьютеров в сети, назначение каждого компьютера, наличие сервера, места прокладки кабелей, устройств телекоммуникации, их расположение и подключение к каналам телефонной связи. Требуется также **выяснить наличие специальных средств защиты от несанкционированного доступа к информации, принять меры к установлению ключей (паролей).**

При непосредственном осмотре средств вычислительной техники необходимо отразить их размещение в помещении, предназначение, название (обычно на лицевой стороне), серийный номер, комплектацию (наличие и тип дисководов, сетевых карт и др.), наличие и тип подключенных периферийных устройств, наличие соединения с ЛВС и (или) сетями телекоммуникации, состояние устройств (целое или со следами вскрытия).

Описывая внешнее состояние вычислительной техники, нужно обращать внимание на места подключения (например, соединительный кабель между коммуникационными портами принтера и системным блоком компьютера) периферийных устройств, винты крепления крышек корпуса, поверхности под системным блоком, монитором и другими устройствами. Обычно в этих местах происходит скопление пыли, а значит могут остаться следы, характер или отсутствие которых должно быть отражено в протоколе. Также, должны быть отмечены наличие и состояние всех пометок, пломб, специальных знаков и наклеек (инвентарных номеров, записей на память, контрольных маркеров фирм-продавцов и др.), нанесенных на корпуса и устройства компьютеров, наличие загрязнений, механических повреждений и их локализация.

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

2.2. Производство осмотра места происшествия (продолжение)

При осмотре средств электронно-вычислительной техники рекомендуется независимо от того, включен компьютер или нет, **описать в протоколе положение всех переключателей на всех блоках и устройствах**. При наличии включенной техники зафиксировать в протоколе осмотра состояние индикаторных ламп (включены или нет, каким цветом горят, мигают и с какой частотой), а также информацию, высвечиваемую на всевозможных индикаторах и табло. **Описать информацию, высвечиваемую на мониторе**, при этом необходимо учитывать, что для предотвращения выгорания экрана в большинстве компьютеров используют специальные заставки - хранители экрана, которые могут быть защищены паролем. В протоколе также должен быть зафиксирован вид этого хранителя. В дополнение к протоколу, кроме составления схемы расположения компьютеров и периферийных устройств в помещении и соединения компьютеров в сети, с помощью видео- или фотосъемки рекомендуется зафиксировать информацию на экране монитора, индикаторных панелях, положение переключателей и состояние индикаторных ламп всех устройств компьютерной системы, о чем сделать соответствующие записи в протоколе.

Перед выключением питания требуется корректно завершить все исполняемые в данный момент программы, по возможности сохранить всю промежуточную информацию (тексты, информацию состояния, содержание буферов обмена и др.) в специальных файлах, если возможно - на отдельных дискетах, в противном случае на жестком диске компьютера. **В протоколе указать имена этих файлов, вид информации, сохраняемой в каждом, расположение файлов** (наименование дискет и их маркировку или логический диск и каталог на винчестере компьютера); **выключить компьютер, который подвергся воздействию, а при наличии сети требуется выключить все компьютеры в сети**. Если из-за особенностей функционирования системы это невозможно, то следует принять все меры для исключения доступа к информации данного компьютера, по возможности снять с нее копию и принять меры для фиксации всех изменений информации, которые будут происходить впоследствии.

В ходе осмотра внутреннего устройства компьютера необходимо **с помощью специалиста установить наличие внутри компьютера нештатной аппаратуры, следов противодействия аппаратной системы защиты** - разрушение или временное изъятие микросхем, отключение внутреннего источника питания (аккумулятора).

При осмотре места происшествия, также следует **обращать особое внимание на записи, относящиеся к работе компьютерной техники**. В них могут оказаться сведения о процедурах входа-выхода с компьютерной системой, пароли доступа и т.п.

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

2.3. Особенности производства некоторых следственных действий.

При производстве следственных или иных действий, в процессе которых изымаются объекты для производства экспертных исследований, необходимо **принять все возможные меры для исключения возможной порчи или уничтожения хранящейся в компьютерах информации. Включать и выключать компьютеры, производить с ними какие-либо манипуляции может только специалист в области вычислительной техники, участвующий в производстве данного следственного действия.**

Поскольку результаты проводимых экспертных исследований, особенно экспертизы программного обеспечения, напрямую зависят от сохранности информации на внутренних и внешних магнитных носителях, необходимо **изъять все образующие ее устройства, независимо от их принадлежности** (личная собственность, собственность данного учреждения, и др.). При изъятии, **для исключения возможности доступа к компьютерной информации, разукрупнения и физического повреждения основных рабочих элементов, рекомендуется поместить средства вычислительной техники в специальную упаковку** (картонные или деревянные коробки, полиэтиленовые пакеты и др.), которые **заклеиваются и опечатываются.**

Если изъятие всего устройства невозможно или нецелесообразно, следует изъять установленный в нем носитель (носители) информации.

При невозможности изъятия носителей информации, **требуется принять меры к исключению доступа к ним заинтересованных лиц.** Идеальным средством обеспечения сохранности вычислительной техники является исключение доступа в помещение, в котором она установлена, с одновременным отключением источников электропитания. **Если последнее не представляется возможным (компьютер является сервером или рабочей станцией в сети), с помощью специалиста создаются условия только для приема информации. В этом случае опечатываются все необходимые узлы, детали, части и механизмы компьютерной системы. Компьютеры и их комплектующие опечатываются путем наклеивания на разъемы листа бумаги и закрепления его краев на боковых стенках компьютера клеем или клейкой лентой, чтобы исключить возможность работы с ними в отсутствие владельца или эксперта. Магнитные носители упаковываются, хранятся и перевозятся в специальных экранированных контейнерах или стандартных футлярах, исключающих разрушающее воздействие ударов, различных электромагнитных и магнитных полей и наводок, направленных излучений. Пояснительные надписи могут делаться на отдельном листе, который вкладывается в коробку.**

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

2.3. Особенности производства некоторых следственных действий (продолжение)

Недопустимо приклеивать что-либо непосредственно к магнитным носителям, пропускать через них бечеву, пробивать отверстия, наносить подписи, пометки, печати, прикасаться пальцами или любым предметом к рабочей поверхности носителей, разбирать корпуса винчестеров, дискет, сгибать носители, изменять состояние переключателей, подносить близко к источникам электромагнитного излучения, сильным осветительным и нагревательным приборам, подвергать воздействию воды и влаги.

Если на объекте было отключено электроснабжение, например, в связи с пожаром или взрывом, то до его включения следует проверить находятся ли все компьютеры и периферийные устройства в отключенном состоянии. Участие специалиста при производстве следственных действий в данном случае необходимо и потому, что для сокрытия информации на компьютерах могут быть установлены специальные защитные программы, которые при определенных условиях автоматически производят полное или частичное стирание информации.

Транспортировка и хранение компьютерной техники и информации должны осуществляться в условиях, исключающих ее повреждение, в том числе в результате воздействия металлодетекторов, используемых для проверки багажа в аэропортах. Хранят компьютеры и их комплектующие в сухом, отапливаемом помещении. Следует удостовериться, что в нем нет грызунов, которые часто являются причиной неисправности аппаратуры.

Учитывая нестандартность обстановки, в которой может производиться осмотр места происшествия, **вопрос о возможности изъятия компьютерной техники и информации, способе упаковки, транспортировки и хранения изъятых объектов решается следователем в каждом конкретном случае совместно со специалистом.** Процессуальный порядок изъятия объектов определяется общими требованиями Уголовно-процессуального кодекса Российской Федерации. В качестве понятых при производстве следственных действий рекомендуется привлекать лиц, обладающих специальными познаниями в области компьютерной техники и информатики.

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

3. СЛЕДСТВЕННЫЕ ВЕРСИИ

При выдвижении версий совершения преступлений в сфере компьютерной информации необходимо учитывать, что они совершаются обычно группой из 2 и более человек, хотя не исключена возможность работы преступника - одиночки. В таком случае он сам или, если действует группа, один из ее членов, является либо сотрудником данного учреждения, либо имеет свободный доступ к компьютерам (представитель службы технической или программной поддержки, программист работающий по контракту и т.д.), умеет работать с вычислительной техникой, хорошо представляет, какая информация и где расположена в компьютере. Интерес обычно представляет информация, содержащая государственную или коммерческую тайну.

В основном, как правило, информация преступниками копируется на магнитный носитель, хотя не исключена возможность передачи ее по сетям телекоммуникации, распечатки на бумаге, фото-, видеосъемки изображения экрана и действий оператора или перехват с помощью специальных технических средств. Копирование может осуществляться как на портативный компьютер (Notebook) с подключением его к локальной вычислительной сети, так и непосредственно к последовательному или параллельному порту конкретной ЭВМ с помощью специального кабеля.

Преступление обычно происходит в рабочее время и внешне не отличается от обычной работы в учреждении. Похищенная информация используется в дальнейшем самими преступниками для подготовки хищений или может быть продана заинтересованным лицам.

Учитывая конкретные обстоятельства, следователем могут быть выдвинуты и проверены следующие общие версии:

3.1. Преступление совершено сотрудником данного учреждения, либо лицом, имеющим свободный доступ к компьютерной технике.

3.2. Преступление совершено сторонним лицом, входящим в круг родственников, друзей, знакомых сотрудников учреждений.

3.3. Преступление совершено группой лиц по предварительномуговору или организованной группой с участием сотрудника данного учреждения, либо лица имеющего свободный доступ к компьютерной технике и в совершенстве владеющего навыками работы с ней.

3.4. Преступление совершено лицом или группой лиц, не связанных с деятельностью учреждения и не представляющих ценность компьютерной информации.

4. Компьютерно-техническая экспертиза

4.1. Объекты компьютерно-технической экспертизы.

4.1.1. Компьютеры в сборке, их системные блоки;

4.1.2. **Периферийные устройства** (дисплеи, принтеры, дисководы, модемы, клавиатура, сканеры, манипуляторы и пр.), **коммуникационные устройства компьютеров и вычислительных сетей**;

4.1.3. **Магнитные носители информации** (жесткие и флоппи-диски, оптические диски и др.);

4.1.4. Словари поисковых признаков систем (тезаурусы), классификаторы и иная **техническая документация**, например, технические задания и отчеты;

4.1.5. Электронные записные книжки, телефонные аппараты с памятью номеров, иные **электронные носители текстовой или цифровой информации, техническая документация к ним.**

В системе Министерства внутренних дел в настоящее время существуют специальные экспертные подразделения, которые производят компьютерно-технические экспертизы носителей машинной информации, программного обеспечения, баз данных и аппаратного обеспечения ЭВМ (лаборатории компьютерно-технических экспертиз при региональных экспертно-криминалистических центрах). Кроме того, для производства этого вида экспертиз можно привлекать специалистов учебных и научно-исследовательских заведений, не относящихся к системе МВД России, фирм и организаций, занимающихся разработкой программного и аппаратного обеспечения для компьютеров, их эксплуатацией и ремонтом. Данный вид экспертиз может быть поручен специалистам в области эксплуатации ЭВМ (системным программистам, инженерам по обслуживанию, работающим с данного вида носителями и др.) и программистам, соответствующей квалификации.

При вынесении постановления о назначении компьютерно-технической экспертизы следователем, в постановлении о ее назначении, обязательно указываются серийный номер компьютера и его индивидуальные признаки (конфигурация, цвет, надписи на корпусе и т.д.).

Учитывая, что **компьютерно-техническая экспертиза - новый формирующийся род судебных экспертиз, необходимость в которых обуславливается широким внедрением компьютерных технологий во все сферы человеческой деятельности полезно дать краткую характеристику ее возможностей.**

В настоящее время в рамках этого рода экспертиз выделяются два вида:

- **техническая экспертиза компьютеров и их комплектующих**, которая проводится в целях изучения конструктивных особенностей и состояния компьютера, его периферийных устройств, магнитных носителей и пр., компьютерных сетей, а также причин возникновения сбоев в работе вышеуказанного оборудования;

- **экспертиза данных и программного обеспечения**, осуществляемая в целях изучения информации, хранящейся в компьютере и на магнитных носителях.

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

4.2. Вопросы, разрешаемые технической экспертизой компьютеров и их комплектующих (диагностические).

4.2.1. Компьютер какой модели представлен на исследование? Каковы технические характеристики его системного блока и периферийных устройств? Каковы технические характеристики данной вычислительной сети?

4.2.2. Где и когда изготовлен и собран данный компьютер и его комплектующие? Осуществлялась ли сборка компьютера в заводских условиях или кустарно?

4.2.3. Соответствует ли внутреннее устройство компьютера и периферии прилагаемой технической документации? Не внесены ли в конструкцию компьютера изменения (например, установка дополнительных встроенных устройств: жестких дисков, устройств для расширения оперативной памяти, считывания оптических дисков и пр., иные изменения конфигурации)?

4.2.4. Исправен ли компьютер и его комплектующие? Каков их износ? Каковы причины неисправности компьютера и периферийных устройств? Не содержат ли физических дефектов магнитные носители информации?

4.2.5. Не производилась ли адаптация компьютера для работы с ним специфических пользователей (левша, слабовидящий и пр.)?

4.2.6. Каковы технические характеристики иных электронных средств приема, накопления и выдачи информации? Исправны ли эти средства? Каковы причины неисправностей?

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

4.3. Диагностические вопросы, разрешаемые экспертизой данных и программного обеспечения

4.3.1. Какая операционная система использована в компьютере?

4.3.2. Каково содержание информации, хранящейся на внутренних и внешних магнитных носителях, в том числе какие программные продукты там находятся? Каково назначение программных продуктов? Каков алгоритм их функционирования, способа ввода и вывода информации? Какое время проходит с момента введения данных до вывода результатов при работе данной компьютерной программы, базы данных?

4.3.3. Являются ли данные программные продукты лицензионными (или несанкционированными) копиями стандартных систем или оригинальными разработками?

4.3.4. Не вносились ли в программы данного системного продукта какие-либо коррективы (какие), изменяющие выполнение некоторых операций (каких)?

4.3.5. Соответствует ли данный оригинальный компьютерный продукт техническому заданию? Обеспечивается ли при его работе выполнение всех предусмотренных функций?

4.3.6. Использовались ли для ограничения доступа к информации пароли, скрытые файлы, программы защиты и пр.? Каково содержание скрытой информации? Не предпринимались ли попытки подбора паролей, взлома защитных средств и иные попытки несанкционированного доступа?

4.3.7. Возможно ли восстановление стертых файлов? Возможно ли восстановление дефектных магнитных носителей информации? Каково содержание восстановленных файлов?

4.3.8. Каков механизм утечки информации из локальных вычислительных сетей, глобальных сетей и распределенных баз данных?

4.3.9. Имеются ли сбои в функционировании компьютера, работе отдельных программ? Каковы причины этих сбоев? Не вызваны ли сбои в работе компьютера влиянием вируса (какого)? Распространяется ли негативное влияние вируса на большинство программ или он действует только на определенные программы? Возможно ли восстановить в полном объеме функционирование данной программы (текстового файла), поврежденного вирусом?

4.3.10. Каково содержание информации, хранящейся на пейджере, в электронной записной книжке и пр? Имеется ли в книжке скрытая информация и каково ее содержание?

4.3.11. Когда производилась последняя корректировка данного файла или инсталляция данного программного продукта?

4.3.12. Каков был уровень профессиональной подготовки в области программирования и работы с компьютерной техникой лица, произведшего данные действия с компьютером и программным обеспечением?

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

4.4. Вопросы идентификационного характера, разрешаемые компьютерно-технической экспертизой.

4.4.1. Имеют ли комплектующие компьютера (печатные платы, магнитные носители, дисководы и пр.) единый источник происхождения?

4.4.2. Не написана ли данная компьютерная программа определенным лицом (решается комплексно при производстве компьютерно-технической и автороведческой экспертиз)?

Кроме приведенного выше перечня вопросов, разрешаемых компьютерно-технической экспертизой, для использования на практике, в зависимости от объекта исследования и конкретной обстановки, можно привести дополнительные примеры, расширяющие перечень вопросов, подлежащих выяснению при исследовании таких объектов, как носители информации, программное обеспечение, базы данных и аппаратное обеспечение ЭВМ.

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

4.5. Перечень вопросов, разрешаемых при исследовании носителей машинной информации.

- 4.5.1. Каков тип носителя, его технические характеристики (на каких типах ЭВМ может быть использован, максимально-допустимая емкость записи и пр.)?
- 4.5.2. Имеет ли носитель механические повреждения?
- 4.5.3. Как размечен носитель, в каком формате информация записана на него?
- 4.5.4. Какая информация записана на данный носитель?
- 4.5.5. Как информация физически размещена на носителе (для лент последовательность записи, для дисков сектора, дорожки, цилиндры и пр.)?
- 4.5.6. Как информация размещена логически на носителе (файлы, каталоги, логические диски)?
- 4.5.7. Имеются ли повреждения информации (плохие сектора, потерянные блоки и пр.)?
- 4.5.8. Возможна ли коррекция информации на носителе?
- 4.5.9. Имеется ли на носителе компьютерный вирус, если да, то какой, какие изменения вносит и возможна ли его нейтрализация без ущерба для информации?
- 4.5.10. Являются ли изменения на носителе результатом действия вируса?
- 4.5.11. Возможно ли копирование информации с данного носителя и возможно ли физическое копирование носителя в целом?
- 4.5.12. При повреждении носителя, возможно ли восстановление информации?
- 4.5.13. Какая информация ранее была записана на данный носитель (отмечена как стертые файлы) и возможно ли ее восстановление?
- 4.5.14. Какой объем занимает вся информация на носителе, ее отдельные части и сколько имеется свободного места?
- 4.5.15. Какое время занимает копирование данной информации с учетом типа ЭВМ?
- 4.5.16. Требуются ли для работы с информацией на носителе специальные аппаратные или программные средства дешифрации и перекодировки?
- 4.5.17. Нет ли на носителе специальных программ, уничтожающих информацию в случае несанкционированного доступа, отсутствия ключей и паролей или использования на другом компьютере, стоит ли счетчик возможных инсталляций и другие средства защиты, возможен ли их обход и каким образом?

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

4.6. Перечень вопросов, разрешаемых при исследовании программного обеспечения (ПО)

Под ПО (программами для ЭВМ) понимается совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата.

ПО обычно хранится на магнитных, оптических или электронных (непосредственно установлено в микросхемах памяти компьютера) носителях машинной информации и управляет работой вычислительной системы. Вся информация, относящаяся к ПО, независимо от носителя, является объектом экспертизы и должна быть представлена эксперту.

4.6.1. Каково назначение данного ПО?

4.6.2. Кто разработчик данного ПО?

4.6.3. Каким образом данное ПО распространяется, кто является владельцем данной копии, имеется ли лицензия или разрешение на использование данного продукта. Каков серийный номер данной копии ПО?

4.6.4. С какими входными и выходными данными оно работает, каким образом и в какой форме эти данные вводятся в ЭВМ, создаются ли (а если создаются, то где) временные файлы и файлы статистики и их содержание, в какой форме выдается, где хранится или куда передается выходная информация?

4.6.5. Требуется ли ПО при своей работе ввода паролей и наличия ключей. Если требуется, то каким образом они хранятся и кодируются, имеется ли возможность прочитать файл с паролем с помощью простейших редакторов?

4.6.6. Возможен ли обход паролей при запуске программы через отладчик?

4.6.7. Имеются ли на машинном носителе исходные коды программ на языке программирования?

4.6.8. Когда последний раз вносились изменения в ПО (например по дате и времени создания или внесения изменений в файлы)?

4.6.9. Имеются ли в программе изменения по сравнению с исходной версией, что было изменено, к каким последствиям данные изменения приводят?

4.6.10. Имеются ли в программе враждебные функции, которые влекут уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ - или их сети. Каким образом эти функции осуществляются и к каким последствиям приводят?

4.6.11. Возможно ли самопроизвольное распространение данной программы, т.е. является ли данная программа компьютерным вирусом?

4.6.12. Возможно ли осуществление копирования информации или требуется инсталляция?

4.6.13. Были ли внесены в программу изменения, направленные на преодоление защиты?

4.6.14. Количественные (занимаемый объем, количество файлов и пр.) и качественные (назначение конкретных файлов, требование к оборудованию и пр.) характеристики программы?

4.6.15. Соответствие алгоритма работы конкретной программы требованиям, указанным в ТЗ или ИЭ.

4.6.16. Имеются ли ошибки при проведении расчетов с помощью данной программы (правильно ли происходит округление чисел, правильный ли алгоритм расчета конкретных данных и пр.?)

4.6.17. Имеется ли полная совместимость конкретного ПО с другими программами выполняемыми на данном компьютере, если нет, то каким образом это влияет на нормальное функционирование системы?

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

4.7. Перечень вопросов, разрешаемых при исследовании баз данных.

Под базами данных понимается форма представления и организации совокупности данных (статей, расчетов и т.д.), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ. С точки зрения организации базы данных могут представлять собой информацию в текстовых файлах и информацию в файлах со специальной структурой, которые обрабатываются специальными программами (системами управления базами данных, сокращенно СУБД), именно их в компьютерной терминологии называют базами данных.

Базы данных обычно хранятся на магнитных, оптических или электронных, непосредственно установлены в микросхемах памяти компьютера, носителях машинной информации. Кроме того, коды баз данных, входные, выходные и промежуточные данные могут находиться на бумажном носителе (распечатки исходных текстов программ баз данных, перфолента, перфокарта). Вся информация, относящаяся к базам данных, независимо от формы носителя, является объектом экспертизы и должна быть представлена эксперту.

4.7.1. Каким образом организована база данных?

4.7.2. В каком формате записана информация и какие СУБД могут ее обрабатывать?

4.7.3. Какая информация записана в данной базе?

4.7.4. Информация в базе записана обычным образом или закодирована?

4.7.5. Когда последний раз обновлялась информация?

4.7.6. Имеются ли в данной базе скрытые (помеченные для удаления) поля и их содержание?

4.7.7. Имеются ли повреждения или изменения в записях базы по сравнению с эталоном или резервной копией, если да, то какие?

4.7.8. Сколько записей в базе?

4.7.9. Имеется ли в данной базе запись конкретного содержания?

4.7.10. Возможно ли внести изменение в данную базу с помощью простейших программных средств (например, текстовых редакторов и пр.)?

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

4.8. Перечень вопросов, разрешаемых при исследовании аппаратного обеспечения ЭВМ

Под аппаратным обеспечением ЭВМ понимается комплекс технических средств, предназначенных для автоматизированной обработки информации, обеспечения хранения и передачи ее по каналам связи, ведения диалога с пользователем и выполнения других функций в составе компьютерной системы.

Аппаратное обеспечение в свою очередь подразделяется на:

1. Центральные устройства ЭВМ (центральный процессор; оперативное и постоянное запоминающие устройства; системную шину; другие устройства для обеспечения работы вычислительной системы - контроллеры, таймер, тактовый генератор, различные буферы и пр.).

2. Периферийные устройства (видеоподсистема; накопители различных типов; устройства вывода информации; устройства ввода информации; устройства организации ЛВС и телекоммуникации; другие устройства, сопряженные с компьютером и которые функционируют под его управлением).

3. Вспомогательные устройства (устройства электропитания; сетевые фильтры; аппаратура защиты, работающая автономно от центрального процессора - генераторы помех и пр.).

4.8.1. Каковы тип устройства и его технические характеристики?

4.8.2. Исправно ли данное устройство или нет, тип неисправности (отказ или сбой), как она влияет на работу системы в целом?

4.8.3. Полностью ли совместимы между собой компоненты данного устройства, если нет, то как это сказывается на его работе?

4.8.4. Полностью ли совместимо данное устройство с каким либо конкретным устройством, если нет то как сказывается это на их работе?

...

Расследование преступлений в сфере компьютерной информации (методические рекомендации)

4.8. Перечень вопросов, разрешаемых при исследовании аппаратного обеспечения ЭВМ (продолжение)

4.8.5. Имеются ли на устройстве следы ремонта, повреждений, демонтажа микросхем, замены блоков?

4.8.6. Соответствует ли комплектация устройства технической документации, если нет, то какие компоненты были изменены, демонтированы?

4.8.7. Нет ли в данном устройстве дополнительных блоков (жучков) с враждебными функциями, если есть, то их предназначение?

4.8.8. Возможно ли на данном оборудовании решать какие либо конкретные задачи?

4.8.9. Какой уровень излучений у данного устройства, возможен ли его прием специальными техническими средствами для последующей расшифровки информации, если возможен, то на каком расстоянии?

4.8.10. Возможно ли отключение аппаратных средств защиты и как это влияет на работу системы?

4.8.11. Соблюдались ли правила эксплуатации?

4.8.12. Могла ли данная проблема возникнуть в результате несоблюдения правил технической эксплуатации?

Вопрос 3

**Правоприменительная практика в области
противодействия преступлениям
в сфере компьютерной информации**

В Белгородской области вынесен приговор за преступления, совершенное в сети Интернет

26 августа 2010 года, 18:00

Собранные следственными органами Следственного комитета по Белгородской области доказательства признаны судом достаточными для вынесения приговора 19-летнему жителю города Белгорода Сергею Бондаренко. Он признан виновным в совершении преступлений, предусмотренных **ч.1 ст.273, ч.1 ст.137, ч.2 ст.129 УК РФ** (использование и распространение вредоносных программ для ЭВМ, заведомо приводящих к несанкционированному копированию информации, нарушение неприкосновенности частной жизни, клевета, содержащаяся в публичном выступлении).

Следствием и судом установлено, что Бондаренко, используя компьютер, подключенный к сети Интернет, осуществлял выходы в социальные сети «Мой мир» и «В контакте». С помощью вредоносной программы злоумышленник получил несанкционированный доступ к личной информации ранее знакомой ему девушки и скопировал ее. От имени девушки он создал страничку в социальной сети «В контакте», используя без ее ведома фотографии, имя, фамилию, сведения о месте рождения, семейном положении и месте учебы. Испытывая к девушке неприязненные отношения и желая унижить ее, Бондаренко распространил в сети сведения о частной жизни и заведомо ложную информацию об интимных предпочтениях потерпевшей. Затем молодой человек путем незаконного доступа заблокировал доступ девушки к своей страничке на сайте «Мой мир» путем смены пароля и от ее имени в течение почти четырех месяцев рассылал различных абонентам предложения интимного характера.

Уголовное дело рассмотрено судом в особом порядке при полном признании Бондаренко своей вины в совершении инкриминируемых деяний. Приговором суда ему назначено наказание в виде 240 часов обязательных работ.

В Кировской области студент университета признан судом виновным в нарушении авторского права и использовании вредоносных компьютерных программ

23 июля 2010 года, 14:20

Собранные следственными органами Следственного комитета по Кировской области доказательства признаны судом достаточными для вынесения обвинительного приговора 20-летнему Руслану Сарыеву. Он признан виновным в совершении преступлений, предусмотренных **ч. 2 ст. 146 УК РФ** (нарушение авторских прав), **ч. 1 ст. 272 УК РФ** (неправомерный доступ к компьютерной информации) и **ч. 1 ст. 273 УК РФ** (использование вредоносных программ для ЭВМ).

Следствием и судом установлено, что в марте 2010 года Сарыев незаконно установил заведомо контрафактные компьютерные программы на персональный компьютер физического лица. В результате незаконного использования объектов авторского права правообладателю был причинён материальный ущерб на общую сумму более 130 тысяч рублей. Кроме того, он осуществил модификацию системной информации, нейтрализовав установленные правообладателем средства индивидуальной защиты лицензионного программного обеспечения, что позволило запускать контрафактное программное обеспечение без ввода установленного правообладателем кода. Он же в марте 2010 года использовал вредоносную программу для ЭВМ, предназначенную для взлома системы защиты программного обеспечения и последующего его запуска без разрешения правообладателя.

Суд приговорил Сарыева к наказанию в виде исправительных работ сроком на ~~8~~250 часов.

Житель Пермского края осужден за незаконное использование объектов авторского права в целях сбыта в крупном размере

28 мая 2010 года, 12:00

Собранные Пермским межрайонным следственным отделом Уральского следственного управления на транспорте Следственного комитета доказательства признаны судом достаточными для вынесения приговора в отношении жителя Пермского края Сергея Зверева. Он признан виновным в совершении преступлений, предусмотренных **ч. 2 ст. 146 УК РФ** (незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений в целях сбыта, совершенные в крупном размере) и **ч. 1 ст. 273 УК РФ** (создание, использование и распространение вредоносных программ для ЭВМ).

Следствием и судом установлено, что 10 февраля 2010 года **при проведении оперативного эксперимента сотрудниками отдела "К" ГУВД по Пермскому краю совместно с сотрудниками следственных органов Уральского следственного управления на транспорте** в одном из офисов города Перми Зверев незаконно сбыл контрафактный экземпляр компьютерной программы "1С Предприятие версия 7.7 Комплексная сетевая" без разрешения на это законного правообладателя. Стоимость реализованного экземпляра оценена правообладателем на сумму более 100 тысяч рублей.

Приговором суда подсудимому назначено наказание в виде 1,5 лет лишения свободы условно с выплатой штрафа в доход государства.

Житель Пермского края осужден за незаконное использование объектов авторского права в целях сбыта в крупном размере

25 мая 2010 года, 17:28

Собранные Пермским межрайонным следственным отделом Уральского следственного управления на транспорте Следственного комитета доказательства признаны судом достаточными для вынесения приговора в отношении жителя Пермского края Михаила Днистряна. Он признан виновным в совершении преступлений, предусмотренных **ч. 2 ст. 146 УК РФ** (незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений в целях сбыта, совершенные в крупном размере) и **ч. 1 ст. 273 УК РФ** (создание, использование и распространение вредоносных программ для ЭВМ).

Следствием и судом установлено, что в декабре 2009 года в **ходе проведения оперативного эксперимента** Днистрян совершил незаконный сбыт контрафактного экземпляра компьютерной программы "КонсультантПлюс" без разрешения на это законного правообладателя. Стоимость реализованного экземпляра оценена правообладателем на сумму более 100 тысяч рублей.

Приговором суда города Березники Пермского края Днистряну назначено наказание в виде 6 месяцев лишения свободы условно с выплатой штрафа в доход государства.

В Калининградской области бывший военнослужащий осужден за незаконное распространение сведений о частной жизни и порнографических материалов

25 декабря 2012 года, 11:32

Собранные военным следственным отделом Следственного комитета Российской Федерации по Калининградскому гарнизону доказательства признаны судом достаточными для вынесения приговора бывшему военнослужащему по контракту войсковой части 30866 старшему матросу запаса Тимуру Бизунову. Он признан виновным в совершении двух преступлений, предусмотренных **ч. 1 ст. 137 УК РФ** (незаконное соби́рание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации), **ст. 242 УК РФ** (незаконное распространение порнографических материалов или предметов), **ч. 1 ст. 272 УК РФ** (неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации).

Следствием и судом установлено, что 3 февраля 2011 года Бизунов, желая отомстить своей девушке за прекращение с ним отношений, создал в службе знакомств ЗАО «Мамба» анкету от ее имени и разместил 38 фотографий, в том числе и интимного характера, а на своей странице в социальной сети «В контакте» выложил видеозапись порнографического содержания с ее участием. Кроме того, 12 февраля 2011 года совершил неправомерный доступ к ее электронному почтовому ящику и изменил пароль доступа к нему.

Приговором Калининградского гарнизонного военного суда Тимуру Бизунову назначено наказание в виде штрафа в размере 110 тысяч рублей.

Предотвращено распространение вредоносного программного обеспечения для хищения денег с банковских счетов

22 Апреля 2014 14:31

Сотрудниками **Управления «К» МВД России** пресечена деятельность по созданию и распространению вредоносных программ, предназначенных для скрытого копирования реквизитов доступа к банковским счетам граждан и различных организаций. Предотвращено хищение около 1 млрд. рублей.

В Управление «К» поступила информация о том, что на сайтах ведущих банков Российской Федерации происходит размещение вредоносного программного обеспечения. Было установлено, что вредоносная программа копирует персональные данные клиентов, с помощью которых потом похищались денежные средства со счетов клиентов.

В ходе оперативно-розыскных мероприятий было установлено, что злоумышленником является 42-летний программист из Тольятти Александр Пакичев. Зарегистрировавшись под псевдонимом «Хамелеон» на нескольких сайтах по компьютерной тематике он разместил объявление о разработке вредоносного программного обеспечения.

Для взлома сайтов каждого из банков злоумышленник создавал персональные вредоносные программы, которые продавал впоследствии заказчикам в среднем за 9 тыс. рублей. За два года злоумышленник написал более 10 таких программ.

Оперативники выяснили, что в результате противоправной деятельности Пакичева его сообщникам удалось получить персональные данные нескольких десятков тысяч клиентов российских банков, на счетах которых, по предварительным данным, в общей сложности находилось около 1 млрд. рублей.

При обыске по месту жительства Пакичева была обнаружена и изъята компьютерная техника, исследование которой подтвердило его причастность к совершению данного преступления.

Возбужденное по **ст. 273 УК РФ** (создание, использование и распространение вредоносных программ) уголовное дело рассмотрено судом. Пакичев приговорен к 1 году лишения свободы условно со штрафом в 100 тысяч рублей.

В МУРМАНСКОЙ ОБЛАСТИ ГРАЖДАНИН АЗЕРБАЙДЖАНА ПРИЗНАН ВИНОВНЫМ В ОСУЩЕСТВЛЕНИИ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ

15 Января 2014 09:22:00

Собранные следственными органами Следственного комитета Российской Федерации по Мурманской области доказательства признаны судом достаточными для вынесения приговора в отношении гражданина Азербайджана Ульви Джаббарова. Он признан виновным в совершении преступлений, предусмотренных **ч. 1 ст. 280 УК РФ** (публичные призывы к осуществлению экстремистской деятельности) и **ч. 1 ст. 282 УК РФ** (возбуждение розни и вражды в отношении людей, объединенных по религиозному признаку). Следствием и судом установлено, что с 31 октября 2011 по 17 января 2012 года Джаббаров, воспользовавшись компьютером, находящимся в Интернет-клубе, **разместил в открытом доступе в сети Интернет на своей персональной странице в социальной сети «ВКонтакте» видеоролики** под названием «Джихад» и «Обращение сестры перед операцией истишхада (самопожертвование), Вилайят Дагестан...», **содержащие признаки возбуждения розни и вражды в отношении людей, объединенных по религиозному признаку, а также признаки призыва к применению насилия, основанного на межрелигиозной ненависти, вражды и розни, то есть призыв к осуществлению экстремистской деятельности.** В ходе проведенных оперативно-розыскных мероприятий 29 июня 2013 года мужчина задержан по подозрению в совершении указанных преступлений сотрудниками правоохранительных органов. В тот же день по месту его фактического проживания и регистрации были проведены обыски, в ходе которых изъята литература экстремистского характера, а также технические средства для выхода в сеть «Интернет». Приговором суда Джаббарову **назначено наказание в виде исправительных работ сроком на 1 год и 9 месяцев с удержанием 10 процентов заработной платы в доход государства.**

В ОРЕНБУРГСКОЙ ОБЛАСТИ МУЖЧИНА ОСУЖДЕН ЗА НЕЗАКОННОЕ ИСПОЛЬЗОВАНИЕ ОБЪЕКТОВ АВТОРСКОГО ПРАВА

16 Декабря 2013

Собранные следственными органами Следственного комитета Российской Федерации по Оренбургской области доказательства признаны судом достаточными для вынесения приговора 22-летнему Виктору Мироненко. Он признан виновным в совершении преступлений, предусмотренных **ч. 2 ст. 146 УК РФ** (нарушение авторских и смежных прав, совершенное в крупном размере), **ч. 1 ст. 273 УК РФ** (создание, использование и распространение вредоносных компьютерных программ).

Следствием и судом установлено, что «интернет-пират» **разместил в глобальной сети Интернет на сайте бесплатных объявлений информацию о предоставлении компьютерной помощи и установке программного обеспечения.** В апреле 2013 года мужчина, находясь в одном из офисных помещений в городе Оренбурге, **использовал нелегальные программные продукты корпорации «Microsoft» и компании «Autodesk Inc.» посредством записи копий на флеш-накопители и распространения путем установки на накопитель жесткого диска программного обеспечения «Windows 7» и «Auto CAD».** Он также незаконно осуществил нейтрализацию средств защиты компьютерной информации одного программного продукта, являющегося **объектом авторского права.** Общая стоимость лицензионных экземпляров программных продуктов составляет более 100 тысяч рублей. Он нанес правообладателю ущерб в крупном размере. Приговором суда Мироненко назначено наказание в виде **исправительных работ на срок один год шесть месяцев с удержанием из заработка 10% в доход государства.**

В МУРМАНСКОЙ ОБЛАСТИ ЗАВЕРШЕНО РАССЛЕДОВАНИЕ УГОЛОВНОГО ДЕЛА В ОТНОШЕНИИ БЫВШЕГО СЛЕДОВАТЕЛЯ ПОЛИЦИИ, ОБВИНЯЕМОГО В ХИЩЕНИИ ДЕНЕЖНЫХ СРЕДСТВ

01 Октября 2013

Следственными органами Следственного комитета Российской Федерации по Мурманской области завершено расследование уголовного дела в отношении бывшего старшего следователя следственного управления регионального УМВД России Дениса Есипова. Он обвиняется в совершении преступлений, предусмотренных **ч. 1 ст. 285 УК РФ** (злоупотребление должностными полномочиями), **ч. 1 ст. 158 УК РФ** (кража), **ч. 3 ст. 30, ч. 3 ст. 159.3 УК РФ** (покушение на мошенничество с использованием платежных карт), **ч. 3 ст. 159.3 УК РФ** (мошенничество с использованием платежных карт).

По версии следствия, Есипов, в производстве которого на первоначальном этапе находилось уголовное дело в отношении бывшего советника экс-губернатора Геннадия Шубина, **незаконно использовал изъятые у последнего в ходе следствия предметы: банковские карты, а также мобильный телефон, которые использовал для хищения денежных средств с банковских счетов Шубина на сумму 198 тысяч 497 руб.** Есипов полагал, что о его действиях никто не узнает, поскольку банковские карты были выпущены иностранными банками. В ходе расследования уголовного дела Есипов раскаялся в совершенном преступлении и полностью возместил ущерб. Следствием собрана достаточная доказательственная база, в связи с чем уголовное дело с утвержденным обвинительным заключением направлено в суд для рассмотрения по существу. Напомним, что в настоящее время уголовное дело в отношении Геннадия Шубина расследуется в следственном управлении СК России по Мурманской области.

Лекция:

**Противодействие преступлениям
в сфере компьютерной информации**

Доклад закончен. Прошу задать вопросы